ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

State-sponsored economic cyberespionage and the risk to nations' prosperity

Briefing Note to G20 Leaders' Summit

Dr Gatra Priyandita, Bart Hogeveen and Dr Ben Stevens

What's the issue?

In 2015, the leaders of the G20, as the premier forum for international economic cooperation, recognised the risks that state-sponsored economic cyberespionage for commercial purposes posed to the long-term economic growth of nations and their prosperity.

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.*'

In conditions of deteriorating amity between major powers, the survival of international rules, norms and principles comes under additional pressure. Strategic competition spills into the economic and technological domains. With that, the risk of economic cyberespionage to nations' prosperity can be expected to grow disproportionally.

What's the current state of play?

State-sponsored forms of economic cyberespionage are increasingly *becoming a global problem*.[1] In developing and emerging economies, commercial firms and universities are targeted as hackers seek trade secrets and opportunities to *exploit cybersecurity weaknesses along transnational supply chains*. While publicly available reports by cybersecurity firms indicate that commercial firms and universities in advanced economies remain the largest targets for theft of intellectual property (IP), there's likely to be a bias in current reporting due to *a culture of underreporting* by industry and governments in most developing economies.

There's reason to assume that *the severity of individual cases has been increasing* over the past few years. For example, in May 2022, it was reported that a single campaign of economic cyberespionage by an advanced persistent threat group[2] named Winnti was responsible for the theft of IP possibly worth trillions of US dollars from 30 multinational corporations based in North America, Europe and East Asia.[3] In direct financial terms, authorities estimated in 2018 that *the cost of IP theft to their economies was between tens and hundreds of billions annually.*[4]

States known to pursue a combination of *assertive industrial development* strategies and *the use of (offensive) cyber capabilities* (including through proxy actors) are on the watchlist for general infringements of IP rights.[5] This applies to some G20 member states.

In the years since 2015, *different interpretations of the remit of the Agreement by the G20 Leaders on Cyber-enabled theft of IP* have surfaced. States differ in their focus on either discrete protective classifications (such as patents, trademarks and registered designs) or non-descript and non-patented forms of valuable commercial information (such as sensitive business information and trade secrets).

15 November 2022

In addition, an increasing number of states portray accelerated economic development in digital transformation and Industry 4.0 as a core national security issue. All this is further compounded by the fact that several G20 states *deny possession or sponsorship of cyber capabilities* that could be leveraged for economic cyberespionage (and theft of IP for commercial gain), while other states are reluctant to accept the risk of economic cyberespionage due to overall *shortcomings in their national cybersecurity resilience*.[6]

Message to the 2022 G20 Leaders' Summit

As the leaders of the G20 meet 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.

This Briefing Note accompanies a more extended Policy Brief that ASPI will present when India takes over next year's presidency of the G20.

This publication is part of a capacity-building project titled 'Strengthening national resilience against the risk of cyber-enabled theft of intellectual property' funded by the US State Department's Bureau of Cyberspace Policy.

This publication is an independent assessment by ASPI, and the authors are responsible for any mistakes. By no means does anything contained in this publication represent the position or opinion of the US Government or any other government.

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

Notes

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

2 Advanced persistent threat groups are organised hacking groups that are distinguished by their ability to sustain unauthorised access into computer networks for an extended period. Due to the extensive resources necessary to sustain such costly processes, such groups are often sponsored or supported by state (cyber)security agencies.

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

4 Commission on the Theft of American Intellectual Property, *Update to the IP Commission report*, National Bureau of Asian Research, 2017, online; European Commission, *The scale and impact of industrial espionage and theft of trade secrets through cyber*, Report by PwC, 2018 online.

5 See, for instance, European Commission, *Report on the protection and enforcement of intellectual property rights in third countries*, 27 April 2021, online; Office of the US Trade Representative, *2022 Special 301 Report*, 27 April 2022, online.

6 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.