POLICY BRIEF

APLN

Cybersecurity Threats to Regional Stability in the Asia-Pacific

SAMEER PATIL

OCTOBER 2023

The views represented herein are the author’s own and do not necessarily reflect the views of APLN, its staff, or its board.

Please direct inquiries to:
Asia-Pacific Leadership Network
APLN Secretariat
4th floor, 116, Pirundae-ro
Jongno-gu, Seoul, ROK, 03035
Tel. +82-2-2135-2170
Fax. +82-70-4015-0708
Email: apln@apln.network

This publication can be downloaded at no cost at www.apln.network.

Cover Photo: Increasing Cyber Attacks (Pixahive 2020)

CYBERSECURITY THREATS TO REGIONAL STABILITY IN THE ASIA-PACIFIC

EXECUTIVE SUMMARY

Cyberspace has become the newest arena for geopolitical contestation. Nation-states are exploiting each other's dependence on information, communication and digital technologies to breach computer networks, harvest sensitive data and proprietary information and disrupt critical national infrastructure operations. This brief examines cybersecurity threats in the Asia-Pacific. It describes how cyberattacks fuelled by geopolitical rivalries pose a new threat to the region's security establishments. With over two billion internet users[1], the Asia-Pacific region is amidst a digital revolution, harnessing technology for economic growth and national transformation. Yet, surging cybersecurity incidents imperil the pace of this revolution and threaten regional security.

Governments in the region have implemented several measures to tackle these cyber threats, including cybersecurity policies, legislations and sector-specific regulations. Some inter-governmental collaborations like the Quad and ASEAN (Association of Southeast Asian Nations) are also addressing these issues. Yet the rising tide of attacks, ransomware incidents and data breaches underlines the need to do more. This policy brief offers some pathways for regional governments to strengthen cyber resilience.

[1] Cisco, "VNI Complete Forecast Highlights", 2018, https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Asia_Pacific_Device_Growth_Traffic_Profiles.pdf.

INTRODUCTION

Rife with geopolitical competition, territorial disputes and ethnic antagonisms, the Asia-Pacific's security landscape has steadily expanded in the last decade to include cybersecurity concerns. Over the last few years, several countries in the region have acquired and developed extensive cyber capabilities to launch attacks against their adversaries' computer networks. In many instances, state actors have utilised non-state actors to execute these attacks. The use of these proxies has not only complicated issues around the 'problem of attribution' – determining the actual perpetrator of a cyberattack – but also blurred the distinction between state and non-state actors.

China, Russia and the United States have varying degrees of influence and ties with states in the Asia-Pacific region. This has also translated into the cyberspace and national cyber policies, with US allies like Japan, South Korea and Australia largely aligning with the United States, while countries like Myanmar, Thailand and Cambodia have deepened digital cooperation with China. The East-West polarisation in cyberspace (with the Western camp led by the United States and Europe and the Eastern camp comprising of Russia and China), has further complicated the regional threat landscape. Some countries like India have exercised 'digital sovereignty,' as an extension of its foreign policy orientation of 'strategic autonomy,' by adopting differentiated postures vis-à-vis issues such as data flows and storage as well as tech platforms' accountability while strengthening relations with the West. This has demonstrated an option that countries can exercise to achieve cyber resilience that countries can endeavour to achieve cyber resilience, rather than getting entangled in broader geopolitical dynamics.

REGIONAL CYBER THREAT SCENARIO

The outbreak of the Russia-Ukraine hostilities in February 2022 has also cast its shadow over the Asia-Pacific's cyber stability. While Russia utilised cyber coercion tools vis-à-vis Ukraine under the rubric of 'hybrid warfare' to support its kinetic war efforts, the People's Republic of China too has adopted 'grey-zone tactics' - methods that seek to exploit the space between peace and war by undertaking actions to attain strategic goals and objectives without triggering an all-out conventional war[2] – as part of its actions to coerce the neighbours. Other powers too like Iran and North Korea have targeted their adversaries through malicious cyber activities. Consequently, cybersecurity concerns have dominated threat perceptions of governments in the region. These concerns span two dimensions: malicious cyber activities performed by state and non-state actors with

[2] John Chambers, "Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army", Modern War Institute, October 18, 2016, https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.

geopolitical motives, and crimes committed by cybercriminal gangs driven by financial motives.

Malicious cyber activities and geopolitical rivalries

Amongst the regional actors, China, North Korea, Iran and Russia have emerged as formidable state actors engaged in malicious and offensive cyber operations primarily targeted at their adversaries.

China is the leading state actor responsible for several cyberattacks, advanced persistent threat (APT) vectors,[3] and cyber espionage campaigns. As noted earlier, China has executed such attacks as part of its 'grey-zone tactics,' specifically directed against those countries with whom China has had long-standing territorial and sovereignty disputes. For instance, Chinese offensive cyber activity against India has intensified since a tense border stand-off broke out between the two countries in the Himalayas in May 2020. Prominent examples attributed to China and Chinese state-sponsored hacking groups against India include the breach of the All India Institute of Medical Sciences healthcare facility (December 2022)[4] and repeated intrusions of national power grids and other parts of critical national infrastructure (October 2020 and April 2022 respectively).[5]

Other neighbours of China have faced similar disruptive cyberattacks, such as attacks on Taiwanese websites during a visit by the US Speaker Nancy Pelosi to the country in August 2022,[6] data breach of Japanese tech firm Fujitsu by Blacktech group (August 2021),[7] and a cyber espionage campaign against the Vietnamese government and

[3] The United States Cybersecurity and Infrastructure Security Agency defines APT as "a well-resourced adversary engaged in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion. APT objectives could include espionage, data theft, and network/system disruption or destruction." See Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threats and Nation-State Actors", https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors.

[4] Lingamgunta Nirmitha Rao, "AIIMS Delhi server attack originated from China, 5 servers successfully retrieved: Report", *Hindustan Times*, December 14, 2022, https://www.hindustantimes.com/india-news/aiims-delhi-server-attack-originated-from-china-5-servers-successfully-retrieved-report-101671008642520.html.

[5] Insikt Group, "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/.

[6] Jonathan Greig, "Taiwanese Government Sites Disrupted by Hackers Ahead of Pelosi Trip", *The Record*, August 2, 2022, https://therecord.media/taiwanese-government-sites-disrupted-by-hackers-ahead-of-pelosi-trip.

[7] Tatsuya Sudo and Hidemasa Yoshizawa, "Hackers sought government data on nuclear plants, Olympics," *The Asahi Tribune*, August 31, 2021, https://www.asahi.com/ajw/articles/14430219.

military by Cycldek group (April 2021).[8] These cyberattacks suggest a combination of Chinese coercion and retribution.

Another malicious activity reportedly attributed (but not definitively established) to Chinese hackers – state-sponsored or otherwise, is the targeting of the election infrastructure and processes. According to the Australian Strategic Policy Institute, Chinese cyber interference in elections has been witnessed in Australia, Indonesia, Singapore and Taiwan.[9] For a decade, Beijing has systematically cultivated contacts in politics, media and universities, which have given it better political access, and enabled its espionage. This has helped Beijing to favourably shaped a pro-China narrative and to facilitate the rise of pro-China political parties and actors in many democracies.[10] In Australia, in one the most high-profile case in 2017, Sam Dastyari, then a senator from New South Wales, was exposed for accepting donations from a Chinese businessman, linked to the Chinese Communist Party.[11]

Other significant regional threat actors are North Korea, Iran and Russia.

The North Korean regime has specialised in cyber heists to compensate for the financial assets freeze imposed by crippling international sanctions.[12] Its proxy, the Lazarus Group, has launched several attacks targeting financial institutions worldwide.[13] Its most significant breach was the 2016 Bangladesh Bank account hacking at Federal Reserve Bank, New York, which fetched it US$ 100 million after attempting to steal US$ 900 million.[14] The group has boosted the ruling Kim dynasty's fortunes with such bank thefts.[15] Of late, the regime has diversified and begun targeting cryptocurrency exchanges. Chainalysis, a blockchain data platform, estimates that in 2022 hacking

[8] "Advanced threat actors engaged in cyberespionage in APAC up their game in new campaign," Kaspersky, April 5, 2021, https://www.kaspersky.com/about/press-releases/2021_advanced-threat-actors-engaged-in-cyberespionage-in-apac-up-their-game-in-new-campaign.

[9] Fergus Hanson, Sarah O'Connor, Mali Walker, and Luke Courtois, "Hacking Democracies", Australia Strategic Policy Institute, May 15, 2019, https://www.aspi.org.au/report/hacking-democracies.

[10] Joshua Kurlantzick, "China's Growing Attempts to Influence U.S. Politics", *Council on Foreign Relations*, October 31, 2022, https://www.cfr.org/article/chinas-growing-attempts-influence-us-politics.

[11] Stephanie Peatling and Fergus Hunter, "China scandal: Embattled Labor senator Sam Dastyari resigns from Parliament", *The Sydney Morning Herald*, December 12, 2017, https://www.smh.com.au/politics/federal/china-scandal-embattled-labor-senator-sam-dastyari-resigns-from-parliament-20171211-h02ddn.html.

[12] Daniel A. Pinkston, "North Korea's Objectives and Activities in Cyberspace", *Asia Policy* 15, No. 2 (2020): pp. 76–83, https://doi.org/10.1353/asp.2020.0031.

[13] "Lazarus Group", Council on Foreign Relations, accessed June 15, 2023, https://www.cfr.org/cyber-operations/lazarus-group.

[14] Joshua Hammer, "The Billion-dollar Bank Job", *The New York Times Magazine*, May 3, 2018, https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

[15] Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat", The Heritage Foundation, September 2, 2021, https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat.

groups linked to the North Korean regime stole US$ 1.7 billion worth of cryptocurrency through several breaches into cryptocurrency exchanges and investment firms.[16]

Within the same ecosystem, the regime has also attacked play-to-earn cryptocurrency video games, cryptocurrency trading companies, venture capital funds investing in cryptocurrency, and individual holders of large amounts of cryptocurrency or valuable non-fungible tokens. This demonstrates the continued upgrading of North Korean offensive cyber capabilities.[17] This profiteering from cyber heists is used to advance its nuclear and ballistic missile capabilities, which are then used to threaten South Korea, Japan and the United States, and has a direct fallout on regional stability . In 2019, the United Nations (UN) reported that Pyongyang had accumulated an estimated US$ 2 billion for its weapons of mass destruction programme by executing cyberattacks.[18]

Likewise, Iran has refined its offensive cyber capabilities over the years. Besides using them for domestic surveillance and repression, Tehran has hit its regional adversaries, Saudi Arabia, Israel,[19] and the United States, while weathering multiple crippling cyberattacks on its infrastructure.[20] For instance, Iran has significantly ramped up its cyber capabilities since the Stuxnet attack in 2010-11, which hit its nuclear programme.[21] In the US government's assessment, Iranian military's Islamic Revolutionary Guard Corps is the driving force behind the country's cyber malfeasance.[22] Their technical assessment suggests that, though not as sophisticated as China or Russia, Iran has advanced social engineering tactics to execute politically motivated, disruptive operations.[23] It has also relied on its proxies, Hamas and Hezbollah terrorist groups.[24]

[16] Chainalysis, "The 2023 Crypto Crime Report", accessed June 21, 2023, https://go.chainalysis.com/2023-crypto-crime-report.html.

[17] Cybersecurity and Infrastructure Security Agency, "Alert (AA22-108A) TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies", April 20, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-108a.

[18] Reuters, "North Korea: Missile programme funded through stolen crypto, UN report says," *BBC*, February 6, 2022, https://www.bbc.com/news/world-asia-60281129.

[19] David Shamah, "Official: Iran, Hamas conduct cyber-attacks against Israel", *The Times of Israel*, August 13, 2015, https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

[20] Center for Strategic and International Studies, "Publicly Reported Iranian Cyber Actions in 2019", accessed June 15, 2023, https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019.

[21] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", WIRED, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[22] Cybersecurity and Infrastructure Security Agency, "Iran Cyber Threat Overview and Advisories", accessed June 15, 2023, https://www.cisa.gov/uscert/iran.

[23] John Leyden, "Iranian cyber-threat groups make up for lack of technical sophistication with social engineering trickery," *The Daily Swig*, July 1, 2021, https://portswigger.net/daily-swig/iranian-cyber-threat-groups-make-up-for-lack-of-technical-sophistication-with-social-engineering-trickery.

[24] David Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks against Israel", *Times of Israel*, August 13, 2015, https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

While not as frequent as China's, Russian malicious cyber activities have also been observed in the Asia-Pacific. For instance, Indonesia accused Russian actors of interfering in its national elections in March 2019.[25] Similarly, several Russian cybercriminal gangs have targeted businesses and critical infrastructure facilities in the region. In July 2023, a ransomware attack disrupted operations at Japan's busiest port facility, the Port of Nagoya, for two days. The attack was reportedly attributed to Russia-based ransomware group Lockbit 3.0.[26] Previously, the US Department of Justice has linked the same threat actor to numerous other ransomware attacks across the United States, Asia, Europe and Africa. [27] At the other end of the region, Israeli experts assess likely collaboration between Iran and Russia in the backdrop of the conflict in Ukraine.[28] According to them, Iranian threat actors linked to Moscow have reportedly been involved in a series of attacks targeting the websites of Israeli banks, telecom firms, and the postal service, among others.

A related challenge faced by democracies in the region is disinformation and foreign state-sponsored propaganda. It became particularly pronounced during the COVID-19 pandemic when Chinese disinformation campaigns focused on themes such as obfuscating Coronavirus' origins, the pandemic's spread, and the alleged ineffectiveness and side effects of COVID-19 vaccines. For instance, when Taiwan saw a spike in COVID-19 infections in 2021, China circulated false information regarding the virus's spread. The onslaught of this disinformation campaign forced the government to accuse China of engaging in cognitive warfare against Taiwan to spread distrust against the authorities and undermine social stability.[29] According to Taiwanese officials, an estimated one-fourth of pandemic-related disinformation had originated from China.[30] In August 2023, social media platform, Meta purged about 7,700 of its social network accounts linked to China-based groups trying to manipulate public opinion. Some of these accounts had posts that claimed that COVID-19 originated in

[25] Viriya Singgih, Arys Aditya, and Karlis Salna, "Indonesia Says Election Under Attack From China, Russia Hackers", *Bloomberg*, March 13, 2019, https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers.

[26] "Ransomware attack from Russia hits Japan's biggest port, delaying cargo", *The Straits Times*, July 5, 2023, https://www.straitstimes.com/asia/east-asia/ransomware-attack-from-russia-hits-japan-s-biggest-port-delaying-cargo.

[27] U.S. Attorney's Office, District of New Jersey, "Russian National Charged with Conspiring to Commit Lockbit Ransomware Attacks Against U.S. and Foreign Businesses", June 15, 2023, https://www.justice.gov/usao-nj/pr/russian-national-charged-conspiring-commit-lockbit-ransomware-attacks-against-us-and.

[28] Avi Davidi, "Iranian-Russian Cooperation on Hack Attacks May Challenge Israeli Cyber Supremacy", *Times of Israel*, April 18, 2023, https://www.timesofisrael.com/iranian-russian-cooperation-on-hack-attacks-may-challenge-israeli-cyber-supremacy/.

[29] Sophia Yang, "Taiwan health official warns of China's 'cognitive warfare'", *Taiwan News*, May 22, 2021, https://www.taiwannews.com.tw/en/news/4208260.

[30] Audrey Tang and Joseph Wu, "Why Taiwan seeks Israel's help to combat cybersecurity threats – opinion", *The Jerusalem Post*, July 26, 2021, https://www.jpost.com/opinion/why-taiwan-seeks-israels-help-to-combat-cybersecurity-threats-opinion-674983.

the United States. The platform added that these accounts targeted the United States, Taiwan, Japan among others, and that some pages were in Japanese.[31]

Besides these countries several other states in the region like Australia, Japan, South Korea[32], as well as Vietnam[33], and Pakistan[34] have developed significant cyber warfare capabilities. In recent years, analysts have also noted a gradual uptick in India's cyberwarfare capabilities.[35]

Soaring cybercrimes

On the other end of the threat spectrum for Asia-Pacific is the unprecedented rise in cybercriminal activities. The unprecedented global health emergency of COVID-19 allowed malicious actors to step up their activities as this period saw persistent attacks on hospitals, healthcare facilities, and vaccine manufacturing firms. Moreover, darknet marketplaces thrived during the COVID-19 pandemic by selling pandemic-related wares like protective gear and hard-to-get medications.[36]

The rising ransomware attacks since 2020 illustrate the menacing proportions the threat of cybercrime has assumed. According to the United Nations Office on Drugs and Crime, there was a 600% rise in cybercrimes in Southeast Asia in 2021, the majority being ransomware attacks.[37] In spite of multilateral and plurilateral initiatives like the Counter Ransomware Initiative that aims to amplify awareness and foster innovative diplomatic solutions to combat the pervasive ransomware threat,[38] the risk persists. Typically, cybercriminals target businesses and organisations that do not possess valuable or critical data, as they lack adequate cyber guardrails, focusing on operating critical facilities and services.

[31] "Meta removes thousands of China-based accounts over alleged disinformation", *NHK World-Japan*, August 30, 2023, https://www3.nhk.or.jp/nhkworld/en/news/20230830_20/.

[32] Bart Hogeveen, "The Future of Cyber Warfare in the Indo-Pacific," ORF Issue Brief No. 604, January 2023, https://www.orfonline.org/research/the-future-of-cyber-warfare-in-the-indo-pacific/.

[33] John Leyden, "Covid-19 cyber-espionage: Vietnam blamed for attacks on Chinese government", *The Daily Swig*, April 23, 2020, https://portswigger.net/daily-swig/covid-19-cyber-espionage-vietnam-blamed-for-attacks-on-chinese-government.

[34] Sameer Patil, and Aditya Bhan, "Pakistan is India's new cybersecurity headache", Gateway House, November 11, 2021, https://www.gatewayhouse.in/pakistan-indias-cybersecurity-headache/.

[35] John Leyden, "Indian cyber-espionage activity rising amid growing rivalry with China, Pakistan", *The Daily Swig*, June 30, 2021, https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan.

[36] David Maimon, "Sketchy Darknet Websites Are Taking Advantage of the COVID-19 Pandemic – Buyer Beware", *The Conversation*, August 19, 2020, https://theconversation.com/sketchy-darknet-websites-are-taking-advantage-of-the-covid-19-pandemic-buyer-beware-143237.

[37] "Ransomware attacks, a growing threat that needs to be countered," United Nations Office on Drugs and Crime, October 18, 2021, https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html.

[38] Tobias Scholz and Sameer Patil, "Harnessing the G20's Potential for Global Counter-Ransomware Efforts", T20, May 2023, https://t20ind.org/research/harnessing-the-g20s-potential-for-global-counter-ransomware-efforts/.

Cybercrimes have also gotten a boost from darknet marketplaces, which hawk stolen personal and financial data, counterfeit items, malware, computer viruses, and narcotic substances. This risk is particularly pronounced in the financial sector. According to the Russian cybersecurity and anti-virus software firm Kaspersky, Australia, China, India, and Singapore comprise 84% of all data leak sell orders placed on darknet sites.[39]

POLICY IMPLICATIONS

The continuing cyberattacks, ransomware incidents and data breaches demonstrably affect Asia-Pacific governments, making cyber threats transnational. National legislations implemented by governments in the region include India's National Cyber Security Policy (2013)[40], Australia's 2023-2030 Australian Cyber Security Strategy, Japan's The Basic Act on Cybersecurity (2014) and the Philippines' Cybercrime Prevention Act (2012). The Computer Emergency Response Teams (CERT) in each country have also taken steps to protect internet users in their countries from malware and viruses.

There have been regional inter-governmental initiatives too. For instance, the INTERPOL's Global Complex for Innovation in Singapore has provided training in digital crime investigation and operational support for cybercrime resolution.[41] The Quad, comprising Australia, India, Japan and the United States, has agreed to deepen cooperation in regional capacity building through the Quad Cybersecurity Partnership.[42] The ASEAN has also initiated Cybersecurity Cooperation Strategy (2021-2025) for information sharing, capacity building and confidence-building measures.[43]

These efforts demonstrate that governments in Asia-Pacific appreciate the need for greater focus on cybersecurity matters. Cyberattacks have a significant economic impact, both on businesses and on governments. As the region expands its digital economy footprint, it has become imperative for governments to expand cybersecurity cooperation. In recent years for instance, the United States has expanded cybersecurity cooperation with its partners in Asia with India, Japan, Australia and South Korea

[39] Securelist, "External Attack Surface and Ongoing Cybercriminal Activity in APAC Region," September 19, 2022, https://securelist.com/external-attack-surface-and-ongoing-cybercriminal-activity-in-apac-region/107430/.

[40] Ministry of Electronics and Information Technology, "National Cyber Security Policy -2013", https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

[41] "Promoting Creative and Innovative Solutions to Fight Technology-Enabled Threats," Interpol, accessed July 14, 2023, https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre.

[42] Ministry of Foreign Affairs of Japan, "Quad Cybersecurity Partnership: Joint Principles", accessed July 14, 2023, https://www.mofa.go.jp/files/100347801.pdf.

[43] "ASEAN Cybersecurity Cooperation Strategy (2021 – 2025)", Association of Southeast Asian Nations, accessed July 14, 2023, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

topping the list.[44] They can indeed build on their existing efforts to foster greater cooperation on addressing cybersecurity threats.

RECOMMENDATIONS

i. Advancing norms for responsible state behaviour

In the context of cybersecurity, governments in the region should initiate a conversation on evolving a common position on responsible state behaviour, violation of sovereignty, attribution for cyberattacks, and the right to self-defence against state-sponsored cyberattacks. This should primarily focus on safeguarding critical national infrastructure, any disruption of which has grave implications. Such an exercise will also give many smaller states in the region a sense of agency in global cyber governance.

ii. Addressing darknet marketplaces-enabled cybercrimes

Darknet marketplaces often operate across borders, making it difficult for law enforcement agencies to track down and prosecute the criminals who operate them. Governments in Asia-Pacific need to expand on the efforts of the INTERPOL to share cyber threat intelligence and develop appropriate cyber forensics capacity to investigate darknet and cryptocurrency transactions activities. They can also work with cryptocurrency exchanges and Virtual Private Network providers to scrutinise malicious network traffic and actors.

iii. Securing critical national infrastructure

Governments in the region can take practical steps to strengthen critical infrastructure security. For instance, to assess the capacity of their critical infrastructure to disruptive ransomware and cyberattacks, they can conduct real-world simulations of such attacks. This will help shape their response to persistent, offensive cyber operations and data breaches and identify areas requiring capacity strengthening. They can also maintain a common malware repository for trend analysis.[45]

[44] Center for Global Security Research, Lawrence Livermore National Laboratory, "U.S. and Allied Cyber Security Cooperation in the Indo-Pacific", https://cgsr.llnl.gov/content/assets/docs/US_and_Allied_Cyber_Security_Cooperation_in_the_Indo-Pacific.pdf.

[45] Trisha Ray, "An ASEAN-India Cybersecurity Partnership for Peace, Progress, and Prosperity: Report of the Third ASEAN-India Track 1.5 Dialogue on Cyber Issues", Observer Research Foundation, April 2022, https://www.orfonline.org/research/asean-india-cybersecurity-partnership-for-peace-progress-and-prosperity/.

iv. Creating a standalone regional cybersecurity agency

The lack of a pan-regional cybersecurity organisation is a significant gap in Asia-Pacific's cybersecurity preparedness. Major regional powers like India, Japan, Indonesia and Australia can facilitate the creation of a dedicated cybersecurity agency to work with the national CERTs and have technical experts from the industry to tackle cyber incidents.

CONCLUSION

Asia-Pacific's cyber threat landscape is evolving and becoming multifaced. Today's cyberattacks are sector-specific, target-specific and highly penetrating. Consequently, they have high economic costs and socio-political outcomes. At the same time, these advancing threats create an urgency for regional governments to act on their shared concerns and deepen their cooperation. Governments in Asia-Pacific can do their bit to strengthen resilience and promote cyber stability even as global cooperation is impeded by the East-West polarisation over the Ukraine conflict and due to differing visions of cyberspace management.

ABOUT THE AUTHOR

Sameer Patil is Senior Fellow, Centre for Security, Strategy and Technology, Observer Research Foundation, India. His work focuses on the intersection of technology and national security, including cybersecurity. Dr Patil also serves as India Commissioner for the Global Tech Security Commission, set up by the Krach Institute for Tech Diplomacy at Purdue and the Atlantic Council. Prior to joining ORF, he was at Gateway House, a Mumbai-based foreign policy think tank. He has previously worked at the National Security Council Secretariat, Government of India. He is the author of *Securing India in the Cyber Era* (Routledge, London & New York, 2022) and co-editor of *Moving Forward EU-India Relations: The Significance of the Security Dialogues* (Edizioni Nuova Cultura, Rome, 2017). Dr Patil has participated in several Track 1 and Track 1.5 dialogues, including India-U.S. and India-U.K. Strategic Intelligence Dialogues, which were convened after the 2008 Mumbai terrorist attacks, and the India-U.K. Track 1.5 Cyber Dialogue in 2017. He is a recipient of the Australian Government's prestigious Canberra Fellowship in 2019.

ABOUT APLN

The **Asia-Pacific Leadership Network for Nuclear Non-proliferation and Disarmament (APLN)** is a Seoul-based organization and network of political, military, diplomatic leaders, and experts from across the Asia-Pacific region, working to address global security challenges, with a particular focus on reducing and eliminating nuclear weapons risks. The mission of APLN is to inform and stimulate debate, influence action, and propose policy recommendations designed to address regional security threats, with an emphasis on nuclear and other WMD (weapon of mass destruction) threats, and to do everything possible to achieve a world in which nuclear weapons and other WMDs are contained, diminished, and eventually eliminated.

@APLNofficial @APLNofficial apln.network