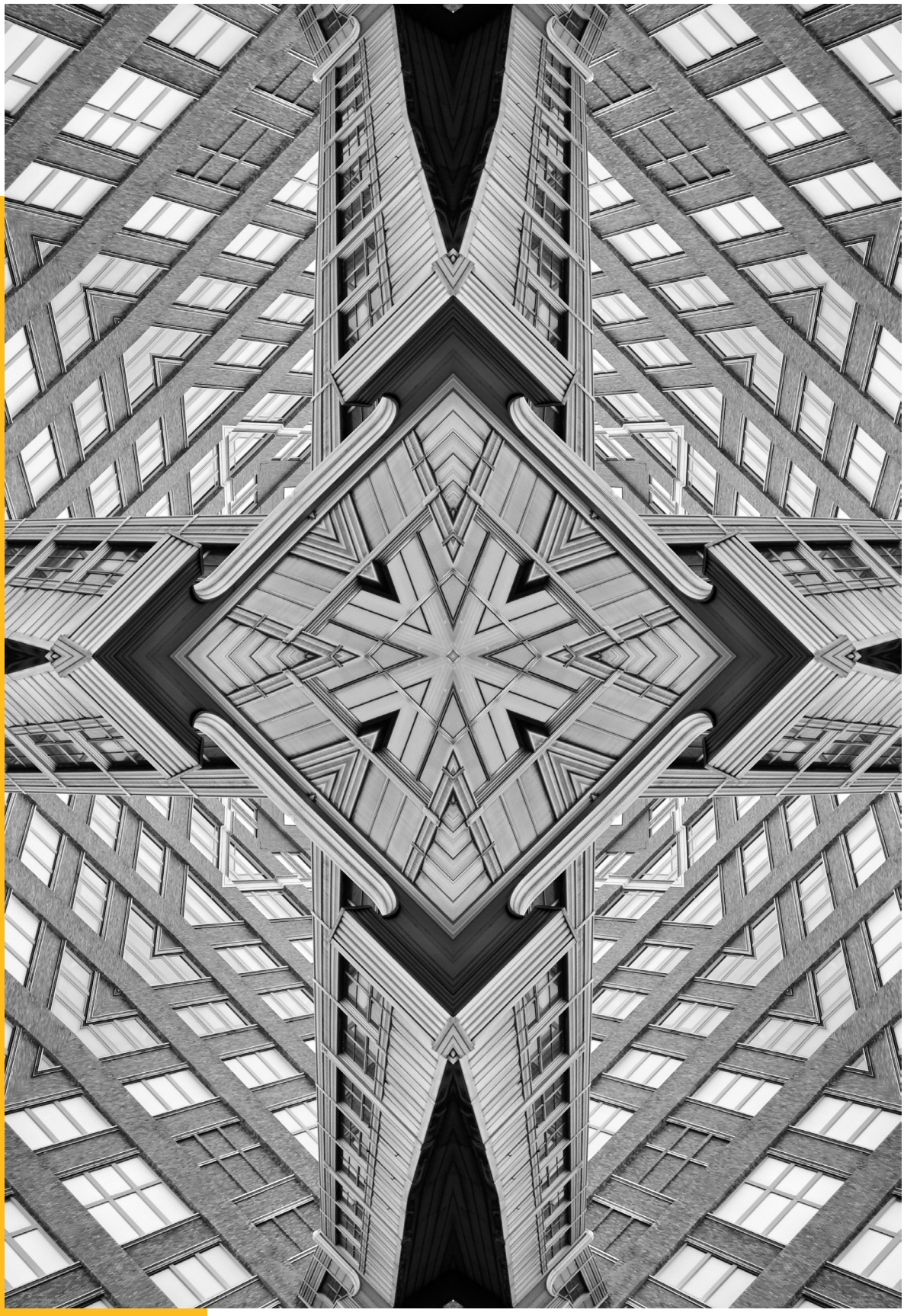
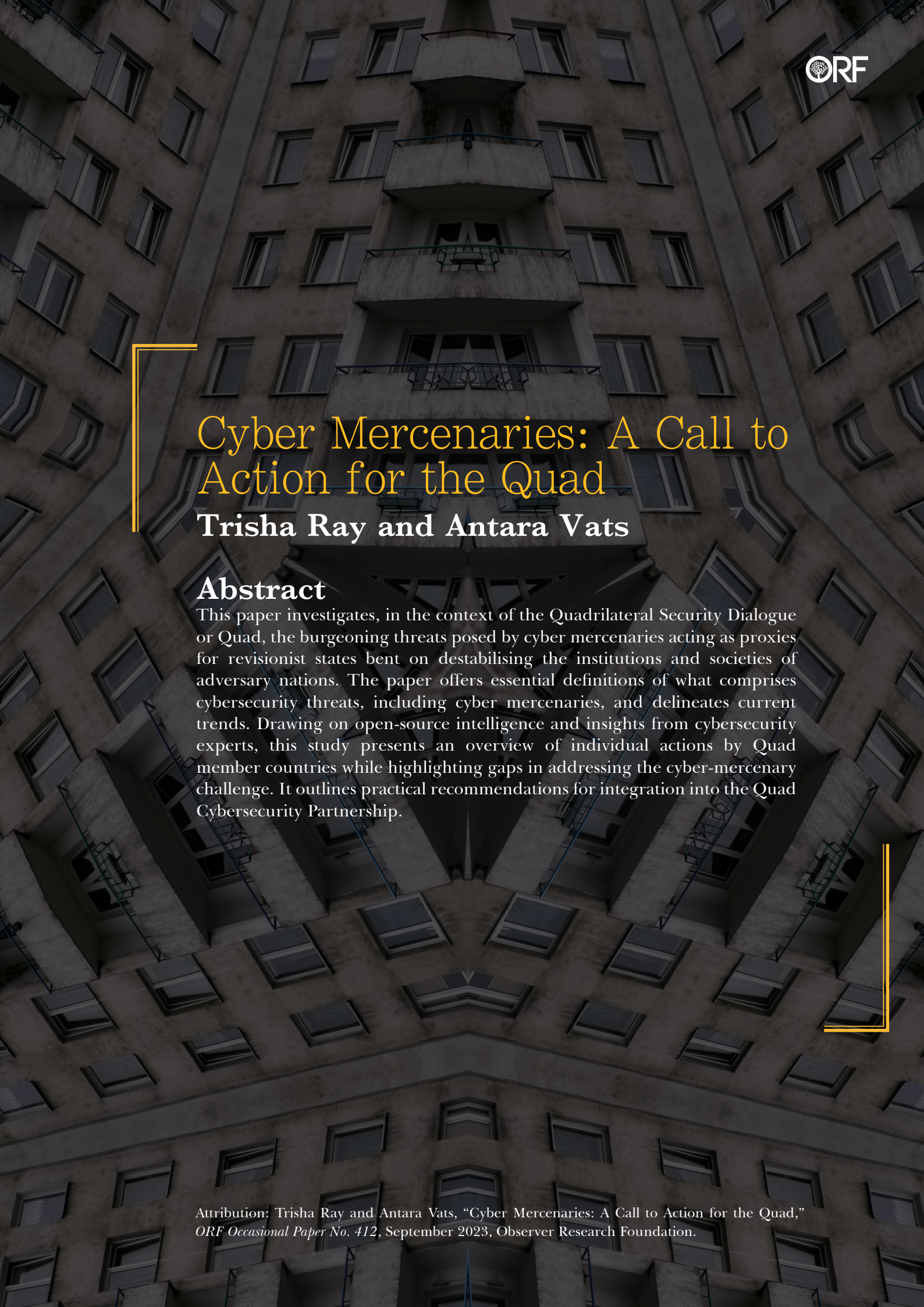
OBSERVER RESEARCH FOUNDATION

Occasional Paper



ISSUE NO. 412 SEPTEMBER 2023



Cyber Mercenaries: A Call to Action for the Quad

Trisha Ray and Antara Vats

Abstract

This paper investigates, in the context of the Quadrilateral Security Dialogue or Quad, the burgeoning threats posed by cyber mercenaries acting as proxies for revisionist states bent on destabilising the institutions and societies of adversary nations. The paper offers essential definitions of what comprises cybersecurity threats, including cyber mercenaries, and delineates current trends. Drawing on open-source intelligence and insights from cybersecurity experts, this study presents an overview of individual actions by Quad member countries while highlighting gaps in addressing the cyber-mercenary challenge. It outlines practical recommendations for integration into the Quad Cybersecurity Partnership.

Attribution: Trisha Ray and Antara Vats, "Cyber Mercenaries: A Call to Action for the Quad," *ORF Occasional Paper No. 412*, September 2023, Observer Research Foundation.

Introduction

Events like the Russia-Ukraine war, disruptions during the COVID-19 pandemic, and the US-China trade war have collectively demonstrated the fragile nature of the interconnected world that we live in today. The conflict in Europe, in particular, has caused massive disruptions in supply chains that have had a telling impact on the world economy. Against the backdrop of these disruptions, even as digital connectivity and distributed supply chains have helped nations adapt, and even prosper, they are now increasingly being viewed by governments as vulnerabilities that must be managed.[1]

Specific mention needs to be made of the Asia-Pacific region, which witnessed a 168-percent increase in cyberattacks in 2021 compared to the previous year. The number of incidents further increased, by 22 percent, in 2022. Of the region's countries, Australia, India and Japan bore the brunt of such attacks. In most of the incidents, malicious actors had targeted utilities, Internet Service Providers (ISPs), healthcare providers, and financial services. There has also been a rise in attacks on educational and research institutions.[2]

Two meta-trends are building at the same time and compounding one another. The first is the growing attack surface for the cyber criminals, primarily because individuals, businesses and governments are online for far longer periods of time, carrying out a host of activities, than they were before the pandemic. The second is the proliferation of malicious actors, especially those that are state-sponsored. In 2020, the SolarWinds hack left multiple agencies of the United States Government scrambling to respond to a series of data breaches.[3] In 2021, the Unique Identification Authority of India (UIDAI), the body in-charge of the country's national biometric ID Aadhaar, was one of many entities targeted by a Chinese state-sponsored group, dubbed TAG-28.[4] In November 2022, 20 websites of the Japanese Government came under DDoS attacks by pro-Russian hacker group, Killnet.[5]

These examples provide a glimpse into the present-day threat landscape in cyberspace. An increasing number of attacks are related to geopolitical conflicts and there is a sizeable risk that no matter how secure one's

Introduction

systems are, there are acute vulnerabilities that can arise if a single point in a software service supply chain falls prey to a cyberattack. This is a massive challenge, given how organisations and governments rely on a variety of vendors for services like payroll, pensions, and healthcare.

Cybercrime-as-a-Service (CaaS) has, according to multiple threat intelligence research groups, witnessed a meteoric rise.[6] For instance, in the past decade, there has been a rise in "hack-for-hire" firms, based in NATO countries, as well as in others like the UAE, Israel, China, and India, operating with varying levels of sophistication.[7] These firms are hired by a global clientele, which includes governments and the private sector, to target financial services, consulting, healthcare corporations, legal firms, as well as individuals involved in civil disputes.[8] To be sure, such threat actors are not new, and some have been operating since the early 2000s. What is novel about the present-day threat actors is the growth in the number of *cyber mercenaries*—a class of private groups that may or may not be linked to specific states and often appear to be engaged by multiple clients, government and non-government alike. A 2021 UN Human Rights report noted that cyberspace has emerged as a key geostrategic space for both state and non-state actors, who increasingly employ proxies in ways that are detrimental to human rights.[9]

This is true for the countries of the Quadrilateral Security Dialogue or Quad—India, Japan, Australia, and the United States. These countries have been at the receiving end of cyberattacks, with governments, critical industries, essential services and research institutions frequently being targeted. As the Quad has identified cybersecurity as a core interest, the grouping must prioritise arresting this thriving marketplace of cyber mercenaries that serve as proxies for revisionist states seeking to disrupt and undermine institutions of adversary nations.[10]

This paper delves into the rise of cyber mercenaries, describes key definitions, and outlines current trends. Leveraging open-source information, as well as interviews with cybersecurity experts, this paper provides an overview of what each member country in the Quad is doing individually and also makes mention of the gaps in addressing the challenges posed by cyber mercenaries. It identifies plausible recommendations that could be incorporated into the Quad Cybersecurity Partnership.

Setting Key Definitions

The employment of mercenaries by states finds its roots in antiquity. During the Middle Ages in Europe, mercenary groups would be hired by city-states to fight wars, maintain public order, and collect taxes.[11] Similarly, for 300 years starting in the 16th century, European mercenaries were engaged by the courts of rulers from the Malabar coast and the Deccan Sultanates to Rajasthan.[12] In contemporary wars, private security contractors like the US's Blackwater, Australia's Unity Resources Group, and Russia's Wagner Group, fulfil a range of functions in conflict zones, including armed combat, guarding key facilities and providing personal security. Most recently, the Wagner Group carried out so-called "false flag" attacks, laying the groundwork for Russia's invasion of Ukraine in early 2022.[13]

In 2018, Tim Maurer, senior fellow in Carnegie's Technology and International Affairs programme, defined a cyber mercenary or cyber proxy as "an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect."[14] Maurer groups proxies into three categories:

a. Delegation: The principal delegates its "authority to an agent to act on its behalf."

b. Orchestration: "Enlistment of intermediary actors on a voluntary basis, by providing them with ideational and material support, and using them to address target actors in pursuit of political goals."

c. Sanctioning: State passively supports a non-state actor by knowingly choosing "to tolerate the actor's activities in spite of having the capacity to do otherwise."

In 2021, the Working Group on Mercenaries under the United Nations Human Rights Council (UNHRC) built upon its definition of mercenaries as "corporate entities providing, on a compensatory basis, military and/or security services by physical persons and/or legal entities" and added that

Setting Key Definitions

activities in cyberspace can "rise to the level of mercenarism".[15] It noted, crucially, that such entities are not the only source of cyber mercenary activities, and that each possible case must be assessed individually.

In the early 2010s, the use of cyber mercenaries was closely identified with rogue states or smaller states with less resources.[16] In the last decade, private tech services companies, primarily based in the US, have been increasingly using the term "cyber mercenaries" to identify the challenges associated with deliberate state-enabled cyber operations. Pukhraj Singh, a cyber operations analyst currently based in Australia interviewed for this paper, notes that the Snowden revelations in 2013 lent an air of legitimacy to state-backed cyber operations and contributed to the proliferation of mercenary groups in the decade since.[17] Terms like 'hacktivists', 'advanced persistent threats' (APTs) and 'cyber mercenaries' are often used interchangeably, yet do need to be differentiated from each other. Hacktivists are generally loosely organised collectives held together by a common ideology or loyalty, who undertake coordinated cyber operations without a specific entity hiring them. APT groups are those that establish an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organisation.

The Challenge

Not all cyber mercenaries are 'noisy'. For many state-sponsored actors, the main aim is to collect information. As a result, they may lie undetected in a system for months, if not years, before they are either detected, or they mobilise and carry out a disruptive cyberattack.[18] Cyber mercenaries may also carry out Intellectual Property (IP) theft, or seek to gather sensitive information on behalf of state clients ahead of key negotiations or in relation to geopolitical conflicts.[19] The Internet is also a trove of information on key individuals working in organisations, which is used for social engineering that lays the groundwork for certain surveillance functions. Spyware entities at the first stage of surveillance chain, for instance, silently profile targets using fake profiles on social media platforms, making it both easy to recruit their services and difficult to identify the ultimate beneficiaries of spyware services.[20]

Nowadays, larger states also employ such companies or groups, making it all the more challenging to build consensus within international rulemaking bodies to restrict these entities in any meaningful way. The 2021 UNHRC report notes that the rise in outsourcing of cyber operations "correlates in some States with a reduction in defence budgets and the more general trend towards involving the private sector in the provision of public services." Additionally, outsourcing also helps states to cut costs and thwart attribution.

The term does not have wide usage outside of the US, where similar synonymous jargon including 'cyber proxies', 'hack-for-hire' or 'APTs' have more purchase. Nevertheless, this paper is of the view that 'cyber mercenaries' as a term captures the linkages—albeit, at times nebulous—of such groups with the State, the range of functions they fulfil, as well as the varying levels of sophistication with which they operate.

The Quad Response

The Quad members are among those who have borne and continue to bear the brunt of cyberattacks globally.[21] In May 2022, the Quad agreed on a set of joint principles to animate the Quad Cybersecurity Partnership (CSP): "The interconnected and interdependent nature of critical infrastructure, without proper cyber security safeguards increases that risk and can deliberately or inadvertently cause disruption and subsequent economic and security concerns within and across borders."[22] The statement takes a sweeping approach towards cybersecurity, encapsulating software development and procurement and supply chain risk management. The fifth to eighth principles are particularly relevant to this paper. The CSP Joint Principles note that "the collective purchasing power of our respective governments can drive cybersecurity improvement and ensure security as a basic design consideration." In India, for instance, the Government is the single largest buyer of goods and services, with public procurement constituting over 20 percent of GDP.[23] Similarly, the United States Federal Government is the largest consumer in the world, with an average expenditure of US$630 billion each year.[24] As such, this gives the Quad considerable sway over software standards and can herald market change.

At the May 2023 Quad Leaders' Summit, the Quad Senior Cyber Group announced a set of overarching principles for secure software.[25] Of particular note are the following measures for government procurement and use of software:

1. Require self-attestation by the software producer, unless a third-party certification is provided, stating that the software's development complies with secure software development practices.

2. Encourage the software developer to report to a respective national vulnerability disclosure program that includes a reporting and disclosure process.

3. Ensure adequate controls and processes to protect software and software platforms from unauthorised access and usage.

4. Ensure adequate controls and processes to protect the confidentiality, integrity, and availability of data used by software and software platforms.

5. Identify and maintain software platforms and the software deployed to those platforms to protect software from exploitation.

Table 1: Relevant Cyber Agencies and Strategies in Quad Member States

	Australia	India	Japan	United States
Cyber Strategy	Cyber Security Strategy for 2023-2030	National Cyber Security Policy (2013) Draft National Cybersecurity Strategy (2021)	International Strategy on Cybersecurity Cooperation (2013) Cybersecurity Strategy (2015) Cybersecurity Strategy 2021	Cybersecurity Strategy, 2023
Relevant implementing bodies	Australian Signals Directorate (ASD), Australian Cyber Security Centre (ACSC), Australian Secret Intelligence Agency (ASIS), Swamwatch by Australian Commission and Competition Commission (ACCC), Office of the Australian Information Commission (OAIC)	National Cybersecurity Coordinator (NCSC), Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), National Technical Research Organisation (NTRO), Defence Cyber Agency	Cyber Security Strategic Headquarters, National Centre of Incident Readiness and Strategy for Cybersecurity (NISC), Cyber Defense Group (under SDF), Controls System Security Centre (CSSC)	The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), U.S. Cyber Command (USCYBERCOM)

Individually, the Quad members make use of a number of policy tools, which are detailed in the following paragraphs. These include public-private partnerships, international partnerships (bilateral and multilateral), skilling and training programmes, and certain arms control instruments such as the US's Entity List and Japan's End-User List. The last of these is linked to the Wassenaar Arrangement, which in 2017 added export controls for surveillance software. However, these are limited to organisations selling or sending technologies with potential military applications abroad and have limited utility with respect to cyber mercenaries.

Australia

Between late 2022 and early 2023, Australia's critical public infrastructure and private enterprises witnessed a number of cyberattacks and ransomware threats which exposed the data of almost 56 percent of the population. [26] Following this, Australia's Minister of Cyber Security, Claire O'Neil announced the release of the discussion paper, 'Cyber Security Strategy for 2023-2030' as an update to the cybersecurity strategy released in 2020. In addition to strengthening cybersecurity practices and securing government systems, the Strategy focuses on harmonising existing regulatory frameworks and priorities on data protection stated within the Australian Commission and Competition Commission's (ACCC) Digital Platform Services Inquiry 2020-25, Attorney General Department's review of the Privacy Act, 1988 and in the Security of Critical Infrastructure Act, 2018. The document has identified enhancing sovereign cyber capabilities as a key issue.

However, the lack of skilled human capital in the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) is the crucial element constraining the two bodies from achieving their stated mandates.[27] Most recently, the Australian Spy Agency was attempting to hire some 1,900 recruits in November 2022.[28] The Australian Government has partnered with private enterprises like IBM, Wipro and Navitas[29] to address the skills gap and protect businesses and critical infrastructure, and start a bug bounty programme[a] to detect cyber security issues.

a Bug Bounty Programmes, used by governments and industry, provide monetary benefits to ethical hackers who identify vulnerabilities and gaps in their technical systems.

The Strategy has also focused on building public-private partnerships for threat sharing, developing national response frameworks and attracting investments in cybersecurity. While Canberra has recognised the role played by the private sector in addressing cyber risks, it has yet to make an official statement on proxy private sector actors or cyber mercenary groups that develop and spread these risks. Moreover, in its recent budget announcement for 2023-2024, Australia announced about US$24 million on digital solutions, including a National Anti-Scam Centre, Digital IDs, and resource allocations to build cyber resilience by training in-house cyber wardens at small business organisations to effectively deal with cyber security attacks.[30]

In addition to exploring cybersecurity cooperative mechanisms within the Quad, Australia is engaging with cybersecurity authorities in the United Kingdom (National Cyber Security Centre or NCSC), in the US (the Federal Bureau of Investigation, FBI; the Cybersecurity and Infrastructure Security Agency or CISA; and the National Security Agency, NSA) to produce joint advisories to reduce ransomware attacks and cyber threats sponsored by Russia.[31,32] Australia has signed a number of Memorandums of Understanding (MoUs) to strengthen cooperation in cyber and critical technologies, including with Papua New Guinea, United Kingdom, and Republic of Korea to build cyber resilience. [33]

India

India has been facing rapidly mounting cyber threats over the last decade largely attributable to the growth in Internet penetration and digitalisation of government services, as well as incidents of instability in its neighbourhood. The Unique Identification Authority of India (UIDAI) was one of many Indian entities targeted by a Chinese state-sponsored group, dubbed TAG-28, in 2021.[34] TAG-28 also targeted The Times Group, a media house. According to cybersecurity firm, Recorded Future, these attacks were part of an ongoing Chinese cyber campaign against India following border clashes in 2020. Other attacks targeted critical infrastructure and state-owned enterprises in the nuclear, space and defence sectors. In the same year, a Chinese APT group, labelled Red Echo by researchers, hacked into India's electricity supply control systems

and power plants and installed malware which was triggered in the coming weeks, intermittently turning off Mumbai's electricity supply; the malware impacted hospitals, which were forced to rely on emergency electricity generators to keep the ventilators of COVID-19 patients operational.[35] In 2023, Phoenix, a pro-Russia hacker group attempted to breach the Ministry of Health and Family Welfare's website, reportedly retaliating against the decision of Indian authorities "not to violate the sanctions as well as comply with the price ceiling for Russian oil approved by the G7 countries."[36]

In 2019, the then National Cybersecurity Coordinator, Lt. Gen (retd) Rajesh Pant, in keeping with the evolving cyber threat landscape, led the drafting of a National Cybersecurity Strategy, a much-needed update from the 2013 policy. The draft was ready by April 2023 and is awaiting Parliamentary approval. The strategy paper will reportedly include guidance on standard operating procedures (SOPs) for responding to cyber incidents and the creation of a national threat exchange.[37] The term 'cyber mercenaries' has not yet appeared in official statements from New Delhi. However, as noted in this paper's introduction, the growth in hack-for-hire groups based or operating in India presents a threat to national security.

New Delhi's engagement on cybersecurity and ICT issues has been extensive, with active efforts to broaden relations with its Quad partners, West Asia, and the European Union. India signed a notable 34 active MoUs focused on ICT and cybersecurity in 2021 alone. Moreover, since the 2010s, India has proactively integrated cybersecurity matters into its engagements with regional groupings such as the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) and the South Asian Association for Regional Cooperation (SAARC). This reflects India's recognition of the growing significance of cybersecurity in the present day and its commitment to fostering cooperation and collaboration in addressing the challenges and opportunities presented by the evolving landscape.[38]

India has made notable strides on offensive cyber capabilities, with a particular focus on Pakistan.[39] Furthermore, there are indications that India may be looking to expand these capabilities, with a keen eye on China.[40]

Japan

Like other Quad members, Japan has witnessed a rapid increase in the incidence of cyberattacks linked to regional geopolitical fissures. In 2013, cybersecurity researchers identified an APT actor dubbed Icefog that targeted the government, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies and mass media organisations of Japan and South Korea.[41] While the report did not explicitly attribute these attacks to China, it noted that it was the origin of several of the IP connections detected. Defence suppliers like Mitsubishi Heavy Industries Ltd and Mitsubishi Electric have been repeatedly targeted by Chinese APTs, most likely because of their access to sensitive weapons research.

Japan's Cybersecurity Strategy 2021 recognises cyberspace as a public space: "In an environment of increasing uncertainty, emergence of vulnerabilities, changes in Japan's national security environment and other factors, cyberspace must have the same level of safety and security as real space in order to be recognised as a public space."[42] As such, the strategy has adopted a stance of 'active cyber defence'. While the nomenclature may sound similar to the US's Defend Forward strategy,[43] it is not likely to advocate for pre-emptive attacks. To advance cybersecurity, the strategy calls for cooperation with like-minded nations and corporations. Building on the success of similar initiatives with the Association of Southeast Asian Nations (ASEAN), Japan has also announced a 'Basic Policy on Cybersecurity Capacity Building Support for Developing Countries', whereby it will support cyber hygiene, measures against cybercrime, cyber situational awareness and skills development in developing countries in the Indo-Pacific.[44]

The national government has also committed to assure trustworthiness of IT devices and services through standards and technical verification, including in the government's procurement of such services. Finally, under the International Strategy on Cybersecurity Cooperation (2013), Japan supports ICT procurement standards processes such as the Common Criteria Recognition Arrangement (CCRA).[45] The CCRA has 31 members, with Australia, India, Japan, US and 14 others recognised under the authorising scheme.

Japan's Ministry of Economy, Trade and Industry (METI) maintains an End User List which names foreign entities suspected to be contributing to the proliferation of Weapons of Mass Destructions (WMD); it also has a Commodity Watch List. At present, however, these lists are limited to proliferation concerns relating to nuclear, missile technology, chemical and biological weapons.[46]

The United States

US-based information technology businesses or critical public infrastructure[47] have been at the receiving end of cyberattacks, specifically by mercenary groups. A hack-for-hire mercenary group, Dark Basin, has targeted American non-profit organisations,[48] especially those working on a campaign[49] requesting the US Department of Justice and the State Attorney General to investigate the role played by Exxon and other big oil companies to sway action on climate change. Dark Basin is also reportedly the entity behind phishing attacks on organisations advocating against net neutrality.[50] While the Citizen Lab based in the University of Toronto has claimed with high confidence that an India-based IT firm, BellTroX is linked to Dark Basin, the research is inconclusive on the clients of BellTroX. On the other hand, research by Meta on cyber mercenary groups using its platform, Facebook, has identified the US as the base of some of the clients for such activities.[51]

Recognising the threat to the US's national security, the Bureau of Industry and Security within the Commerce Department added four entities to the Entity List in November 2021: NSO, Candiru, Computer Security Initiative Consultancy PTE. Ltd., and Positive Technologies[52,b]

b "The Entity List (supplement no. 4 to part 744 of the EAR) identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States."

The Quad Response

The Biden administration has committed to using export controls against entities "that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organisations here and abroad."[53] Moreover, the Department of Defense Cyber Strategy laid the ground for the US to defend forward under the leadership of the US Cyber Command (USCYBERCOM) since 2018.[54] The US Defend Forward Strategy recognised partnerships as integral to addressing persistent threats. For instance, Hunt Forward Operations (HFOs) are defensive operations conducted by USCYBERCOM on the invitation of partner countries to identify malicious cyber activities or vulnerabilities in the networks of host nations.

Private tech companies have also been vocal in opposing the use of services of such mercenary groups. At the US Summit for Democracy in March this year, the 'Principles to Counter Rising Threat Posed by Cyber Mercenaries' was launched, signed by 150 companies.[55]

Pathways for Cooperation

Recommendation 1: The Quad's Senior Cyber Group must build a shared taxonomy of cyber mercenary groups.

This analysis of policy measures within each Quad member country illustrates two fundamental issues. The first is the absence of a shared lexicon around the threats from cyber mercenaries. A multitude of terms—'hack-for-hire', 'proxy actors', 'Private Sector Offensive Actors', 'APTs'—relate to but do not directly describe this threat. Even within the US, where this term has most purchase, the government has not officially endorsed the term 'cyber mercenaries'.

At present, the term 'cyber mercenaries' is used to refer to a wide range of enterprises and operations involved in the development and proliferation of zero-day exploits to supply of malicious software. The Quad Senior Cyber Group should design and adopt a schema of the types of actors that classify as cyber mercenaries along with their responsibilities and scale of impact to determine liabilities and obligations. The three aforementioned classifications of proxy actors that Maurer has specified in his book could serve as a starting point, and consultations with white hat hacker communities[c] and online platforms should inform this process. This taxonomy would also be essential to specify and forge alignment on the degree and distribution of punishments and penalties. For instance, the act of supplying malicious software to States and conducting attacks on behalf of States might need to be classified separately, with respective liabilities and obligations for the involved parties.

Beyond a common vocabulary, it is also important to recognise the asymmetric attribution capabilities between states, including in terms of appropriate channels between Computer Emergency Response Teams (CERTs), national security councils, and other relevant departments or ministries. At present, India conducts bilateral cyber dialogues with the rest of the Quad member countries and has identified cyber threat assessments and capacity building as a priority in those dialogues and at the Quad.

c White hat hacker communities include ethical hackers who utilise their hacking skills to support organisations in identifying security vulnerabilities in networks, hardware and software.

Pathways for Cooperation

Recommendation 2: Inter-sectoral collaboration to support investigations on cyber mercenary networks.

One of the obstacles to addressing the challenges posed by cyber mercenaries is the sheer amount of research required in investigating, exposing and preventing targeted cyberattacks including state-sponsored mercenary spyware created by private companies. Only a few entities are capable of conducting such time- and resource-intensive research, which involves multiple stakeholders to account for how different communities experience such activities.

In 2021, Apple announced a US$10-million grant to civil society organisations supporting cyber surveillance research and advocacy.[56] It also offered researchers at Citizen Lab and other organisations pro-bono threat intelligence, technical and engineering assistance to aid their research. The grant was made to the Dignity and Justice Fund established by the Ford Foundation, and is open for other companies and donors to join and contribute.[57] Initial funding statements for the 2022-2023 cycle of the grant state that the project attempts to explore the mercenary industry by:

a. Building organisational capacity, enhancing collaboration between civil society research and advocacy groups specialising in cybersecurity;

b. Enhancing and supporting partnerships between software developers, device manufacturers and commercial security firms with civil society to effectively identify and address vulnerabilities;

c. Increasing stakeholder awareness on global mercenary spyware industry;

d. Supporting standardised forensic methods to provide evidence for spyware infiltration; and,

e. Building external and internal capabilities within organisations to respond to such attacks through security audits.

Pathways for Cooperation

Another notable example of stakeholder collaboration is the release of the 'Principles to Counter Rising Threat Posed by Cyber Mercenaries', signed by 150 companies in 2023 at the U.S. Summit for Democracy.[58] The implementation of these principles is designed to ensure synchronisation with government processes, existing legal obligations, and internal policies of the tech companies.

Recommendation 3: Quad intelligence agencies must coordinate service procurement guidelines for cyber mercenaries.

Considering the limitations in sophisticated cyber skills and capabilities amongst Quad countries, the possibility of leveraging cyber mercenaries may seem appealing despite the stated risks. Quad countries can forge alignment on service procurement guidelines based on principles of transparency, accountability and openness. Since information about the hired groups, types of attacks and targets, is classified, this exercise would have to be accompanied by an information-sharing agreement that will require countries to define the scope of cooperation and data sharing. Such an exercise could also help identify redundancies in operations targeting shared adversaries, leading to greater efficiency in resource allocation.

The US approach to cyber mercenaries could serve as a starting point for other countries to adopt strict approaches to disrupt the CaaS market by imposing sanctions on enterprises like NSO along with cryptocurrency exchanges to interfere with the flow of monetary incentives. However, there could be some points of concern regarding the approach that needs to be adopted since other Quad countries lack the appropriate policy instruments with the same level of flexibility as the US Entity List. As such, forging alignment on service procurement guidelines could serve as a market signal and a concrete starting point for further collaboration.

Recommendation 4: State- and private-sector supported bounty programmes.

Bug bounty programmes started in 1995 but gained traction only in the 2010s when established tech enterprises like Google started offering rewards for finding security bugs in their products. Since then, to invite

feedback and support from the wider security research community, large enterprises like Apple, Facebook, Microsoft, Etsy, and GitHub offer rewards through Security Bounty programmes to identify vulnerabilities and improve their product offerings.[59] Apple, for instance, in November 2022 offered a bounty of up to US$2 million to researchers with qualifying findings in the Lockdown Mode,[d] making it the highest maximum bounty payout in history.[60] Countries all over the world run similar bug bounty programmes. The US Federal government, for example, launched the Hack the Pentagon programme in 2016.[61] The European Commission also initiated the EU-FOSSA 2 bug bounty initiative in 2019.[62]

As noted with the previous recommendations, the cyber security agencies of the Quad countries are not resourced at the same level. The launch of joint bug bounty programmes could prove to be a more sustainable way for Quad countries to leverage their skilled cyber workforce that would gain recognition and rewards in exchange for ethically and lawfully improving product quality through testing and inspections of government cyber infrastructure.

d Lockdown Mode is one-of-a-kind optional protection offered by Apple to a small group of users to protect themselves from targeted digital threats.

Conclusion

The rise of cyber mercenaries remains underexplored, both as an area of research and a space for cooperation between the Quad countries. This paper sought to highlight the adverse impacts of the unchecked proliferation of such groups, the promising but currently scattered initiatives on cybersecurity undertaken by the Quad countries, and potential touchpoints for cooperation.

While the paper highlights the rise of cyber mercenaries and their operations, there is a need for more comprehensive data on the specific types of actors and the cyberattacks they carry out. There is also an observability bias at play: most publicly available information on cyber mercenaries is based on new groups that are not necessarily sophisticated, and are thus caught or tracked more easily. Understanding the tactics, techniques, and procedures employed by a fuller spectrum of such groups can help in developing more targeted and effective countermeasures.

Furthermore, the motivations and incentives driving individuals to join cyber mercenary groups require further investigation. By delving into the factors that attract individuals to engage in hack-for-hire, policymakers and cybersecurity experts can better address the root causes of this phenomenon and devise strategies to deter potential recruitments. Finally, investigating the legal and diplomatic complexities surrounding state-sanctioned cross-border cyber mercenary activity can offer insights into the mechanisms needed for international cooperation and law enforcement.ORF

Trisha Ray *is a Resident Fellow with the GeoTech Center at the Atlantic Council.*

Antara Vats *is an IIC-UChicago Fellow, currently stationed at the Ministry of Electronics and IT, Government of India.*

Endnotes

1 "What is Software Supply Chain Security?", *Red Hat*, https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security (accessed February 24, 2023).

2 "Check Point Research: Education sector experiencing more than double monthly attacks, compared to other industries", *Checkpoint*, August 9, 2022, https://blog.checkpoint.com/2022/08/09/check-point-research-education-sector-experiencing-more-than-double-monthly-attacks-compared-to-other-industries/

3 "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president", *Reuters*, February 15, 2021, https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R.

4 Recorded Future, "China-Linked Group TAG-28 Targets India's "The Times Group" and UIDAI (Aadhaar) Government Agency With Winnti Malware", *Recorded Future*, September 21, 2021, https://www.recordedfuture.com/china-linked-tag-28-targets-indias-the-times-group.

5 "Japan probes possible involvement of pro-Russian group in cyberattacks", *Reuters*, September 7, 2022, https://www.reuters.com/technology/japan-investigating-possible-involvement-pro-russian-group-cyberattack-nhk-2022-09-06/.

6 *BlackBerry 2022 Threat Report*, (Blackberry: 2022), https://www.blackberry.com/us/en/forms/enterprise/report-bb-2022-threat-report-aem; *Microsoft Digital Defence Report*, (Microsoft: 2022), https://www.microsoft.com/en-us/security/business/security-insider/mddr/nation-state-threats-and-the-rise-of-cyber-mercenaries/

7 Raphael Satter and Christopher Bing, "A Reuters Special Report: How mercenary hackers sway litigation battles", *Reuters*, June 30, 2022, https://www.reuters.com/investigates/special-report/usa-hackers-litigation/; Franz Wild, Ed Siddons, Simon Lock, Jonathan Calvert and George Arbithnott, "Inside the Global Hack-For-Hire Industry", *The Bureau of Investigative Journalism*, November 5, 2022, https://www.thebureauinvestigates.com/stories/2022-11-05/inside-the-global-hack-for-hire-industry; Winnona DeSombre, Lars Gjesvik, and Johann Ole Willers, *Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets* (Washington D.C.: Atlantic Council, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/

8 Shane Huntley, "Updates about government-backed hacking and disinformation", *Google Threat Analysis Group*, May 27, 2020 https://blog.google/threat-analysis-group/updates-about-government-backed-hacking-and-disinformation/.

9 *A/76/151: The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyber activities - Report of the Working Group on the use of mercenaries*, (Geneva: United Nations Human Rights Office of the High Commissioner, 2021), https://www.ohchr.org/en/documents/thematic-reports/a76151-human-rights-impacts-mercenaries-mercenary-related-actors-and

Endnotes

10 White House, "Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits", February 7, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/07/quad-joint-statement-on-cooperation-to-promote-responsible-cyber-habits/

11 Deborah Avant, "Mercenaries", *Foreign Policy*, July-August, No. 143, pp. 20-28 (2004), https://www.jstor.org/stable/pdf/4152906.pdf

12 William Dalrymple, *White Mughals: love and betrayal in eighteenth-century India* (Penguin Books, 2004).

13 "What is Russia's Wagner Group of mercenaries in Ukraine?", *BBC*, January 23, 2023, https://www.bbc.com/news/world-60947877.

14 Tim Maurer, *Cyber mercenaries: the state, hackers, and power*, (Cambridge, Cambridge University Press, 2018): p. 31.

15 *The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyber activities - Report of the Working Group on the use of mercenaries*

16 Denis Makrushin, "Legal malware and cyber-mercenaries", *Kaspersky Lab*, October 9, 2014, https://www.kaspersky.com/blog/legal-malware-counteraction/6282/. Scott Depasquale and Michael Daly, "The growing threat of cyber mercenaries", *Politico*, October 12, 2016, https://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221/.

17 "NSA files decoded: What the revelations mean for you", *The Guardian*, November 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

18 "The 'Icefog' Apt: A Tale of Cloak and Three Daggers", *Kaspersky Lab*, 2013, https://media.kaspersky.com/en/icefog-apt-threat.pdf

19 Fireye, *Southeast Asia: An Evolving Cyber Threat Landscape*, 2015, https://paper.bobylive.com/Security/APT_Report/rpt-southeast-asia-threat-landscape.pdf

20 Mike Dvilyanski, Margarita Franklin, and David Agranovich, *Threat Report on the Surveillance-for-Hire Industry*, *Meta*, December 2022, https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

21 "The Top 10 Countries Most Targeted by Cyber Attacks", *Blackberry*, February 2023, https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report

Endnotes

22 Ministry of Foreign Affairs of Japan, "Quad Cybersecurity Partnership: Joint Principles" accessed March 2, 2023, https://www.mofa.go.jp/files/100347801.pdf

23 "FM Reviews Capital Expenditure & Payments of Maharatnas and Navratnas CPSEs", *Press Information Bureau*, September 28, 2019, https://pib.gov.in/PressReleasePage.aspx?PRID=1586546.

24 "Selling Greener Products and Services to the Federal Government", *United States Environmental Protection Agency*, accessed March 4, 2023, https://www.epa.gov/greenerproducts/selling-greener-products-and-services-federal-government

25 Ministry of External Affairs, Government of India, "Quad Cybersecurity Partnership: Joint Principles for Secure Software", May 20, 2023, https://mea.gov.in/bilateral-documents.htm?dtl/36574/Quad_Cybersecurity_Partnership_Joint_Principles_for_Secure_Software

26 Lewis Jackson, "Australia sees spike in cyber-attacks from criminals and states", *Reuters*, November 5, 2022, https://www.reuters.com/world/asia-pacific/australia-sees-spike-cyber-attacks-criminals-states-2022-11-03/.

27 Byron Kaye and Lewis Jackson, "Analysis: In Australia, a hacking frenzy spurred by an undersized cybersecurity workforce", *Reuters*, November 1, 2022, https://www.reuters.com/technology/australia-hacking-frenzy-spurred-by-an-undersized-cybersecurity-workforce-2022-10-31/.

28 Campbell Kwan, "Top spy agency is hiring 1900 workers. Here's what it takes", *The Australian Financial Review*, November 2, 2022, https://www.afr.com/work-and-careers/careers/what-a-cyber-spy-actually-does-according-to-our-top-spy-chief-20220701-p5ayaf.

29 Mordor Intelligence, *Australia Cybersecurity Market - Growth, Trends, COVID-19 Impact, and Forecasts (2023 - 2028)*, 2023, https://www.mordorintelligence.com/industry-reports/australia-cybersecurty-market

30 Peter Maloney, "Federal Budget 2023-2024: What it means for Cyber Security and Defence", *Australia Cloud*, May 9, 2023, https://www.australiacloud.com.au/news/federal-budget-2023-24/

31 *Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalised Threat of Ransomware, 2022*, (Cybersecurity & Infrastructure Security Agency: 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

32 *Joint Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022.

Endnotes

33 *Partnerships and Agreements,* Department of Foreign Affairs and Trade, Australian Government, accessed April 22, 2023, https://www.internationalcybertech.gov.au/our-work/partnerships-and-agreements

34 Recorded Future, *Cyber Threat Analysis: China,* (September 2021), https://www.recordedfuture.com/china-linked-tag-28-targets-indias-the-times-group

35 Recorded Future, "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions", *Recorded Future*, February 28, 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector

36 "Russian Hacktivist group Phoenix targets India's Health Ministry Website", *CloudSEK*, March 16, 2023, https://cloudsek.com/threatintelligence/russian-hacktivist-group-phoenix-targets-indias-health-ministry-website

37 Deeksha Bhardwaj, "Cybersecurity strategy proposes measures for data breaches", *Hindustan Times,* February 6, 2023, https://www.hindustantimes.com/india-news/cybersecurity-strategy-proposes-measures-for-data-breaches-101675623543530.html

38 Ministry of External Affairs, Government of India, "Joint Statement from Quad Leaders", September 24, 2021, https://mea.gov.in/bilateral-documents.htm?dtl/34318/Joint+Statement+from+Quad+Leaders. Ministry of External Affairs, Government of India, "India-EU Connectivity Partnership", May 8, 2021 https://www.mea.gov.in/bilateral-documents.htm?dtl/33854/IndiaEU_Connectivity_Partnership, Ministry of Electronics & Information Technology, Government of India, "Active MoUs", accessed March 2, 2023, https://www.meity.gov.in/content/active-mous

39 *Cyber Capabilities and National Power: A Net Assessment*, International Institute for Strategic Studies, June 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

40 *Cyber Capabilities and National Power: A Net Assessment*, June 2021.

41 "The 'Icefog' Apt: A Tale of Cloak and Three Daggers", Kaspersky Lab, 2013.

42 *Outline of Japan's Next Cybersecurity Strategy,* National Center of Incident Readiness and Strategy for Cybersecurity, 2021, https://www.nisc.go.jp/eng/pdf/txt_next_CS_strategy_outline.pdf

43 "CYBER 101 - Defend Forward and Persistent Engagement", U.S. Cyber Command, October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

44 Ministry of Foreign Affairs, Government of Japan "Basic Policy on Cybersecurity Capacity Building Support for Developing Countries", 2021, https://www.mofa.go.jp/files/100347812.pdf

Endnotes

45 *International Strategy on Cybersecurity Cooperation,* Information Security Policy Council, 2013, https://www.nisc.go.jp/eng/pdf/International Strategyon Cybersecurity Cooperation_e.pdf, The CCRA was established in 1999 and acts as a platform for mutual recognition of secure and trusted ICT products.

46 Ministry of Economy, Trade and Industry, Government of Japan, "End User List", accessed April 13, 2023, https://www.meti.go.jp/english/press/2020/pdf/0508_002a.pdf

47 Brad Smith, "A moment of reckoning: the need for a strong and global cybersecurity response", *Microsoft Blog*, December 17, 2020, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

48 Bahr Abdul Razzak, Bill Marczak, Siena Anstis, Ron Deibert et al, "Dark Basin: Uncovering a Massive Hack-For-Hire Operation", *Citizen Lab Research Report* No. 128, 2020, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

49 Exxon Knew, https://exxonknew.org/

50 Eva Galperin and Cooper Quintin, "Phish for the Future", *Electronic Frontier Foundation*, September 2017, https://www.eff.org/deeplinks/2017/09/phish-future

51 Mike Dvilyanski, Margarita Franklin, and David Agranovich ,*Threat Report on the Surveillance-for-Hire Industry*, (California: Meta, 2022), https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

52 US Bureau of Industry and Security, Commerce, "15 CFR Part 744, [Docket No. 211019–0210], RIN 0694–AI64, Addition of Certain Entities to the Entity List", November 4, 2021, https://www.federalregister.gov/documents/2021/11/04/2021-24123/addition-of-certain-entities-to-the-entity-list

53 US Department of Commerce, "U.S. Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities", November 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

54 U.S. Cyber Command, "CYBER 101 - Defend Forward and Persistent Engagement", October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

55 US Department of State, "Private Sector Commitments to Advance Democracy", March 29, 2023, https://www.state.gov/private-sector-commitments-to-advance-democracy/

56 Apple Newsroom, "Apple sues NSO Group to curb the abuse of state-sponsored spyware", November 2021, https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

Endnotes

57 Apple Newsroom, "Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware", Apple Newsroom, July 2022, https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

58 "Cybersecurity Tech Accord principles limiting offensive operations in cyberspace", March 2023, Australian Government, https://cybertechaccord.org/uploads/prod/2023/03/Cyber-mercenary-principles_Tech-Accord_032723_FINAL.pdf

59 "Bug Bounty Explained", DDOS Guard, May 11, 2023, https://ddos-guard.net/en/blog/bug-bounty-explained#

60 "Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware", *Apple Newsroom*, July 2022, https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

61 U.S. Department of Defense, "Hacking the Pentagon", https://www.usds.gov/projects/hack-the-pentagon#

62 "European Commission launches new Open-Source Bug Bounties", European Commission, January 25, 2021, https://commission.europa.eu/news/european-commission-launches-new-open-source-bug-bounties-2021-01-25_en

Images used in this paper are from Getty Images/Busà Photography (cover and page 2) and Getty Images/Otto Stadler (back page).

OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org