# State-sponsored economic cyber-espionage for commercial purposes

## Tackling an invisible but persistent risk to prosperity

Dr Gatra Priyandita, Bart Hogeveen and Dr Ben Stevens

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 67/2022

## About the authors

**Dr Gatra Priyandita** is an analyst with ASPI's International Cyber Policy Centre.

**Bart Hogeveen** is the head of the cyber capacity-building program with ASPI's International Cyber Policy Centre.

**Dr Ben Stevens** is a research intern working with ASPI's International Cyber Policy Centre.

## Acknowledgements

The authors would like to thank Dr Maaike Okano-Heijmans (Netherlands Institute of International Relations 'Clingendael'), the MITRE Corporation and colleagues at ASPI for their valuable feedback on drafts of this report.

## 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 Cyberspace and Digital Policy, US State Department.

This publication is an independent assessment by ASPI, and the views contained in this report are of the authors only.

More information about ASPI's work on norms of responsible state behaviour in cyberspace can be found at: https://www.aspi.org.au/cybernorms

## What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

## ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies and issues related to information and foreign interference and focuses on the impact those issues have on broader strategic policy. The centre has a growing mixture of expertise and skills, including teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity-building, satellite analysis, surveillance and China-related issues. The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The centre enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and the Indo-Pacific region, the ICPC has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public and private sectors. We thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre, contact: icpc@aspi.org.au.

## Important disclaimer



## ASPI

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_ICPC



First published December 2022. ISSN 2209-9689 (online). ISSN 2209-9670 (print).

Cover image: Pixelwise Creative Media, Canberra.


Funding for this report was provided by the US State Department.

# State-sponsored economic cyber-espionage for commercial purposes

## Tackling an invisible but persistent risk to prosperity

Dr Gatra Priyandita, Bart Hogeveen and Dr Ben Stevens

Policy Brief
Report No. 67/2022

# Contents


**Executive summary** 03

**Introduction** 04

**Establishing a norm of responsible state conduct in cyberspace** 06

- Key points 06
- Political commitments 06
- An agreement underpinned by principles of international law 06
- Public attributions of noncompliance 07
- Challenges in operationalising the norm against cyber-enabled theft of IP 07

**Current state practices of economic cyber-espionage** 10

- Key points 10
- The difference between ‘targeted’ and ‘affected’ 10
- Scale of reported incidents of economic cyber-espionage 11
- Cases of economic cyber-espionage attributed to the PRC Government 13
- Selection of targets, by geography and industry 13
- Severity of known cases of economic cyber-espionage 16
- Operation CuckooBees 17

**Strengthening national resilience against economic cyber-espionage** 18

- Key points 18
- Awareness and recognition of the risk 18
- Whole-of-government effort to advise, to assist and, *in extremis*, to intervene 19

**Conclusion and recommendations** 20

- Message to the 2022 G20 Leaders’ Summit 21

**Notes** 22

**Figure 1 references** 25

**Acronyms and abbreviations** 25

# Executive summary

In this policy brief, we examine the current state practice of cyber-enabled theft of intellectual property (IP)—or economic cyber-espionage—for commercial purposes. In 2015, the members of the G20 agreed that no state should engage in or support that practice.

Since 2015, the commitment to not conduct or support cyber-enabled theft of IP has clearly emerged as an accepted norm of responsible state behaviour in cyberspace, even though the norm is primarily advocated by the US, EU and individual European nations.

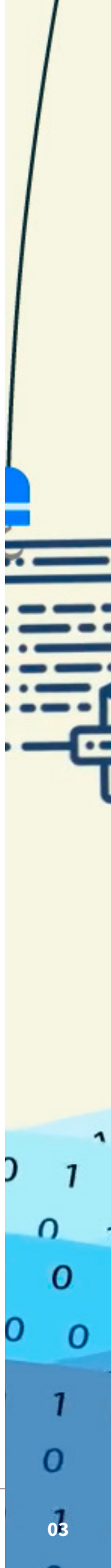
Based on databases of publicly reported incidents of cyber operations, it becomes clear that the risk of economic cyber-espionage hasn't disappeared. In fact, efforts to steal IP from universities and private firms have tripled as a significant component of states' cyber-espionage activities after a dip between 2015 and 2017.

The scale and severity of economic cyber-espionage has grown proportionally with the rise in and effect of overall acts of malicious cyber activities by states, such as political–military espionage, offensive operations and the use of cybertools during armed conflict. However, developing and emerging economies, such as countries in South and Southeast Asia and Latin America, increasingly see entities targeted and affected in their territory, in particular those that are part of transnational value chains.

At the national level, addressing the threat of economic cyber-espionage requires a combination of strengthened awareness and recognition, and outreach by national cybersecurity authorities and (counter)intelligence agencies to industries that produce and possess IP critical to future competitiveness and economic prosperity. The recent practice by the US Government of pre-emptively sharing intelligence assessments ahead of anticipated hostile Russian actions against Ukraine may herald a shift in culture of not sharing cyberthreat intelligence.[1] Also, governments may need to adjust domestic legislation to allow sensitive data to be shared with non-government and non-critical entities.

At the international level, the commitment to not engage in or support economic cyber-espionage would benefit from endorsement across various multilateral forums. Those include the UN First Committee on Disarmament and International Security, mechanisms related to the enforcement of the TRIPS Agreement on minimum standards for IP protection, and the various G20 policy tracks. Members of those forums have a duty to strengthen collective accountability for malicious cyber activities and to clarify mutual expectations of responsible behaviour in states' use of cybertools.

In this report, we look at emerging international rules and norms covering state-sponsored acts of economic cyber-espionage for commercial gain, offer an assessment of current state practice and finally we present a series of policy options governments could consider to defend their economies against the risk of economic cyber-espionage.



# Introduction

Modern economies increasingly rely on a nation's ability to absorb new (digital) technologies and be innovative. Both advanced and emerging economies are increasingly turning into knowledge- and technology-driven economies that are driven and enabled by intellectual property (IP). IP is accounting for the main value-add in today's trade interactions.[2] For instance, 47% of the European Union's GDP is estimated to be generated by industries that use a high number of intellectual property rights per employee.[3]

As IP becomes a central part of commercial success, businesses and research institutes have to invest more and more in securing their data and communication systems so that they can protect their sensitive business information and trade secrets from malicious actors. The surge in cybersecurity incidents during the Covid-19 pandemic[4] highlighted the challenges that come with dependencies on trust and confidence in a safe and secure digital environment.

The public movement restrictions that formed part of many nations' approaches to dealing with Covid-19 powered an unprecedented further push to digital transformation in both emerging and advanced economies. At the same time, disruptions to global supply chains and concerns about overdependence on foreign countries (particularly in critical technologies), have reinvigorated debates about the need for greater economic and technological sovereignty.

The drive for technological sovereignty is exacerbating the existing challenge of managing the misappropriation of IP held by foreign companies, including that of stopping and defending against state-sponsored theft of IP. For instance, businesses operating in the semiconductor industry[5] or laboratories involved in vaccine development are facing sophisticated and sustained attempts by outsiders to steal sensitive business information and industrial designs.[6] Cybersecurity agencies worldwide reported that, during the pandemic, those threats increased not only in scale but also in severity.[7]

State cybersecurity and intelligence agencies are dominant actors at this intersection of national security, economic progress and cybersecurity. On the one hand, they offer critical infrastructure operators and high-value industries in their economies advice and support to defend against cybersecurity threats. On the other hand, some (cyber)security and (counter)intelligence agencies are also involved in conducting, sponsoring or condoning campaigns of ICT-enabled espionage to support domestic commercial firms (a practice we refer to as *economic cyber-espionage*; see Table 1).

Given our economies' strong dependence on the confidentiality, integrity and availability of systems, networks and data, compromises have a significant impact—at individual, sectoral and national levels. This concern is even more urgent when nations use state resources against private organisations, such as individual companies and research institutes. Such practices have severe ramifications for medium-term economic growth and future prosperity.

Table 1: Glossary

| | |
|---|---|
| **Economic cyber-espionage**: the unauthorised collection of commercially valuable assets, through compromises of digital systems and communication channels, *by one state against another, or by one state against a private entity.* | **Intellectual property (IP)**: items that are the property of the mind or proprietary knowledge.<br><br>IP can be protected in various ways, such as through patents, trademarks, registered designs, geographical indications and copyrights.<br><br>These forms of protection are referred to as 'IP rights'. They're based on eligibility criteria and are legally binding and enforceable.<br><br>**Sensitive business information and trade secrets**: non-described and non-disclosed forms of information of (high) value. They're protected as long as they're not known to the public. Sensitive business information and trade secrets cease to exist after public disclosure, by whichever means. Their protection is not enforceable, and the burden for protection lies with the owner of the IP. |
| **Industrial or commercial cyber-espionage**: the unauthorised collection of commercially valuable assets, through compromises of digital systems and communication channels, *by one private entity against another private entity.* | |
| **Cyber-enabled intellectual property crime**: gaining access to, distribute and/or use of IP through digital means without and/or beyond initial authorisation and in violation of the rights of the owner(s). | |

The sense of urgency and visibility of this issue is compounded by the fact that most of these activities are largely invisible or are discovered years after they have occurred.[8] Even though former US National Security Agency Director Keith Alexander referred to cyber-enabled IP theft in the US as the 'greatest transfer of wealth in history'[9], in comparison to many other forms of malicious cyber activity, such as ransomware or offensive cyber operations, the risk of economic cyber-espionage often doesn't create the same sense of urgency among policymakers or the business community.

Yet, the consequences are significant. For individual entities, evidence of stolen IP may lead to a loss in royalties from patents or trademarks, costs in litigation and court proceedings and a need to repair and uplift IT systems and cybersecurity measures. There are also more enduring economic impacts, such as a competitor gaining unfair R&D or market access. For those who are on the receiving end of such theft, larger costs include the devaluation of trade names, revoked contracts and lost market opportunities.[10]

But beyond losses to individual firms or research institutes, IP theft has broader implications nationally and globally. In 2018, the US national intelligence community estimated an annual US$400 billion loss because of commercial cyber espionage.[11] Assessments of risk for the EU are in the range of €60 billion annually, affecting some 300,000 jobs.[12] The longer term economic stakes may even be higher, as such cyber-enabled theft not only harms the enabling environment for R&D and innovation but may also deter foreign direct investment, particularly in industries that are part of transnational supply chains.

Last but not least, the effects of unhalted persistent forms of economic cyber-espionage may undermine overall trust and confidence in the internet, its technical integrity, and its use. The inability of the international community to manage responsible behaviour of states in the cyber domain will negatively reflect on inter-state relations, global trade and innovation and industries' confidence in a rules-based international order.

# Establishing a norm of responsible state conduct in cyberspace

## Key points

- Traditional espionage and cyber-enabled forms of espionage are accepted state practice, but state-sponsored espionage for commercial purposes is not. The US and the People's Republic of China (PRC) formally clarified this constraining norm in 2015, which was followed by an endorsement by the full G20 membership.
- The G20-agreed norm against cyber-enabled theft of IP is underpinned by a body of international law, including the UN Charter and the international trade regime centred on the World Trade Organization (WTO). It has also featured in a couple of public attributions of malicious cyber incidents.

## Political commitments

In 2015, the leaders of the G20, which is the premier forum for international economic cooperation, recognised the risk that state-sponsored economic cyber-espionage poses to the long-term economic growth of nations for the first time. They agreed 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.*'[13]

This agreement can be traced back to a meeting between US President Barack Obama and Chinese President Xi Jinping in September 2015, where the US and Chinese governments reached a shared understanding that neither country would conduct or support the cyber-enabled theft of IP, including trade secrets and confidential business information, for commercial gains.[14]

The purpose of the 2015 agreement was to constrain states in their use of cyber capabilities and put an end to their theft of commercially valuable data with the aim of benefiting local companies. The bilateral agreement between the US and the PRC was subsequently endorsed by the G20 and supplemented with bilateral agreements between China and the UK, Germany, Australia and Canada.[15]

## An agreement underpinned by principles of international law

This norm is underpinned by various existing international legal and regulatory frameworks that deal with (inter)national security, economic security and cybersecurity. Foundational is the acceptance that international law, particularly the UN Charter, is applicable to state conduct in cyberspace.[16] This recognition was conceived in the context of the UN General Assembly's First Committee, which deals with inter-state cooperation on issues of cybersecurity that may affect international peace and security.

On the issue of state-sponsored cyber operations, the UN General Assembly in 2021 recognised the principles of sovereignty, non-intervention and state responsibility and reaffirmed:


'that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. It also reaffirms that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.'[17]

The 1994 WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS agreement) aims to support states to 'reduce distortions and impediments to international trade ... [and] promote effective and adequate protection of intellectual property rights'.[18] It commits signatories to assure nationals of other states minimum guarantees of 'effective protection against unfair competition' in their territory.[19] For the moment, those obligations don't appear to extend to state-to-state IP infringements.[20]

## Public attributions of noncompliance

To date, in efforts to apply norms of responsible state behaviour, two major cases of public attributions of cyber incidents are based on the norm against economic cyber-espionage. In 2018, the UK Government held the PRC Ministry of State Security responsible for 'a malicious cyber campaign targeting intellectual property and sensitive commercial data in Europe, Asia and the US' and asserted that parts of the Chinese Government were:

> not upholding the commitments China made directly to the UK in a 2015 bilateral agreement. It is also inconsistent with G20 commitments that no country should conduct or support ICT enabled theft of intellectual property, including trade secrets or other confidential business information.[21]

In 2021, the US Government, in conjunction with seven other countries and two international organisations, held the PRC Government responsible for 'an intelligence enterprise that includes contract hackers who also conduct unsanctioned cyber operations worldwide, including for their own personal profit' and stated that those operations stand 'in stark contrast to the PRC's bilateral and multilateral commitments to refrain from engaging in cyber-enabled theft of intellectual property for commercial advantage.'[22]

Together, those political commitments, in combination with those legal underpinnings and a set of public callouts of states that violate their obligations, have arguably led to the emergence of a norm against cyber-enabled theft of IP (see Figure 1 on page 9). However, challenges in pursuing compliance and imposing means of verification remain.

## Challenges in operationalising the norm against cyber-enabled theft of IP

It isn't uncommon for international agreements to be interpreted and followed up differently in various domestic contexts. But when those discrepancies are too large, they undermine efforts to ensure compliance and affect the overall observance of the norm. In fact, the terms on which the norm is based—such as 'IP', 'cyber-enabled theft' and 'for commercial gain'—are quite undefined and subject to competing interpretations.

In terms of IP protection, the US tends to be most concerned with the theft, reselling and misappropriation of trade secrets and sensitive business information.[23] Those are the forms of IP that are not registered or disclosed and the protection of which is hardly enforceable and left to the IP owner. [24] Most other economies, however, concentrate on the protection of *IP rights*, such as patents, copyrights and registered trademarks. In fact, some economies, including China, have made notable progress in strengthening their domestic IP protection regimes as required under the TRIPS agreement.[25]

With the modifier 'for commercial gain', the signatories to the various bilateral and multilateral agreements intended to make a distinction between accepted forms of cyber espionage (such as intelligence-gathering for political, military and national security purposes) and non-acceptable forms (such as the theft of economic or corporate data for commercial purposes). This may work in jurisdictions where political, military and economic objectives and responsibilities among state agencies are clearly separated. For some countries, however, industrial development and other efforts to bridge the (digital) development divide are considered fundamental on grounds of national interests. For instance, China's stated ambition of becoming the world's most technologically advanced economy also includes an acceptance of the legitimacy of obtaining commercial information for the development of military (industrial) capabilities.[26]

All this is further compounded by the fact that several states, including members of the G20, deny their possession or sponsorship of (offensive) cyber capabilities that could be leveraged for economic cyber-espionage (and the theft of IP for commercial gain). In particular, Russia, China and Iran fall into this category.[27] Despite ample evidence, they categorically deny and object to reports of their state-sponsored cyber activities.[28] Meanwhile, other states are in a state of denial of the fact that states use their cyber capabilities for political, military and economic advancement. That group, mostly from the global South, struggle to acknowledge and recognise the seriousness of the risk of cyber espionage generally due to overall shortcomings in their national cybersecurity maturity.[29]

Figure 1: Evolution of the norm against cyber-enabled theft of IP

# Evolution of the norm against cyber-enabled theft of IP

**US DoD: Strategy for Operating in Cyberspace** — July 2011
The Pentagon's Strategy for Operating in Cyberpace lists theft of IP as "the most pervasive cyber threat today"

**Pentagon's Annual Report to Congress** — May 2013
The Pentagon's annual report to Congress directly accused China of using its military to conduct cyberespionage operations against US firms

**US DoJ: Indictment of PLA officers** — May 2014
The US Department of Justice indicts five PLA officers with charges of crimes related to cyberespionage

**US & China agree not to engage in economic cyberespionage** — Sept 2015
Presidents Obama and Xi reach a shared understanding that neither government would support or conduct cyber-enabled theft of intellectual property

**G20 Leaders agree not to support economic cyberespionage** — Nov 2015
The G20 Leaders agree 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.'

**Germany & China agree not to engage in economic cyberespionage** — June 2016
China and Germany release joint declaration that neither operates or knowingly supports 'the infringement of intellectual property, trade or business secrets through the use of cyberspace in order to attain competitive advantage for their businesses or commercial sectors

**Australia & China agree not to engage in economic cyberespionage** — April 2017
China and Australia agree to commit to a norm of refraining from the theft of IP.

**Germany: China, Russia and Iran conduct economic espionage** — July 2017
Germany's Federal Ministry of Interior identifies China, Russia and Iran as responsible for espionage and cyberattacks against Germany.

**Eight states, NATO and EU attribute a cyberespionage campaign** — July 2021
A coalition of countries accuse a hacker group affiliated with Chinese state for exploiting zero-day vulnerabilities in the Microsoft Exchange software, enableing a large-scale campaign of cyberespionage.

**"Greatest transfer of wealth in history"** — July 2012
Director NSA and Cyber Commander Gen. Keith Alexander refers to the loss of industrial information and intellectual property through cyberespionage as "the greatest transfer of wealth in history".

**Presidential Directive: refrain from collecting trade secrets** — January 2014
US President Obama issues Presidential Policy Directive 28, which refrains the U.S. from the 'collection of foreign private commercial information or trade secrets' to 'afford a competitive advantage' to U.S. commercial firms.

**UN member states endorse 11 norms of responsible state behaviour** — August 2015
The UN member states, through a Group of Governmental Experts, agree a set of 11 norms describing what States should and should not be doing in cyberspace

**UK & China agree not to engage in economic cyberespionage** — October 2015
The UK and China sign a cybersecurity agreement where they commit to not use cyberespionage to steal commercial secrets.

**G7 Leaders embrace G20 commitment** — May 2016
The G7 Leaders endorse the wording from the 2015 G20 Communique and reaffirm that no state should sponsor economic cyberespionage operations.

**G7 Foreign Ministers commit not to sponsor economic espinage** — April 2017
The G7 Foreign Ministers issue a statement on responsible state behaviour in cyberspace, including a commitment not to sponsor ICT-enabled theft of IP, including trade secrets or confidential business information

**Canada & China agree not to engage in economic cyberespionage** — June 2017
China and Canada agree not to engage in state-sponsored hacking of each other's trade secrets and business information

**US, UK and others attribute a cyber-espionage campaign** — December 2018
A coalition of states, including the US and UK, condemns China for sponsoring aglobal cyberespionage campaign with reference to China's bilateral and multilateral commitments.

**FBI & MI6 warn industry of cyberespionage risks** — July 2022
The Director of the FBI and MI5 Director-General warn business leaders that China's sponsorship of intellectual property theft constitutes one of the biggest threats to advanced economies.

Figure 1 references can be found on page 25.

# Current state practices of economic cyber-espionage

## Key points

- The risk of economic cyber-espionage to nations' long-term prosperity can be expected to continue to increase now that major-power competition is increasingly spilling into economic and technological domains.
- The number of known cyber intrusions affecting commercial firms and universities around the world has increased proportionally with overall state-sponsored cyber operations since 2015, and such intrusions are now also affecting developing and emerging economies.
- States known for a combination of assertive industrial development strategies, strong state–industry relations and recognised (offensive) cyber capabilities are on the watchlist for general infringements of IP rights.

In this section, we assess current state practice of economic cyber-espionage by looking at:

1. the *scale* of reported cases of state-sponsored cyber operations
2. the *spread* of targeted and affected industries (see box) across geographical locations
3. the *severity* of reported cases.

### The difference between 'targeted' and 'affected'

Generally, entities that are *targeted* in cyber operations face sustained efforts by malign actors to infiltrate their networks and systems. Entities that are *affected* by cyber operations may fall victim because vulnerabilities in their systems expose them to attacks or espionage operations. While this may seem straightforward, distinguishing between entities that are *targeted* and those that are *affected* constitutes a central challenge in the technical attribution of a cyber incident.

For instance, when Microsoft Exchange servers were breached in 2021, more than 250,000 entities (including government and commercial firms) worldwide were affected.[30] Those entities may have had some of their data and networks exposed, and some may have had their data stolen. However, for many of them, it's very much possible that they weren't targeted because of their economic value or IP, but because of the compromised software they were using on their systems. Many Microsoft Exchange clients had failed to patch their systems in a timely manner.

For the purposes of identifying the theft of IP, the distinction may be less relevant. This is because, once sensitive business information or trade secrets are stolen, their economic value has been lost. However, for the purposes of protection and risk mitigation, and potentially government intervention, it's relevant to know whether a company, sector or industry is specifically targeted.

This assessment of current state practice is based on data listed in the Council on Foreign Relations' Cyber Operations Tracker, which tabulates publicly known cyber incidents that are alleged to be state sponsored. It's nearly impossible to make a firm estimate of the scale, spread and severity of economic cyber-espionage. Taking the three categories together, by working with numbers at the macro level

and by corroborating reported incidents with public materials, a plausible operational picture can be sketched of economic cyber-espionage operations conducted by 'advanced persistent threat' (APT) actors.[31]

APTs is the term used by commercial cybersecurity firms and national cybersecurity authorities to refer to organised hacking groups that are distinguished for their ability to sustain unauthorised access into computer networks for extended periods. Because of the extensive resources needed to sustain such costly processes, they're often either parts of a state (security) organisation or serve as proxy actors for a state. In these instances, they're referred to as 'state sponsored'.

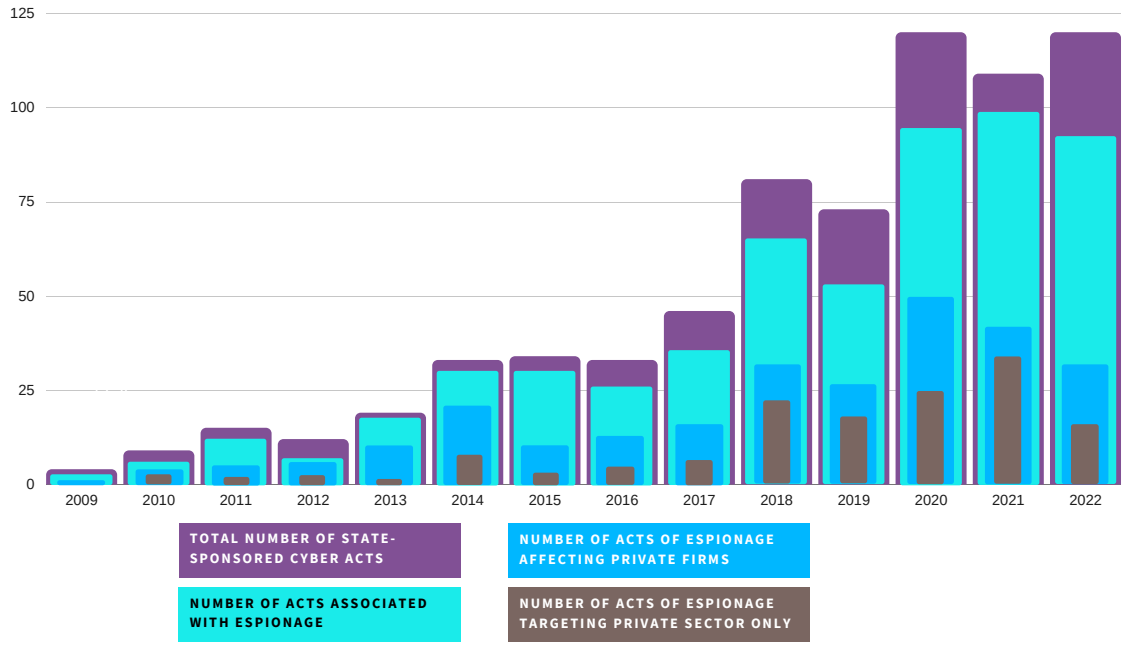
## Scale of reported incidents of economic cyber-espionage

The scale of state-sponsored cyber operations can be assessed by looking at the numbers of reported incidents. Figure 2 shows that those numbers have drastically increased in the past 10 years, from fewer than 40 between 2014 and 2016 to more than 100 since 2020.[32]

The tripling of the number of incidents today compared to 2015 is a reflection of a range of developments, including the deteriorating climate of global inter-state cooperation,[33] the increased and improved cyber capabilities of states,[34] and strengthened efforts in public reporting and disclosures.[35]

State-sponsored cyber-espionage is undeniably an integral part of this operational picture. It accounts for more than 80% of all reported state-sponsored cyber incidents. Similarly, an uptick can be observed in the number of cyber intrusions carried out by hacking groups that affect commercial firms and universities.[36]

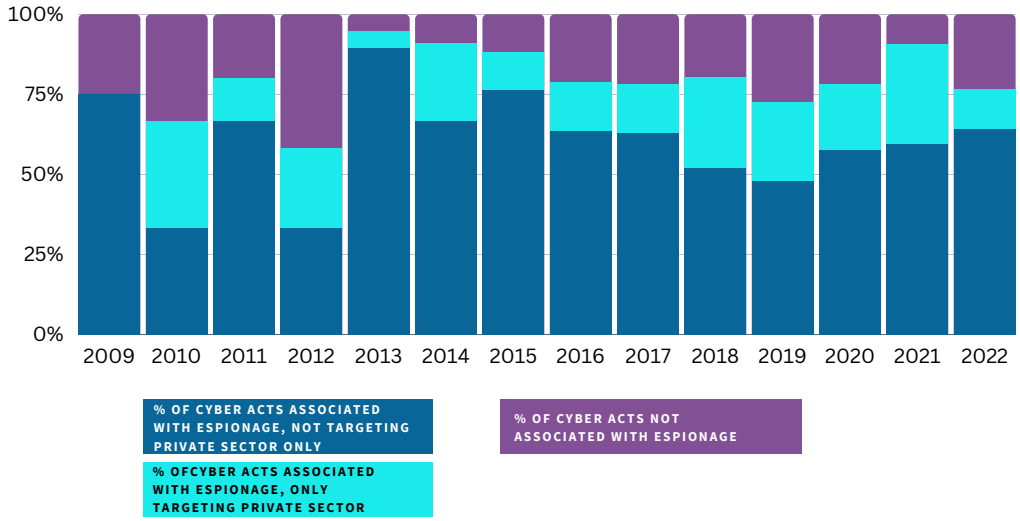
Figure 2: Number of reported incidents of state-sponsored cyber operations between 2009 and 2022




Source: Based on the Council on Foreign Relations' Cyber Operations Tracker.

From 2010 onwards, cyber-espionage campaigns that specifically target private-sector entities have made up a noticeable share of all known acts of cyber espionage (see light blue bar in Figure 3). In 2020 and 2021, they accounted for from 21% to 31% of all known cyber-espionage operations. The initial relative downturn for 2022 can be explained by the spike in state-sponsored cyber operations in the context of the Russia–Ukraine war for purposes other than espionage.

Figure 3: Proportions of reported acts of state-sponsored cyber espionage among overall numbers of reported acts of state-sponsored cyber operations between 2009 and 2022




Source: Based on the Council on Foreign Relations' Cyber Operations Tracker.

Figure 3 also shows an initial relative decrease in espionage acts exclusively targeting the private sector between 2015 and 2017. This dip in the share of economic cyber-espionage as part of overall state-sponsored cyber operations was also partly acknowledged by US intelligence officials. In February 2016, for instance, Director of National Intelligence James Clapper stated that 'private-sector security experts have identified limited ongoing cyber activity from China but have not verified state sponsorship or the use of exfiltrated data for commercial gain.'[37] At the same time, the raw number of incidents targeting the private sector continued to rise (see Figure 2).

Despite concerns from the US side about China's compliance with the norm, a 2018 joint report by the Center for Strategic and International Studies and US cybersecurity firm McAfee estimated that the US–China and G20 agreement may have 'saved' the US economy as much as US$15 billion a year in reduced stolen IP.[38]

It's possible that the political consensus in the mid-2010s persuaded APT actors to play more by the book and act less blatantly in their commercialisation of stolen trade secrets. The threat of trade sanctions that was reportedly on the table in Washington, in combination with ongoing criminal investigations into individual officials, may have also had an initial deterrent effect.[39] Another hypothesis that's gaining credence is that an important reorganisation of cyber responsibilities within the People's Liberation Army (PLA) and Ministry of State Security (MSS) between 2015 and 2017 had a dampening effect on operations.[40]

From 2018 onwards, however, the share of economic cyber-espionage resurged to pre-2015 levels (see Figure 3), and in 2021 the global number of reported incidents tripled compared to 2017.[41] Of the alleged state-sponsored hacking operations after 2018, many are assessed to be affiliated with or coordinated by the MSS and the PLA (see box on next page).[42]

## Cases of economic cyber-espionage attributed to the PRC Government

- In 2017, three Chinese hackers affiliated with the China-based cybersecurity firm Boyusec were arrested for compromising the networks of financial, engineering and technology firms in the US continuously since 2011.[43]
- In 2018, the UK and others held 'APT 10' responsible for a cyber-espionage campaign against managed service providers (MSPs) with the aim of seeking 'intellectual property and commercially sensitive information of the MSPs and their clients'. APT 10 is assessed to have 'an enduring relationship' with China's MSS in support of China's 'state requirements'.[44]
- In 2020, four members of the PLA's 54th Research Institute, which is a component of the Chinese military, were charged by the US Department of Justice with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax.[45]
- Criminal indictments by the US Department of Justice have extended to MSS personnel. In February 2020, four Chinese nationals belonging to 'APT 40', with alleged links to the MSS, were charged with a global intrusion campaign targeting IP and confidential business information.[46] Computer systems of dozens of universities, companies, research entities and government organisations were targeted by APT 40 actions between 2011 and 2018.
- In 2021, a coalition of eight countries, NATO and the EU held a hacker group affiliated with China's MSS, dubbed Hafnium, responsible for exploiting zero-day vulnerabilities in Microsoft Exchange software that enabled a large-scale campaign of espionage, including acquiring personally identifiable information and intellectual property.[47]

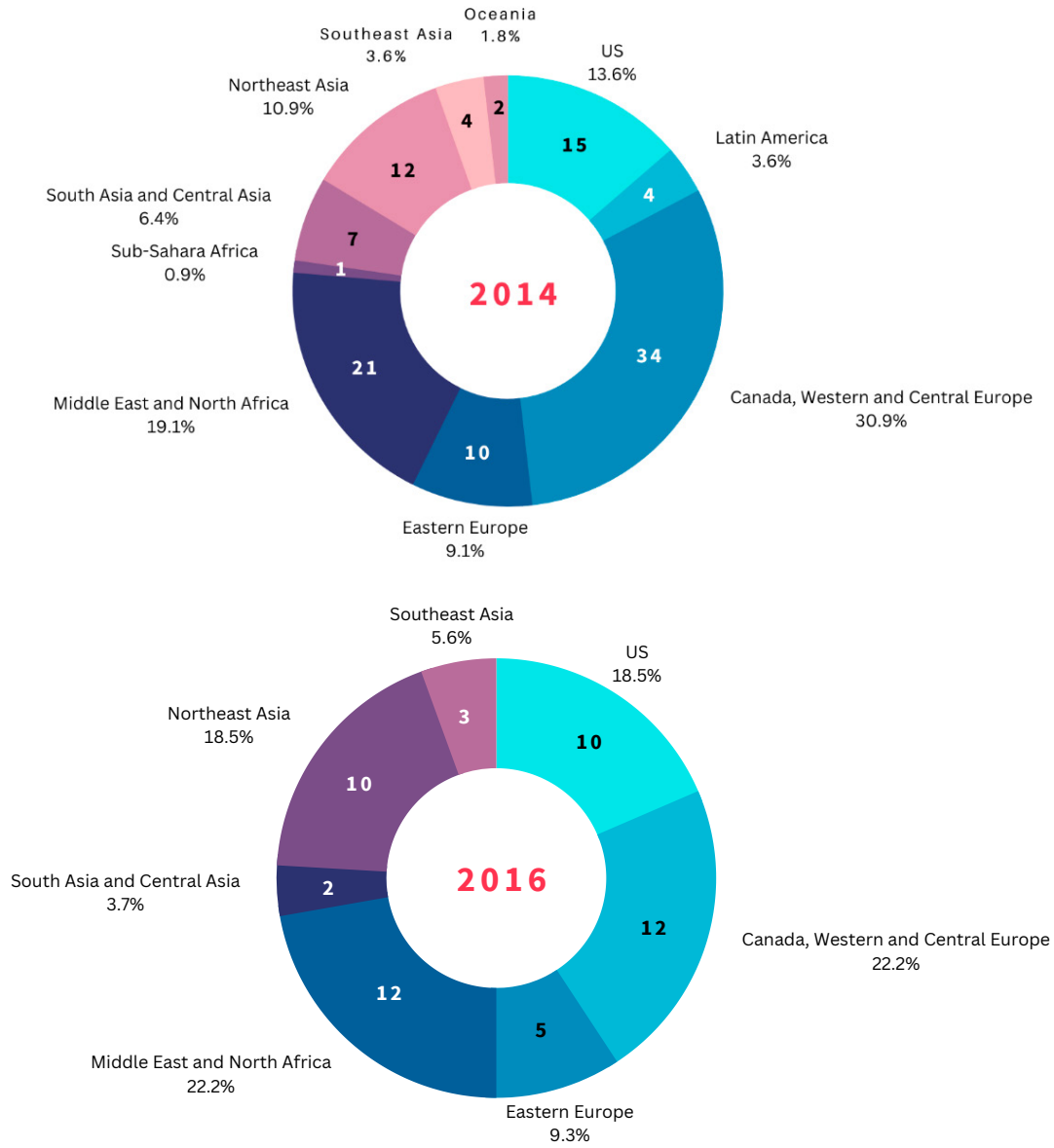
## Selection of targets, by geography and industry

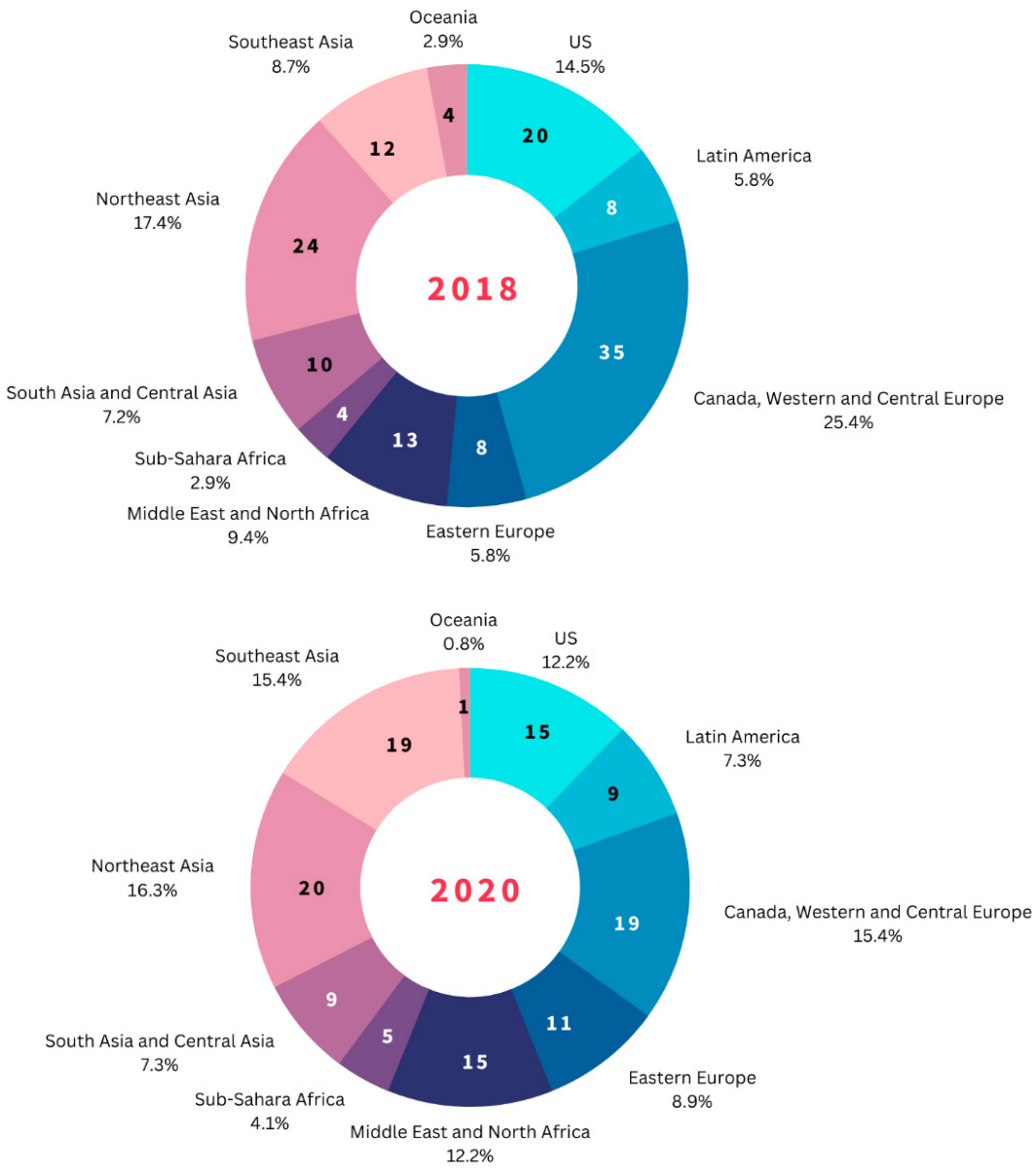
A further indication of the state practice of economic cyber-espionage is the spread in geographical range and the targeting of industrial sectors.[48] The US continues to stand as the biggest single economy targeted by state-sponsored cyber espionage, but private entities in Northeast Asia, Southeast Asia, South Asia and the Middle East are increasingly among those affected or targeted (see Figure 4).[49]

As hackers seek trade secrets and opportunities to exploit cybersecurity weaknesses along transnational supply chains, commercial firms and universities in developing and emerging economies have increasingly become victims. For instance, incidents affecting and targeting private-sector entities in Southeast Asia grew from 3.6% in 2014 to 15.4% in 2020. Similar trends (see Figure 4) can be observed from the numbers for South Asia (6.4% in 2014 to 7.3% in 2020) and Latin America (3.6% in 2014 to 7.3% in 2020). This is an indication of how the increase in absolute numbers of acts of cyber espionage has spread across other regions in the world.

Private entities in other advanced economies such as Canada and those of Western and Central Europe also remain important targets of cyber-espionage. Their total share of cyber-espionage intrusions fluctuated between 30.9% in 2014 and 15.4% in 2020. Economies in the Middle East and North Africa were faced with 21% of reported cyber-espionage incidents in 2014 and 12.2% in 2020.

Figure 4: Private entities (including commercial firms and universities) affected and targeted by APTs, by region, in 2014, 2016, 2018 and 2020. Note: Numbers in pie chart reflect the number of recorded incidents affecting firms in these regions.



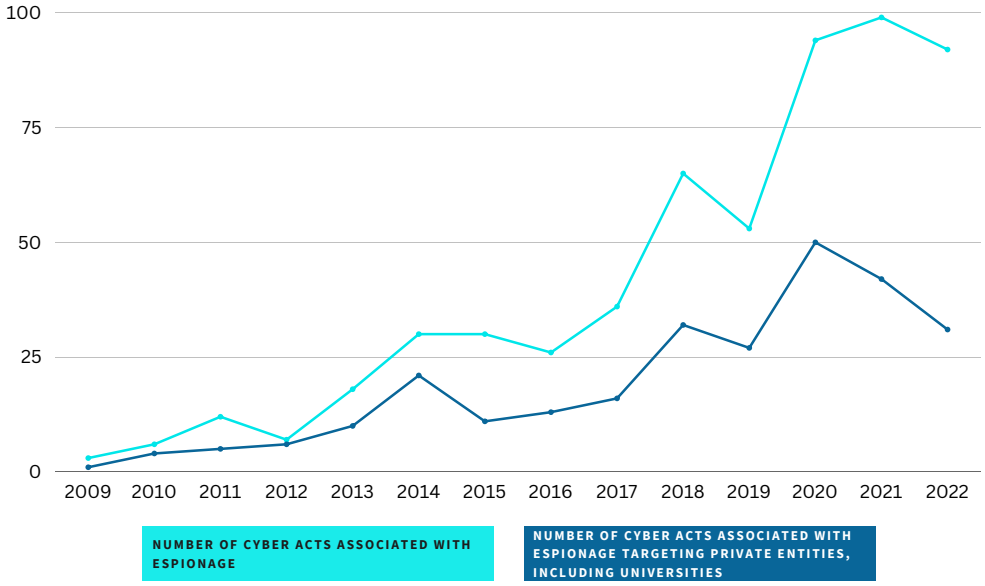



Source: Based on data from the Council on Foreign Relations' Cyber Operations Tracker.

The data further seems to affirm that companies and universities in advanced economies are the main targets of cyber-espionage operations. Of the known cyber intrusions perpetrated by APTs (Figure 5), the number affecting commercial firms and universities around the world has increased significantly since 2015. Out of the 329 known cases recorded since 2009, the majority (80%) took place between 2016 and 2022.

It's plausible, however, to assume that many instances of cybersecurity compromises in developing and emerging economies remain unreported. Whereas the greater (capabilities for) situational awareness in cyber-mature nations have led to more cases of economic cyber-espionage being detected and hence this issue is flagged as a distinct national and economic security threat.

Figure 5: Number of APT-attributed cyber-espionage operations that affect commercial firms and universities, 2009 to 2022




Source: Based on data from the Council on Foreign Relations' Cyber Operations Tracker.

While the graph suggests a decline in cases from 2020, it's foreseeable that these figures will change in future, as public disclosures and media reporting of cyber operations often come with a significant delay. Furthermore, the Covid-19 pandemic, lockdowns and health-response priorities may have affected the operational readiness of state-sponsored APTs or may have led to more purpose-specific targeting of specific sectors, such as medical research, which is a sector that's seen an uptick in hacks.[50]

## Severity of known cases of economic cyber-espionage

Another factor to consider in assessing the current state practice of economic cyber-espionage is the severity of cases. There's reason to assume that the severity of individual cases has increased over the years in terms of the tactics, techniques and procedures (TTPs) used, the specific targeting and the perseverance of attackers.

An assessment of APTs operating in Southeast Asia shows that many have been operational for an average of 10 years, during which their tactics developed from 'unspecific' targeting to 'inclusive' and finally 'specific' targeting.[51] While hackers tend to gain access through common means such as phishing attempts, their subsequent TTPs show a higher level of sophistication and access to resources. They pursue targets selectively, show persistence in their commitment, and demonstrate agility when victim organisations make changes to their IT security. APTs' toolset comprises advanced use of supply-chain compromises, consistent signing of malware using compromised digital certificates, and the deployment of bootkits.[52]

## Operation CuckooBees

In May 2022, the US–Israeli cybersecurity firm Cybereason reported on an economic cyber-espionage campaign that it dubbed 'Operation CuckooBees'.[53] The company estimated that a hacking group exfiltrated hundreds of gigabytes of information from some 30 multinational companies, which may potentially be worth trillions of US dollars.[54]

The attackers were observed to have spent years clandestinely conducting reconnaissance and identifying valuable data. They targeted IP developed by the victim companies, including 'sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data'.[55] Targets of Operation CuckooBees are said to be technology and manufacturing companies located in Asia, Europe and North America.

Mandiant, which is a major American cybersecurity firm, observes that targeting by 'APT 41' is 'consistent with China's national strategies to move production capabilities into research and development (R&D)-heavy fields', particularly those associated with the 'Made in China 2020' strategic plan.[56] The entities targeted may include those within the healthcare sector, pharmaceuticals, high-tech semiconductors and advanced hardware, electric vehicles, and telecommunications.

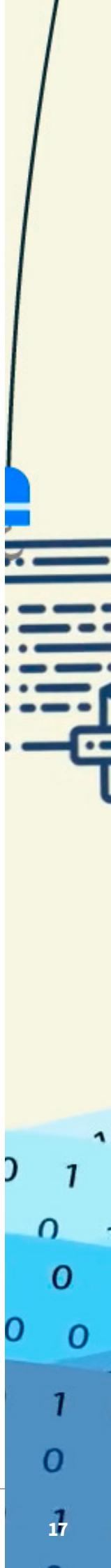
The severity of cases is further compounded by situations in which some states exert a growing ability and confidence in using offensive cybertools in support of an assertive industrial development strategy.

For instance, the PRC has some of the most pronounced ambitions to build indigenous technology capabilities, as is evident in its 'Made in China 2025' strategic plan. In an effort to accelerate its R&D processes, China seeks to push government and industry to address technology choke-points (undesirable dependences on foreign markets) and encourage 'little giants'—a set of globally competitive and highly specialised companies dominating niche markets—to find key and core technologies as a prerequisite to securing funding.[57] This objective is further facilitated by the close relationships between China's intelligence and security agencies, academia and tech industry.[58]

Altogether, such situations create a conducive and incentivised environment for non-state and state-sponsored APTs to engage in economic cyber-espionage for commercial gain in other—more progressed or competing—economies.

But it's not only an issue with the PRC. There are other states with similarly assertive industrial development strategies, strong state–industry relations and recognised offensive cyber capabilities.

For example, Russia, Israel and France have long been on watchlists for being suspected of stealing IP from US firms, including through economic cyber-espionage.[59] Other APTs reportedly associated with states such as Iran, North Korea and Vietnam are also involved in cyber-espionage operations for commercial gain. For example, 'APT 31', which is affiliated with Vietnam's intelligence and security sector, has been linked to cyber-enabled espionage operations against foreign companies based in Vietnam and Thailand.[60]



# Strengthening national resilience against economic cyber-espionage

## Key points

- Defending against cyber-enabled theft of IP only works in a preventive manner. Therefore, national efforts to strengthen cybersecurity resilience are an important avenue to address the risk of falling victim to economic cyber-espionage.
- Governments have a duty and responsibility to help protect companies in defending against state actors or their proxies, given their skills, resources and endurance.

Constraining the state practice of economic cyber-espionage requires a two-pronged approach of international and domestic cybersecurity resilience measures. On the one hand, malicious state and state-sponsored actors can be deterred by a combination of diplomatic and national defence measures. Those measures include policy responses such as public attributions, (the threat of) countermeasures through offensive cyber operations, invoking WTO dispute-settlement instruments and a variety of sanctions—often in a collaborative effort by multiple states. Overall, however, this cyberdiplomacy toolkit has proven to be rather weak in stopping unacceptable forms of cyber operations.

On the other hand, the negative consequences of economic cyber-espionage can be mitigated only in a preventive manner, and most effectively through domestic measures. Once trade secrets are stolen, they can't be retaken and have lost their value. Therefore, greater and more immediate effect can be achieved in the domestic cybersecurity space.

The effort to strengthen domestic capabilities of cybersecurity resilience isn't unique to the threat of economic cyber-espionage. It equally addresses other cybersecurity risks, such as ransomware attacks, data breaches and cybercrime. It requires the participation of various parts of government, including national computer emergency response teams (CERTs), as well as local industry, research institutes and commercial cybersecurity service providers.

Prevention of an invisible yet persistent risk requires awareness and recognition of the risk first at the political and C-suite levels before any regulatory, operational and technical measures can be introduced and effectively deployed.

## Awareness and recognition of the risk

A foundational step for governments in raising their awareness of the issue of state-sponsored economic cyber-espionage is to improve visibility. National CERTs or national cybersecurity centres in combination with non-commercial and private cybersecurity service providers play an important role in flagging risks. Many of them have started a practice of publishing regular threat reports.

For instance, a report by cybersecurity firm Mandiant on 'APT 1' in 2013 served as an eye-opener to the US public policy community. One of the accomplishments of the 2015 G20 leaders' agreement was the elevation of the issue of state-sponsored economic cyber-espionage to the agenda of political leaders and bringing the threat of IP theft (including that of trade secrets and sensitive business information) into the public policy discourse.

The US had first identified economic cyber-espionage as a threat in its 2011 International Strategy for Cyberspace. Australia, the UK and Canada, as well as Denmark, Estonia, Germany, the Netherlands, Poland and Spain, followed years later in recognising this threat in their own cybersecurity strategies and cyber threat and national intelligence assessments.[61]

The challenge in qualifying the real consequences of IP theft to the economy is an important cognitive hindrance. This is further compounded by the sense of a lack of capacity to protect and withstand foreign states' malicious cyber operations, as well as reluctance by many industries to report and disclose any compromises, or to even acknowledge they may be targets of foreign espionage.

In the US, Canada, Japan and some EU member states, the (counter)intelligence and law-enforcement agencies have taken up a role in ringing alarm bells in the public domain while at the same time privately tipping off domestic companies that they consider at risk.[62]

The structural and consistent sharing of technical forensic data and cybersecurity analyses by government agencies has been a systemic challenge in domestic settings as well as between states. The recent practice by the US Government of pre-emptively sharing intelligence assessments ahead of anticipated Russian actions against Ukraine may herald a shift in culture.[63] Also, government should consider adjusting domestic legislation to allow the sharing of sensitive data with non-government and non-critical entities, as the Netherlands has recently done.[64]

## Whole-of-government effort to advise, to assist and, *in extremis*, to intervene

The economic sectors most vulnerable to state-sponsored economic cyber-espionage are likely to include 'softer' ones, such as start-ups, academia and other research, development and innovation hubs. They may maintain less hardened security perimeters, since they're not considered entities of national security or critical infrastructure, and often entertain international cooperation with peers operating in jurisdictions of less like-minded states.

Knowing which companies, industries and sectors are the most IP-intensive and critical assets of future economic growth is a first step before being able to assess their exposure to foreign intelligence agencies and to monitor specific cybersecurity threats to them. Such an effort would require government agencies responsible for economic policy and digital transformation as well as national IP authorities to work together with their counterparts in the national security domain.

Government authorities have a clear duty and responsibility to help protect and defend companies operating in their territory against state actors or their proxies, given the skills, resources and endurance that APTs can bring to bear.[65] This can range from active awareness-raising campaigns and assertive sharing of good IT security practices to running regular health checks and elevating the adoption of internet security standards by network operators and internet service providers upon which businesses are dependent.

# Conclusion and recommendations

In the seven years since the shared understanding between the US and China and the G20 agreement that followed, the international system has come to be marked by strategic distrust between the world's major economic powers. In a global environment shaped by strategic rivalry and political distrust, states are increasingly incentivised to pursue their national interests by using all levers of national power and acting with contempt for international rules, norms and principles.

Strategic competition has spilled into the economic and technological domains and states have become more comfortable and capable using offensive cyber capabilities. Our analysis shows that the state practice of economic cyber-espionage appears to have resurged to pre-2015 levels and tripled in raw numbers. State-sponsored and cyber-enabled theft of IP has increased in scale, geographical spread and severity, and in an increasing number of situations the private sector and universities have been specifically targeted. This assessment is based on publicly recorded incidents. Given the clandestine and invisible nature of these acts, and the lag in time before the effects of IP theft are noticeable and disclosed or reported, there's reason to believe that the real scale, spread and severity are even higher.

Addressing this invisible but persistent threat to economic competitiveness and prosperity first requires awareness before government can start to acknowledge and recognise the nature of the risk. This could be enabled through more rigorous and specific assessments of the impact of lost IP on the national economy in terms of financial costs, jobs and industry competitiveness. Also, national cybersecurity authorities and (counter)intelligence agencies could invest more in efforts to determine the scale and severity of state-sponsored economic cyber-espionage in their territory.

Thus far, only US and European authorities have published such assessments, and even those are already more than five years old. Most emerging economies in Southeast Asia, South Asia and the Middle East and North Africa appear to be increasingly affected, but governments there are yet to acknowledge and recognise the true risk.

The focus of most legislative initiatives is currently geared towards adding strengthened cybersecurity reporting requirements for providers of critical infrastructure and critical information infrastructure. This is critically important, but this report shows that industries that develop and commercialise high-value IP in the form of IP rights, trade secrets and sensitive business information equally require attention from policymakers. Ideally, governments would map those economic sectors and bring those industries or companies into the vault of arrangements for additional government protection in case they happen to be targeted by foreign states.

Finally, members of the G20 and the broader UN membership should continue to raise and address the threat of economic cyber-espionage in relevant forums. Even in situations in which there's no acceptance of state responsibility for acts of cyber espionage, the authorities have a responsibility to 'not knowingly allow their territory to be misused' and to 'not support ICT-enabled theft of intellectual property'. Those are agreed norms of responsible state behaviour in cyberspace and, furthermore, those duties align with existing obligations under the TRIPS agreement to provide minimum standards of IP protection.

In this light, we issued a Briefing Note[66] on 15 November 2022 recommending that the G20 members recognise that state-sponsored ICT-enabled theft of IP remains a key concern for international cooperation and encouraging them to reaffirm their commitment made in 2015 to refrain from economic cyber-espionage for commercial purposes. Further, we suggest that the chair establishes a cross-sectoral working group with the tasks of developing concrete guidance for the operationalisation and implementation of the agreement and of assessing the scale and impact of ICT-enabled theft of IP, while accounting for different geographies and economic sectors.

### Message to the 2022 G20 Leaders' Summit

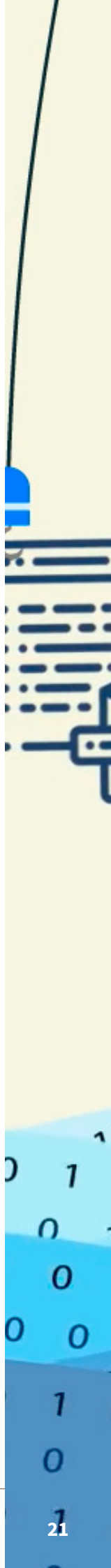
As the leaders of the G20 met in Bali on 15 and 16 November, and in the light of increasing inter-state tensions in the political, military and economic domains, we recommend that the G20 leaders:

a) reaffirm paragraph 26 of their 2015 Leaders' Communique and recognise that state-sponsored ICT-enabled theft of IP remains a key concern for international cooperation

b) place the issue of state-sponsored ICT-enabled espionage of IP for commercial gain on the agenda of a cross-sectoral G20 working group, and task that working group:
   - to develop concrete guidance for the operationalisation and implementation of the agreement
   - to assess the scale and impact of ICT-enabled theft of IP, while accounting for different geographies and economic sectors

c) consider additional intergovernmental and multistakeholder platforms to address issues involving state-sponsored ICT-enabled theft of IP, including the UN First Committee and relevant regional organisations such as the Association of Southeast Asian Nations (and its plus mechanisms), the South Asian Association for Regional Cooperation, the Organization of American States and the African Union

d) maintain a consistent intergovernmental dialogue on the norm against state-sponsored ICT-enabled theft of IP at subsequent G20 forums, including those hosted by the Indian presidency in 2023.



# Notes

1 Ken Dilanian, Courtney Kube, Carol E Lee, Dan De Luce, 'In a break with the past, US is using intel to fight an info war with Russia, even when the intel isn't rock solid', *NBC News*, 6 April 2022, online.

2 Stephen Ezell, Nigel Cory, *The way forward for intellectual property internationally*, Information Technology & Innovation Foundation, 25 April 2019, online.

3 European Patent Office and EU Intellectual Property Office, *IPR-intensive industries and economic performance in the European Union: industry-level analysis report*, 4th edition, October 2022, online. The concept of IP-rights-intensive industries was introduced by the EU. No similar metrics exist yet for, among others, the ASEAN market or India.

4 Interpol, Cybercrime: Covid-19 impact, August 2022, online.

5 Insikt Group, 'Semiconductor companies targeted by ransomware', *Recorded Future*, 29 September 2022, online.

6 Stilgherrian, 'Cyber attacks on Covid-19 vaccine production are not quite a war crime', *ZDNet*, 6 December 2020, online.

7 UN Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security, 'Existing and potential threats', in *Final substantive report*, 10 March 2021, online; UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UNGGE), 'Existing and emerging threats', in *Report*, A/76/135, 2021, online.

8 Nationaal Coördinator Terrorismebestrijding en Veiligheid [National Coordinator for Counterterrorism and Security], *Dreigingsbeeld Statelijke Actoren 2* [*State actors threat assessment 2*], Netherlands Government, November 2022, online.

9 Josh Rogln, 'NSA chief: Cybercrime constitutes the "greatest transfer of wealth in history"', *Foreign Policy*, 9 July 2012, online.

10 Emily Mossburg, J Donald Fancher, John Gelinne, 'The hidden costs of an IP breach: cyber theft and the loss of intellectual property', *Deloitte Review*, issue 19, 2016, online.

11 Commission on the Theft of American Intellectual Property (CTAIP), 'Update to the IP Commission report: The theft of American intellectual property: reassessment of the challenge and US policy', 2017, online.

12 European Commission, *Report on the protection and enforcement of intellectual property rights in third countries*, 27 April 2021, online.

13 G20, 'Leaders' Communiqué', Antalya Summit, 15-16 November 2015, paragraph 26, online.

14 The White House, 'Remarks by President Obama and President Xi of the PRC in joint press conference', 25 September 2015, online.

15 Rowena Mason, 'Xi Jinping state visit: UK and China sign cybersecurity pact', *The Guardian*, 22 October 2015, online; Department of Foreign Affairs and Trade, 'High-level security dialogue with China: joint statement', Australian Government, 24 April 2017, online; 'Canada and China sign no-hacking agreement to protect trade secrets', *CBC*, 26 June 2017, online; Wendy Wu, 'Handshake to end the hacking: China and Germany pledge for peace in cyberspace by 2016', *South China Morning Post*, 9 November 215, online.

16 UN Office of Disarmament Affairs, *International law in the consensus reports of the UN Groups of Government Experts*, background paper, 2020, online.

17 UNGGE, *Report*, A/76/135, paragraph 71(g), online. An 'internationally wrongful act' is an act that constitutes a breach of a state's international obligation and is attributable to a particular state or states under international law. According to the letter of the International Law Commission's articles, internationally wrongful acts don't vary with the gravity of the breach. However, in practice, internationally wrongful acts will concern 'breaches' and typically 'serious breaches' of international obligations that inflict harm on other states and/or jeopardise regional or international peace and security. State responsibility for internationally wrongful acts applies equally during situations of peacetime (non-armed conflict) and armed conflict. See Bart Hogeveen, *The UN norms of responsible state behaviour in cyberspace: guidance on implementation for member states of ASEAN*, ASPI, Canberra, April 2022, 27, online.

18 The TRIPS agreement incorporated specific preceding IP legislation such as the Paris Convention for the Protection of Industrial Property from 1883 and its accompanying series of Acts.

19 Article 10*bis* (1) of the Paris Convention; Christina Parajon Skinner, 'An international law response to economic cyber espionage', *Connecticut Law Review*, 2014, 239, online; Russell Buchan, Inaki Navarrete, 'Cyber espionage and international law', in Nicholas Tsagourias, Russell Buchan (eds), *Research handbook on international law and cyberspace*, 2021, 248–250.

20 Skinner, 'An international law response to economic cyber espionage'.

21 'UK and allies reveal global scale of Chinese cyber espionage', media release, UK Government, 20 December 2018, online.

22 The White House, 'The United States, joined by allies and partners, attributes malicious cyber activity and irresponsible state behavior to the People's Republic of China', 19 July 2021, online.

23 CTAIP, *The IP Commission report: the report of the Commission on the Theft of American Intellectual Property*, Chapter 5, online.

24 Michael R McGurk, Jia W Lu, 'The intersection of patents and trade secrets', *Hastings Science and Technology Law Journal*, 7(2):191.

25 Yukon Huang, Jeremy Smith, 'China's record on intellectual property rights is getting better and better', *Foreign Policy*, 16 October 2019, online. See also *International Property Rights Index 2022*, online.

26 EB Kania, L Laskai, *Myths and realities of China's military–civil fusion strategy*, Center for a New American Security, 28 January 2021, online.

27 See, for instance, Josh Gold, 'A cyberspace FIFA to set rules of the game? UN states disagree at second meeting', *CfR Net Politics*, 2 March 2020, online.

28 For Russia, see, for example, Janne Hakala, Jazlyn Melnychuk, *Russia's strategy in cyberspace*, NATO Strategic Communications Centre of Excellence, June 2021, online; for China, see, for example, 'Experts say China's low-level cyberwar is becoming severe threat', *The Guardian*, September 23, 2021, online; for Iran, see, for example, Congressional Research Service, *Iranian offensive cyber-attack capabilities*, US Congress, January 2020, online.

29 'Statement by the delegation of the Republic of Indonesia on behalf of the Non-Aligned Movement', First Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 9 September 2019, Permanent Mission of the Republic of Indonesia to the UN, New York, online.

30 Clare Duffy, 'Here's what we know so far about the massive Microsoft Exchange hack', *CNN Business*, 10 March 2021, online.

31 Indeed, there are limitations to this methodological approach. State-sponsored cyber intrusions into commercial firms can be for a wide variety of reasons beyond commercial benefit. Some cyber intrusions may be purely for political purposes, for example.

32 Based on reported incidents of state-sponsored operations contained in the Council on Foreign Relations' Cyber Operations Tracker.

33 See, for example, Australian Cyber Security Centre, 'State actors', in *Annual cyber threat report, July 2021 to June 2022*, Australian Government, 4 November 2022, online; National Coordinator for Counterterrorism and Security (NCCS), 'NCTV: Risk of disruption greater due to imbalance between threat and resilience', news release, Netherlands Government, 4 July 2022, online.

34 International Institute for Strategic Studies, 'Conclusion', in *Cyber capabilities and national power: a net assessment*, 171–174, online; Julia Voo, Irfan Hemani, Daniel Cassidy, *National Cyber Power Index 2022*, Belfer Center, September 2022, online.

35 Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan, Jared Stancombe, 'Opportunities for public and private attribution of cyber operations', *Tallinn Papers*, 2021, no. 12, online.

36 Council on Foreign Relations, 'Cyber Operations Tracker', online; European Repository of Cyber Incidents, 'Cyber Incident Dashboard', online; Thai Electronic Transactions Development Agency, *Threat group cards: a threat actor encyclopaedia*, online; Center for Strategic and International Studies, *Significant cyber incidents*, online.

37 See, for example, James Clapper, 'Statement for the record: worldwide threat assessment of the US intelligence community', Senate Armed Services Committee, US Congress, 9 February 2016, online.

38 McAfee, *Economic impact of cybercrime—no slowing down*, Center for Strategic and International Studies, February 2018, online.

39 Everett Rosenfeld, 'Would cybertheft sanctions on China be effective?', *CNBC*, 14 September 2015, online.

40 Mandiant, 'Red line drawn: China recalculates its use of cyber espionage', *Fireeye iSight Intelligence*, June 2016, online.

41 Council on Foreign Relations, 'Cyber Operations Tracker'.

42 Office of the Director of National Intelligence, *Annual threat assessment of the US intelligence community*, US Government, February 2022, online, page 8: 'We assess that China presents the broadest, most active, and persistent cyber espionage threat to US Government and private sector networks. China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.' NCCS, *Cyber security assessment Netherlands 2022*, Netherlands Government, online, page 22: 'States increasingly promote their interests by means of cyber operations, for example for political, economic and military espionage. China is unparalleled in terms of the scale on which and the range within which information is gathered.'

43 Department of Justice (DoJ), 'US charges three Chinese hackers who work at internet security firm for hacking three corporations for commercial advantage', news release, US Government, 27 November 2017, online.

44 'UK and allies reveal global scale of Chinese cyber espionage', media release, UK Government, 20 December 2018, online.

45 DoJ, 'Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax', news release, US Government, 10 February 2020, online.

46 DoJ, 'Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax'.

47 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', news release, UK Government, 19 July 2021, online.

48 For this section, we looked at the data entries form the CfR Cyber Operations Tracker that are categorised "private sector", "government & private sector", "government, military, private sector" and "civil society, government and private sector".

49 'Significant cyber incidents', Center for Strategic and International Studies, online; *Threat group cards: a threat actor encyclopedia*, Electronic Transactions Development Agency, online.

50 'Pharma data theft ion the rise: protecting your data in the digital age', *LabForward*, Thought Leadership: Information Security, June 2022, online.

51 Assessment of Cyber-enabled Information Theft by APTs targeting Southeast Asia, conducted privately by the MITRE Corporation for ASPI.

52 Mandiant, *APT41, a dual espionage and cyber crime operation*, February 2022, online; 'Hack the real box: APT41's new subgroup Earth Longzhi', *TrendMicro*, 9 November 2022, online; Cybersecurity and Infrastructure Security Agency, 'Alert AA21-200B: Chinese state-sponsored cyber operations: observed TTPs', US Government, 19 July 2021, online. Kaspersky defines a *bootkit* as 'a malicious program designed to load as early as possible in the boot process, in order to control all stages of the operating system start up, modifying system code and drivers before anti-virus and other security components are loaded', online.

53 'Operation CuckooBees: Cybereason uncovers massive Chinese intellectual property operation', *Cybereason*, 4 May 2022, online.

54 Nicole Sganga, 'Chinese hackers took trillions in intellectual property from about 30 multinational companies', *CBS News*, 4 May 2022, online.

55 'Operation CuckooBees: Cybereason uncovers massive Chinese intellectual property operation'.

56 Mandiant, 'AP41, a dual espionage and cyber crime operation', 2022, online.

57 Coco Feng, 'China has named nearly 9,000 "little giants" in push to preference home-gown technologies from smaller companies', *South China Morning Post*, 9 September 2022, online.

58 See Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, Elise Thomas, *Mapping China's tech giants*, ASPI, Canberra, 18 April 2019, online; Meia Nouwens, Helena Legarda, *China's pursuit of advanced dual-use technologies*, International Institute of Strategic Studies, 18 December 2018, online; HR McMaster, 'How China sees the world. And how we should see China', *The Atlantic*, May 2020, online.

59 Ellen Nakashima, 'US said to be target of massive cyber-espionage campaign', *Washington Post*, 10 February 2013, online; Darren E Tromblay, Robert G Spelbrink, *Securing US innovation: the challenge of preserving a competitive advantage in the creation of knowledge*, Rowman & Littlefield, Lanham, Maryland, 2016, 65–99; Hedieh Nasheri, *Economic espionage and industrial spying*, Cambridge University Press, Cambridge, 2004; Adam Rawnsley, 'Espionage? Moi?', *Foreign Policy*, 2 July 2013, online. Philip Ewing, 'Gates: French cyber spies target US', Politico, 22 May 2014, online.

60 Nick Carr, 'Cyber espionage is alive and well: APT32 and the threat to global corporations', *Mandiant Threat Research*, 14 May 2017, online.

61 PwC, *The scale and impact of industrial espionage and theft of trade secrets through cyber*, Directorate General Internal Market, Industry, Entrepreneurship and SMEs, European Commission, December 2018, online.

62 See Federal Bureau of Investigation, 'The China threat', US Government, no date, online; Algemene Inlichtingen en Veiligheidsdienst [General Intelligence and Security Service], 'Cyberaanvallen door statelijke actoren—zeven momenten om een aanval te stoppen' [Cyber attacks by states—seven opportunities to stop an attack], Netherlands Government, 28 June 2021, online; 'Japan police educating firms on foreign spy tactics to protect themselves from data theft', *The Mainichi*, 25 December 2015.

63 Ken Dilanian, Courtney Kube, Carol E Lee, Dan De Luce, 'In a break with the past, US is using intel to fight an info war with Russia, even when the intel isn't rock solid', *NBC News*, 6 April 2022, online.

64 National Cyber Security Centre, 'Meer mogelijkheden NCSC om dreigings en incidentinformatie te delen' [More opportunities for NCSC to share threat and incident information], Netherlands Government, 1 December 2022, online.

65 Ian Levy, 'So long and thanks for all the bits', UK National Cyber Security Centre, 27 October 2022, online.

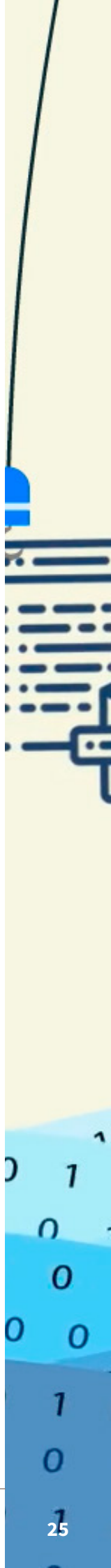
66 Gatra Priyandita, Bart Hogeveen, Ben Stevens, 'State-sponsored economic cyberespionage and the risk to nations' prosperity: Briefing Note to the G20 Leaders's Summit', ASPI, Canberra, 15 November 2022, online.

# Figure 1 references


July 2011: US DoD Strategy for Operating in Cyberspace, online.
July 2012: 'Greatest transfer of wealth in history', online.
May 2013: Pentagon's Annual Report to Congress, online.
January 2014: Presidential Directive: refrain from collecting trade secrets, online.
May 2014: US DoJ: indictment of PLA officers, online.
August 2015: UN member states endorse 11 norms of responsible state behaviour, online.
September 2015: US and China agree not to engage in economic cyber-espionage, online.
October 2015: UK and China agree not to engage in economic cyber-espionage, online.
November 2015: G20 Leaders agree not to support economic cyber-espionage, online.
May 2016: G7 leaders embrace G20 commitment, online.
June 2016: Germany and China agree not to engage in economic cyber-espionage, online.
April 2017: G7 foreign ministers commit not to engage in economic cyber-espionage, online.
April 2017: Australia and China agree not to engage in economic cyber-espionage, online.
June 2017: Canada and China agree not to engage in economic cyber-espionage, online.
July 2017: Germany: China, Russia and Iran conduct economic espionage, online.
December 2018: US, UK and others attribute a cyber-espionage campaign, online.
July 2021: Eight states, NATO and EU attribute a cyber-espionage campaign, online.
July 2022: FBI and MI6 warn industry of cyber-espionage risks, online.


# Acronyms and abbreviations

| | |
|---|---|
| APT | advanced persistent threat |
| CERT | computer emergency response team |
| IP | intellectual property |
| MSP | managed service provider |
| MSS | Ministry of State Security |
| PLA | People's Liberation Army |
| PRC | People's Republic of China |
| TTP | tactics, techniques and procedures |
| WTO | World Trade Organization |



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE