



Task Force 2
Our Common Digital Future: Affordable, Accessible
and Inclusive Digital Public Infrastructure



COMBATTING THE THREAT OF CYBER- ENABLED IP THEFT

June 2023

Gatra Priyandita, Analyst, Australian Strategic Policy Institute

Teesta Prakash, Analyst, Australian Strategic Policy Institute


Bart Hogeveen, Head of Program: Capacity Building and International Norms in
Cyberspace, Australian Strategic Policy Institute

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE



Abstract




A common digital future should include a safe and prosperous cyber ecosystem wherein nations can pursue their digital development as well as economic and innovation fairly and competitively. This is threatened by a growing practice among criminals and states to misappropriate and steal intellectual property from other jurisdictions. Since 2015, there has been an agreed normative understanding that states must refrain from cyber-enabled theft of intellectual property. In Antalya, Türkiye, the G20 leaders considered cyber-enabled theft to be detrimental to national security and recognised how it would undermine global digital infrastructure and the economic competitiveness of nations. However, this commitment

is yet to translate into broader policy action among the G20 states; state-sponsored economic cyber-espionage activities for commercial gain have quadrupled between 2015 and 2022. Limited understanding of the damage posed by cyber-enabled IP theft to national economies impedes international cooperation and efforts to raise political priority. Furthermore, domestic and regional industries that develop and commercialise high-value IP in the form of IP rights, trade secrets, and sensitive business information require the attention of policymakers. This Policy Brief proposes that the G20 member states should build the capacity of individual states to detect, prevent, and respond to sophisticated cyber intrusions.



The Challenge



1



A digital revolution is underway in the developing world. Countries are increasingly focusing on digitising everyday services such as healthcare and public service delivery as well as their associated knowledge economy. Globally, countries are banking on the transformative powers of digital technology as a means to ensure economic growth and competitiveness and bolster prosperity. Consequently, the G20 has placed impediments to digital economy high on the agenda; the Indian chairmanship has made the governance of digital technology a centrepiece of its G20 presidency in 2023.¹

The ability to produce and protect intellectual property (IP), such as patents and trademarked goods, is foundational to a modern economy. However, this is increasingly becoming a challenge in the current digital world. One distinct factor for this is criminal syndicates which, alongside state actors, are engaged in efforts to collect commercially valuable assets (such as trade secrets and sensitive business information, i.e., intellectual property) through targeted compromises of digital systems and communication channels.

This threat of economic cyber-espionage is being faced by both developed and emerging economies, as well as by both cyber-mature and weak cybersecure nations. Governments carry the responsibility to ensure a safe cyber ecosystem. This starts by taking these forms of criminal and state-sponsored cyber intrusions seriously and by putting in place appropriate preventive responses and remediations.

The leaders of the G20 member states, as the premier forum for international economic cooperation, have recognised the need for global action. In 2015, the G20 leaders made a commitment 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.”² This agreement followed a shared understanding between the US and China in September 2015 that the two countries would not conduct or support cyber-enabled theft of IP, including trade secrets and sensitive business information, for commercial gains.³

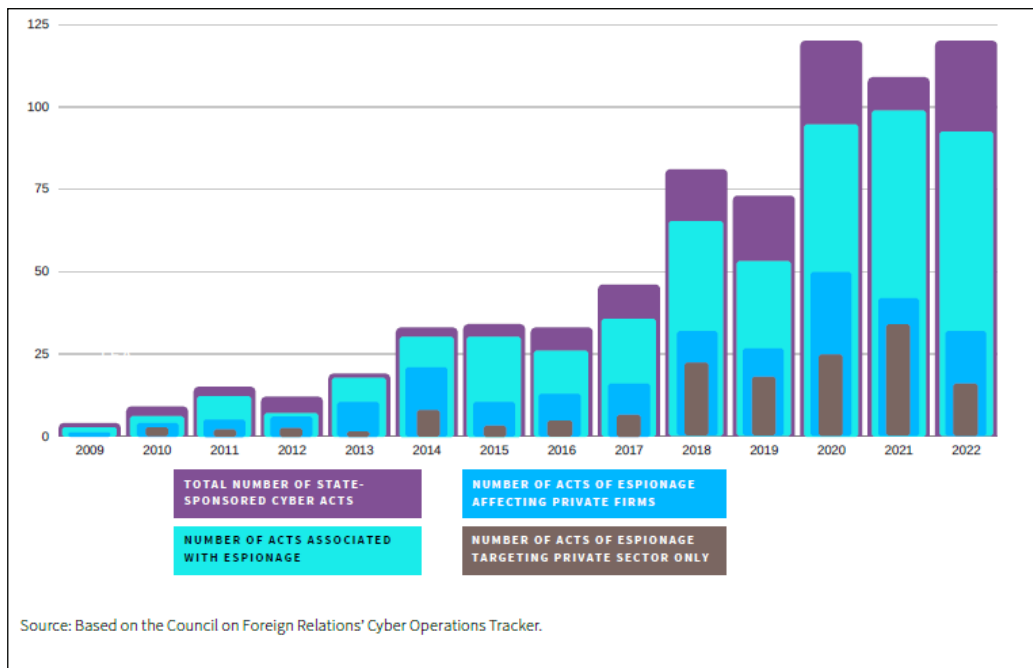
These shared commitments formed the basis for an agreed international norm where states refrain from misusing the cyber domain to steal IP with the aim of providing unfair benefits to local industries or companies.⁴

Despite these agreements, the practice of economic cyber-espionage has continued to develop rapidly across the globe. Table 1 shows the number of state-sponsored cyber intrusions against private entities.⁵ Out of more than 300 cases that the Council of Foreign Relations (CFR) has recorded

since 2009, 229 have taken place since 2016. Of these, 40 took place between 2014 and 2016, and more than 100 have taken place since 2020.

It is possible that the real numbers are much higher, as we only know of possible cases of cyber intrusions after they have occurred and been reported. State-sponsored cyber-espionage is undeniably an integral part of this operational picture, accounting for more than 80 percent of all reported state-sponsored cyber incidents.⁶

Table 1: Reported Incidents of State-Sponsored Cyber Operations Between 2009 and 2022





Government agencies and the military remain the biggest targets of these cyber-espionage operations, but there has also been an uptick in the number of cyber intrusions carried out by hacking groups that affect commercial firms and universities.⁷ From 2010 onwards, cyber-espionage campaigns specifically targeting private-sector entities have grown to constitute a considerable share of all known acts of cyber-espionage. Roughly 20-30 percent of all cyber-espionage operations since 2020 have targeted commercial firms or universities.⁸

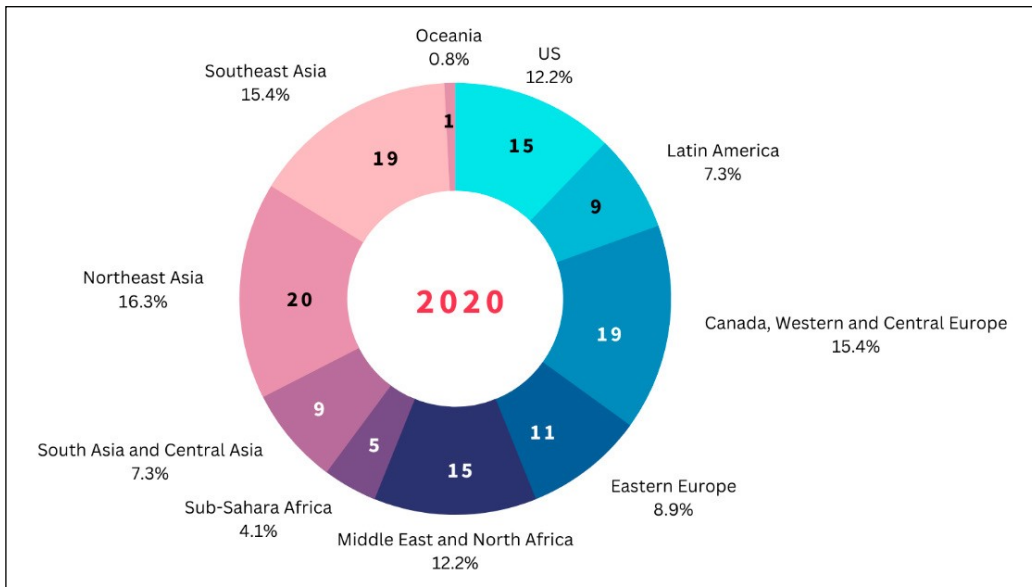
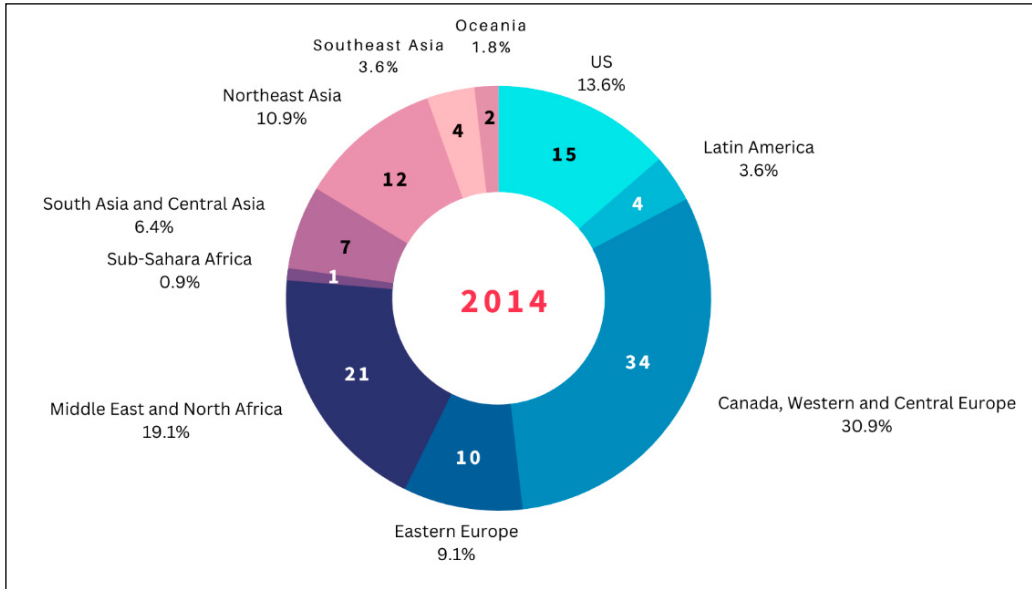
Moreover, while advanced economies continue to be the biggest targets of state-sponsored cyber-espionage operations, developing economies are also emerging as larger targets. Table 2 shows the regional distribution of private entities affected and targeted by APTs. For example, South East Asian economies constituted only 3.6 percent of the targets of all reported cases of state-sponsored cyber operations in 2014. By 2020, their share grew to 15.4 percent. Meanwhile, South Asian economies constitute roughly 6-7 percent of overall cases from 2014 until 2020.⁹

Countries are already struggling to establish a level of cybersecurity

resilience to bounce back from 'regularised' forms of cybercrimes. They struggle even more in dealing with sophisticated cybersecurity threats actors that rely on support from state actors. On the one hand, this poses a threat to national independence and economic security. Even more significantly, if this phenomenon remains unaddressed, it would undermine global trust and confidence in a safe and secure digital environment, thus affecting governments, industries, research, development and innovation, and human security.

While there has been considerable examination into the costs of cyber-attacks, the medium- to long-term economic consequences of unsafe cyberspace have not been explored fully, including the scale of the damage on the prosperity of nations. For the EU and US economies alone, conservative estimates point to an annual direct economic loss of US\$60-200 billion.¹⁰ The undermining effect can be expected to be even more serious in emerging economies. The theft of IP developed and acquired locally uproots the foundations of innovation, competitiveness, and employment, thus compromising a nation's prospects for prosperity.

Table 2: Private Entities (Including Commercial Firms and Universities) Affected and Targeted by APTs, by Region, in 2014 and 2020



Note: Numbers in the pie chart reflect the number of recorded incidents affecting firms in these regions.

Source: Gatra Priyandita, Bart Hogeveen, and Ben Stevens, "State-Sponsored Economic Cyber-Espionage for Commercial Purposes," ASPI, December 16, 2022, <https://www.aspi.org.au/report/state-sponsored-economic-cyberespionage>



In the current strategic environment, which is marked by growing tech bifurcation, strategic competition, and growing distrust, more states are inclined to employ cyber tools to pursue economic and strategic goals. The cyber domain is therefore likely to be misused even more, and campaigns

targeting the economic crown jewels of other nations will ramp up. The G20 member states, including emerging economies, must address this, since their economies are so interconnected that disruptions in the confidentiality, integrity, and availability of global value chains will affect all.



The G20's Role

2





With the growing ubiquity of digital technology, economic espionage is emerging as a serious global problem. In response to this threat, leaders of the G20, at the 2015 G20 summit in Antalya, Türkiye, agreed that no state should engage in or support the practice of cyber-enabled intellectual property crime.¹¹ In fact, this practice emerged as an accepted norm of responsible state behaviour in cyberspace.

Eight years on, and in a dramatically changed global environment for interstate cooperation, there is a need to adopt a three-pronged approach to address the issue of economic cyber-espionage at the global, national, and regional levels.

First, there is an urgent need for the G20 member states to strengthen cybersecurity resilience and address the risk of countries falling victim to economic cyber-espionage since major power competition is increasingly spilling into economic and technological domains.¹² The G20 has the power to drive systemic change in the global system. A first step would be to foster collaboration to enhance the cyber diplomacy toolkit of countries which

are currently quite weak in stopping unacceptable forms of cyber operations.

Beyond the G20, governments can also move to utilise existing international forums to engage on the topic, including the UN First Committee on Disarmament and International Security and mechanisms related to the enforcement of the TRIPS Agreement on minimum standards for IP protection. It is vital that members of these forums break down the silos between them and collectively address state-supported and tolerated malicious cybersecurity activities.

When collaborating internationally, a foundational step for governments would be to acknowledge the issues, improve overall visibility, and clarify mutual expectations of responsible behaviour in states' use of cyber tools.

Second, there is a need for stronger engagements by and through regional organisations, for example, through arrangements such as ASEAN, APEC, AUC, and OAS. ASEAN and OAS have already made headway with efforts such as the implementation of the UN norms of responsible state behaviour and fostering confidence-building measures on cyber issues.



Member countries should invest more in this as part of their UN- and G20-level commitments. This would also open up opportunities for regionally sourced and resourced investments in cyber capacity building and institutionalised forms of threat information-sharing. Regional networks of recognised CERTs are an important platform, such as APCERT in the Asia Pacific, as well as nascent inter-state cybersecurity initiatives such as ASEAN Defence Ministers' network of cyber-operations centres.

Additionally, regional organisations have an opportunity to leverage their convening power and get the IT industry and R&D sectors around the (same) table. At the regional level, a comprehensive approach to cyber, national, and economic security has the highest chance of success and impact.

Third, national governments must individually work towards building awareness and capacity to respond to the threat of economic espionage. As a first step, this will involve assessing the extent of the risk of malicious cyber

activities targeting the government, critical (information) infrastructure, and competitive assets of national economies. The latter requires governments to identify what sectors of their economy are most likely to be vulnerable to cyber-enabled theft of IP. This may involve 'softer' industries such as start-ups, academia, and other research, development, and innovation hubs. They may maintain less hardened security perimeters, since they are 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 essential assets of future economic growth is a first step to assess their exposure to foreign intelligence agencies and to monitor specific cybersecurity threats. Such a whole-of-government effort involves government agencies responsible for economic policy and digital transformation, national and cybersecurity, and national IP authorities.



Recommendations to the G20



3



The functionalities within a national cybersecurity centre constitute an essential government capability. Along with non-commercial and private cybersecurity service providers, such entities are at the face of identification, protection, detection, response, and recovery of stolen IP data. Every country is expected to be able to perform these functions, albeit to different degrees of maturity.


The G20 provides a platform for countries to coordinate according to cybersecurity maturity levels, particularly where these impact economic development, free trade and commerce, and issues such as secure transboundary data flows.

The threat of economic cyber-espionage is real and persistent, and its invisible but undermining nature affects the long-term prosperity of nations. With India as well as other economies in the Global South moving towards greater digitalisation in the context of geo-economic competition, there is a need to take the joint issues of economic, knowledge, and digital security seriously. The 2015 G20 commitment to refrain from cyber-enabled IP theft provides the capstone to this effort and needs to be implemented.

The G20 program of action on cybersecurity issues affecting economic security

In the light of increasing inter-state tensions in the political, military, and economic domains, we make the following recommendations to the G20 leaders:¹³

- a. Reaffirm paragraph 26 of the 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:
 - with developing concrete guidance for the operationalisation and implementation of the agreement, and
 - with assessing the scale and impact of ICT-enabled theft of IP while accounting for different geographies and economic sectors.
- c. consider additional intergovernmental and multistakeholder plat-



forms to address issues involving state-sponsored ICT-enabled theft of IP, including the UN First Committee and relevant regional organisations such as the ASEAN (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.

Attribution: Gatra Priyandita et al., “Combatting the Threat of Cyber-Enabled IP Theft,” *T20 Policy Brief*, June 2023.

Endnotes

- 1 Indian Ministry of Electronics & IT, “The First Digital Economy Working Group (DEWG) Meeting under India’s G20 Presidency to Kick Start Tomorrow in Lucknow,” *Press Information Bureau*, February 12, 2023, <https://pib.gov.in/PressReleasePage.aspx?PRID=1898556>.
- 2 G20 Information Centre, “G20 Leaders’ Communiqué,” University of Toronto, accessed April 7, 2023, <http://www.g20.utoronto.ca/2015/151116-communication.html>.
- 3 Barack Obama and Xi Jinping, “Remarks by President Obama and President Xi of the People’s Republic of China in Joint Press Conference,” The White House: President Barack Obama Archives, September 25, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>.
- 4 Gatra Priyandita, Bart Hogeveen, and Ben Stevens, “State-Sponsored Economic Cyber-Espionage for Commercial Purposes: Tackling an Invisible but Persistent Risk to Prosperity,” Australian Strategic Policy Institute, *Policy Brief Report No. 67/2022*, December 2022, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-12/State-sponsored%20economic%20cyber-espionage_0.pdf?VersionId=L0VXw3il0y4lQv4PcMLT07.a7yZzdJNs.
- 5 “Cyber Operations Tracker,” Council of Foreign Relations, accessed May 5, 2023, <https://www.cfr.org/cyber-operations/>
- 6 “Cyber Operations Tracker”
- 7 “Cyber Operations Tracker”
- 8 “Cyber Operations Tracker”
- 9 “Cyber Operations Tracker”
- 10 European Commission, “Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries,” April 27, 2021.
- 11 G20, “Leaders’ Communiqué,” Antalya Summit, accessed on June 2, 2023, <https://www.oecd.org/g20/summits/antalya/G20-Antalya-Leaders-Summit-Communiqu%C3%A9.pdf>.
- 12 Jamie Gaida et al., “ASPI’s Critical Technology Tracker: The Global Race for Future Power,” Australian Strategic Policy Institute, March 2, 2023, <https://www.aspi.org.au/report/critical-technology-tracker>

- 13 These recommendations were also provided by ASPI to the G20 leaders in 2022. See Priyandita, Hogeveen, and Stevens, “State-Sponsored Economic Cyber-Espionage for Commercial Purposes,” 21.



वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE