Issue Brief

July 2024
No : 403

Quad's Cyber Quandary: Navigating the Digital Minefield in the Indo-Pacific

Govind Nelika

Quad's Cyber Quandary: Navigating the Digital Minefield in the Indo-Pacific

Govind Nelika

Abstract

The Quadrilateral Security Dialogue (Quad) has evolved into a strategic partnership addressing Indo-Pacific security challenges. The Quad Leaders' Summit in May 2023 reaffirmed the commitment of the United States, Japan, India, and Australia to regional resilience and prosperity, focusing on critical areas, including sustainable energy, infrastructure, telecommunications, and cybersecurity.

This paper thoroughly examines the cyber threats confronting Quad member states, providing a detailed analysis of notable state-sponsored attacks and their ramifications. It further explores the dynamics of resource sharing and collaborative agreements within the Quad framework, highlighting its potential to emerge as a robust platform for security dialogue. The paper focuses on the collective security arrangements in the Indo-Pacific, offering insights into the intersection of cybersecurity, geopolitics, and international relations in an increasingly digital world.

Keywords: Cybersecurity, QUAD, USA, Japan, India, Australia, APT, Indo-Pacific, State-sponsored attacks, regional stability

Introduction

The Quadrilateral Security Dialogue (Quad) was initially formed in response to the 2004 tsunami. Since its inception, the Quad has significantly deepened its engagement, culminating in the Quad Leaders' Summit on May 20, 2023, hosted in Hiroshima. The summit marked a pivotal moment for the group, with leaders from the United States, Japan, India, and Australia reaffirming their commitment to enhancing the resilience and prosperity of the Indo-Pacific region. Key focus areas included sustainable energy, infrastructure development, and the development of telecommunications and network capabilities and means to combat threats in cyberspace.

As the Quad continues to solidify its position, it faces challenges, notably increasing hybrid warfare scenarios its member states face. The Quad's evolution from an ad hoc entity handling disaster management to a strategic dialogue addressing shared security concerns is crucial. In this context, the paper will analyse the threat actors faced by QUAD countries and the exchange of resources and agreements that are set in place for a more secure Indo-Pacific.

State-sponsored "Advanced Persistent Threat" (APT)

State-sponsored threat groups, or APTs, have been a cause for concern for nations over the last decade. In 2024, the government of Australia identified and imposed cyber sanctions on Russian citizen Dmitry Yuryevich Khoroshev for his alleged role with the Lock-Bit ransomware group (Australia, 2024). While other members of the QUAD are facing similar cyber intrusions, another example would be China-aligned Evasive Panda targeting the Monlam Festival held in India, essentially creating a watering hole to target users on specific networks visiting the festival website and injecting malicious executables into their systems (ESET Research, 2024). The same goes for Japan, which has been the centre focus altogether; Kazutaka Nakamizo, Deputy Director of Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), stressed the rise of Chinese-backed cyber-attacks which

had grown significantly in recent years, at the Munich Security conference. He said the attacks focused primarily on critical infrastructure and telecom networks. In conjunction, in 2024, the U.S. identified the Volt Typhoon, a threat actor supposedly linked to Beijing that had breached their infrastructure and collected vital information by utilising the living of the land approach (Microsoft Threat Intelligence, 2023). As we proceed, we will briefly analyse each country's threat profile.

Australia

In the context of the QUAD and the broader Indo-Pacific region, Australia occupies a significant geopolitical position due to its traditional ties to the West and its membership in alliances such as AUKUS and SQUAD. As a member of the QUAD, Australia has faced numerous cyberattacks, highlighting its vulnerability in this domain. The Australian Signals Directorate (ASD) Cyber Threat Report for 2022-23 provides a detailed overview of the escalating cyber threat landscape; the Australian Cyber Security Centre (ACSC) under ASD is the lead agency of the Australian government on cybersecurity. The chart below illustrates the sectors most affected by these cyber incidents in 2023.

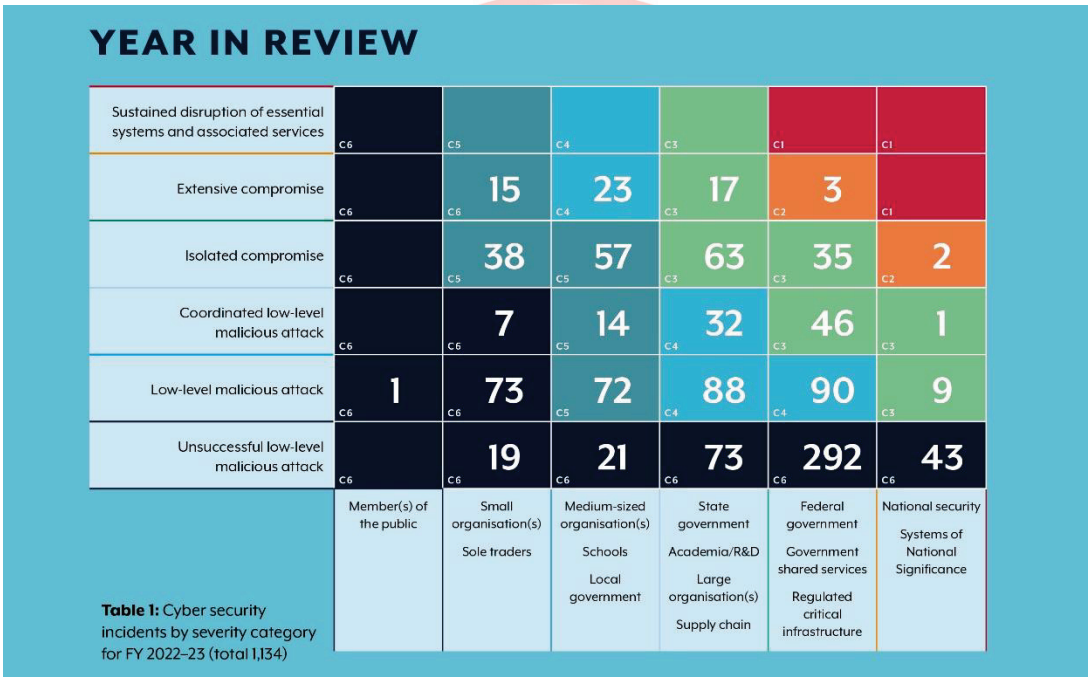

Figure 01 (ASD, 2024)

While several industries were attacked, a special note is given to ransomware attacks, where the extortion is phased, the attacker extorts the target with the decrypt key and for not selling their data on the deep web. The report by ASD notes ransomware as the most destructive cybercrime threat in 2022–23 to Australian entities, with it focusing on the following industries

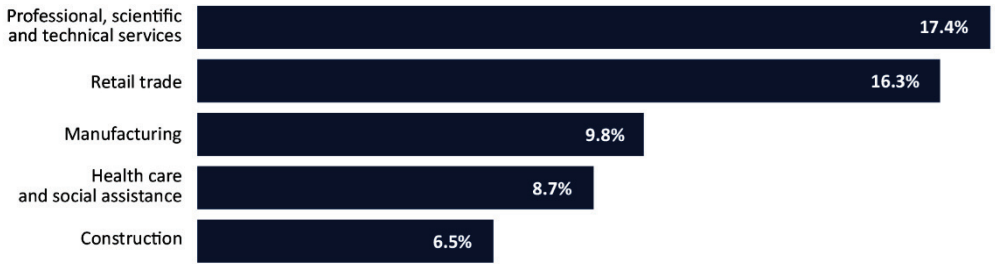

Figure 02 (ASD, 2024)

Some notable threat actors targeting Australia are BlackCat/AlphaV, Lockbit3.0 and CLOP. All three have been linked to Russian hacker groups, which primarily operate as ransomware as a Service (RaaS). In contrast, BlackCat/AlphaV and Lockbit actor groups were taken down by the combined efforts of international law enforcement agencies in December 2023 and February 2024, respectively. The ransomware group BlackCat is said to be a rebranding of Blackmatter, a former ransomware group which had been shut down in 2021 (Gatlan, 2022). As a result of Operation Cronos, a coordinated effort involving the US, Canada, the U.K., Europe, Japan, and Australia, the Lockbit group was disrupted. The joint operation seized the Lockbit website and flashed Press releases from the NCA, the FBI, and Europol, taking down the group (Boyton, 2024). However, while the combined efforts of these agencies were able to take down then-active Lockbit sites, the group's new Tor site is again live. The screenshot is attached under:

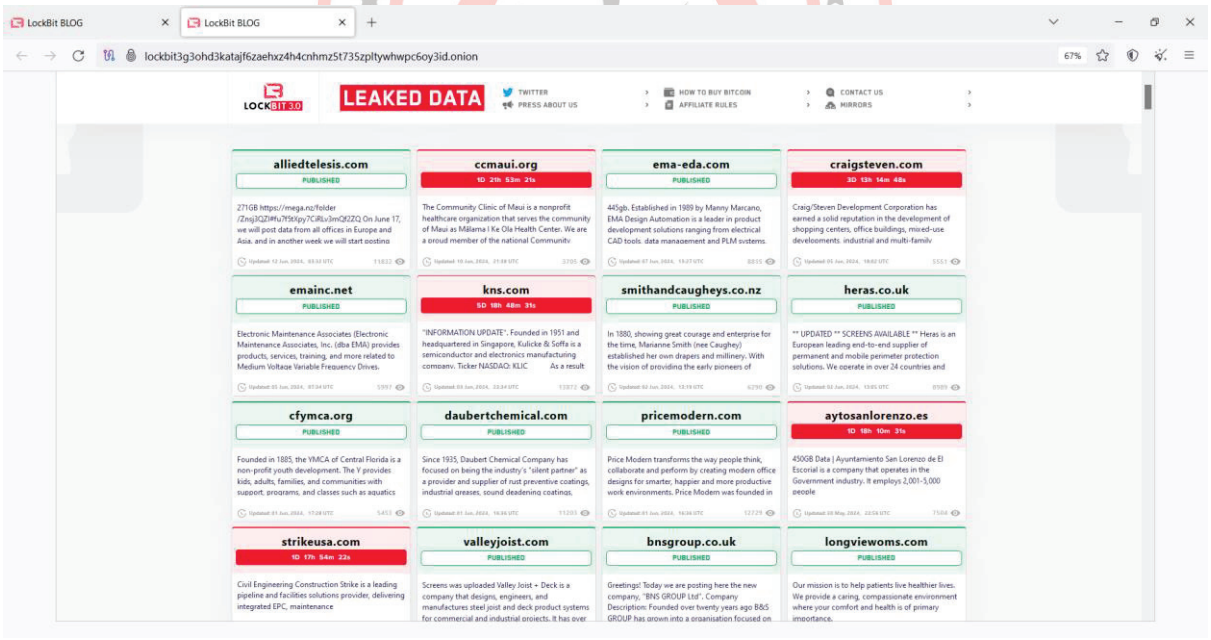

Figure 03 (Lockbit3.0, n.d.)

India

India's profile for cybercrimes differs somewhat from that of other countries. Due to its unique geopolitical location, India plays a crucial role in the larger Indo-Pacific region. The Indian Computer Emergency Response Team (CERT-In) has significantly improved. However,

it still lacks access to the advanced facilities available to its counterparts in other nations and is slowly working towards the same stature as its counterparts. The National Crime Records Bureau (NCRB) of India in 2023 alone estimates an increase of 24.4 per cent in cybercrimes (ANI, 2023). While Internal cybercrimes are an issue, so are the Advanced Persistent Threats (APT) against India. There are several APTs which have targeted India over the years mainly for profit and malicious reasons.

A prompt example would be APT 36, better known as Tribe/Earth Karkaddan, linked to Pakistan, primarily targeting Indian Defence and government agencies, focusing on those dealing with the Kashmir region and human rights activists working in Pakistan (Trendmicro, 2022). Their latest campaign was identified by Sentinel One, a cybersecurity company based in the U.S. According to their report, APT 36 was utilising a Remote Access Trojan (RAT) embedded in the YouTube APKs distributed outside the Google Play store. In most instances, targets are identified prior, and a combination of social engineering & spear phishing tactics are used on the victim to download the infected APK. Once the malware is executed, the RAT gains access to the directory, collecting passwords, browser data, and other information. (Delamotte, 2023). A detailed modus operandi of APT 36 was analysed by Trend Micro and is as follows:

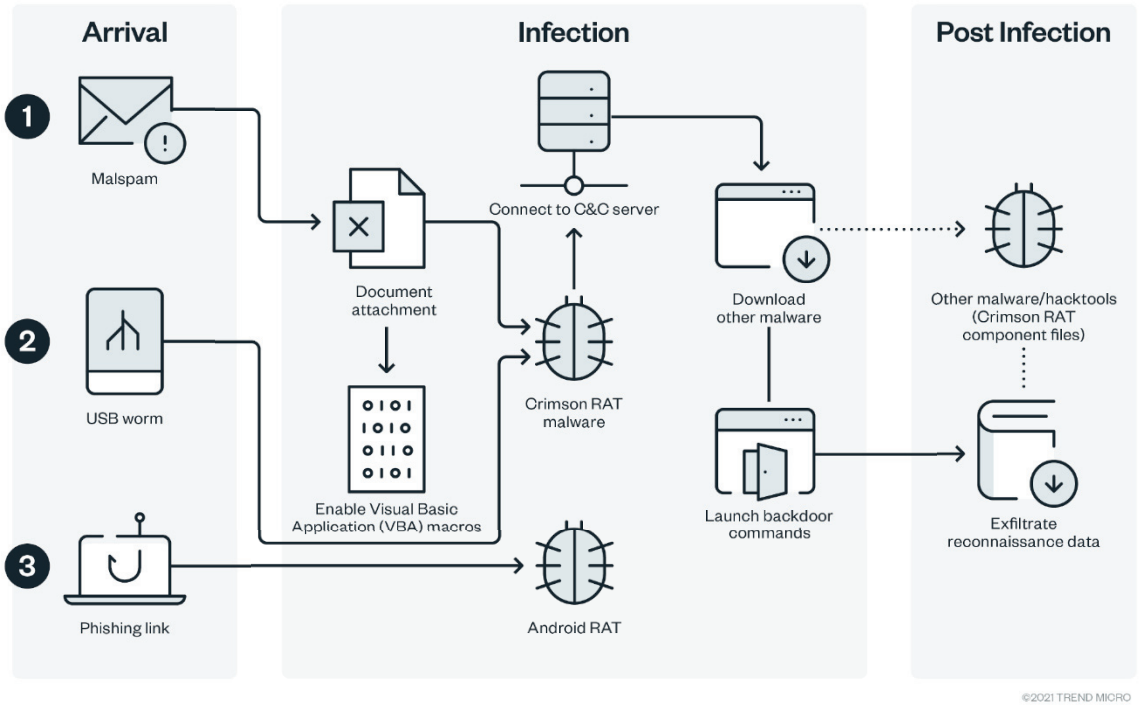

Figure 04 (Trendmicro, 2022)

As seen above, while we look at Pakistan-linked APT 36, little can be done about such threat actors, primarily because of a lack of International Laws addressing such issues and India not being party to the Budapest Convention on Cybercrime. Furthermore, threat groups originating from China, specifically APT 41, known by its many aliases like twin dragons/Winnti, had targeted websites in India focusing on government and airline websites (Mengle, 2022). Another threat actor linked to PLA Unit 69010, identified as Red-Foxtrot, attacked Indian power grids. Although the attack failed, it may indicate that the group conducted a system vulnerability analysis for future attacks (Inskit Group, 2022). At the same time, other QUAD

members can leverage their Western partners to disrupt such threats, but the same cannot be said for India. India is focusing more on defensive cyber tactics than offensive ones compared to its allies.

Japan

Japan has a long history of being targeted by threat actors, leading to the formation of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC). The cyber attacks on Japan mainly focused on internal systems, defence contractors, and even the foreign ministry's telecommunication systems. In 2011, Mitsubishi Heavy Industries Ltd, Japan's largest defence contractor, holding licenses to aircraft, Patriot missiles, F-15J, Fighter Jets and several other guided weapons systems, had been breached. While speculations existed that China had been the perpetrator, it was never verified (Lennon, 2011). In 2024, China-linked threat actors had supposedly also breached Japan's Foreign Ministry telecommunications system, handling official telegrams and classified diplomatic information (Shimbun, 2024). In the case of Japan, a specific APT had been detected, classified as APT 10, better known as Stone Panda/Red Apollo, known for targeting construction and engineering, aerospace, and telecom firms in Japan and other countries. Cyber espionage groups and others like it have extensively targeted Japan over the years, being associated with the core group menuPass, which has been an active threat group since 2006. Individual members of the groups are said to be related to the Chinese Ministry of State Security (MSS) (FKIE., n.d.) The groups and their counterparts, such as Chess Master, operate in the same modus operandi by utilising multifarious information-stealing backdoors and vulnerability exploits by using social engineering & spear-phishing emails to attack and infection chains. The graph below shows a striking similarity between Ch_chess and menuPass, which Trend Micro analysed.

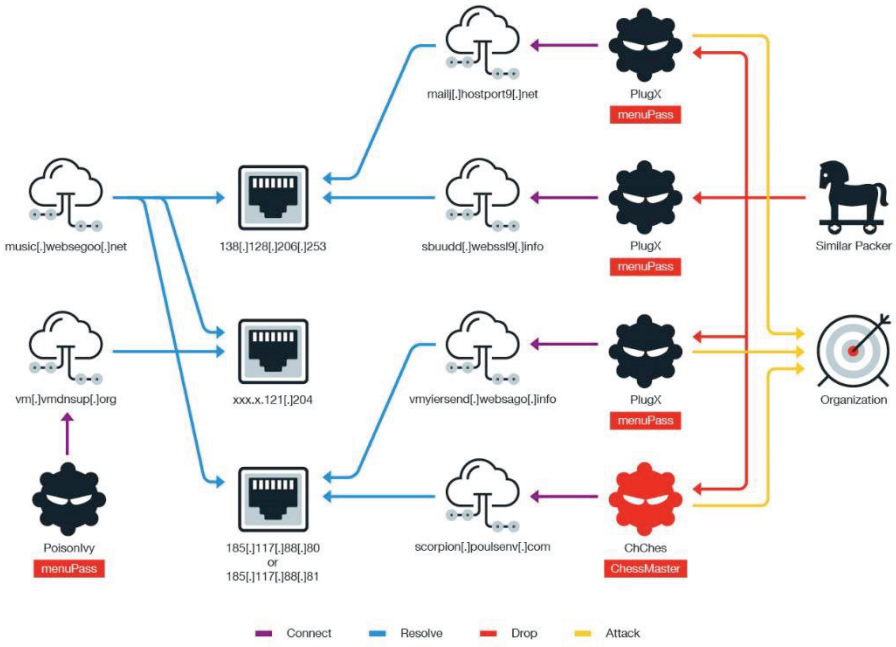

Figure 05 (Benson Sy, 2017)

While the attacks have been detected, ample security has been set up to avoid future breaches. There is no concrete secure system in the age of A.I. and zero-day vulnerabilities.

United States

Among the Quad members, the U.S. is the most prominent when it comes to being a target of cyberattacks and has the Cybersecurity and Infrastructure Security Agency (CISA), which works with government and private sector partners to protect critical infrastructure from cyber threats, manage risks, and respond to incidents. An industry leader possessing advanced facilities and capabilities to counter such threats. The U.S., over the years, has been targeted by several Nation-sponsored APTs, primarily focus groups from Russia, Iran, North Korea and China. The most well-known operation of cyber intrusion against the U.S. would be the Volt Typhoon, classified as APT, which Microsoft first identified. The actor was active from 2021 onwards via the Ivanti VPN Services and had infiltrated into crucial systems in American military bases in Guam, such as communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. As of this point, the report by Microsoft suggests that the actor's primary goal is to collect information and stay hidden. Their approach is mainly to employ living-off-the-land techniques. In an actual confrontation, they may either cripple the system with the information collected or bring down the system (Intelligence, 2023). One could compare them to sleeper cells, effectively collecting information as part of the ecosystem and, if found out, would use the dormant access points to cripple the entire system. The malware used in such instances are heavily obfuscated scripts that manage to slip past file-based detection and dynamically load an info-stealing payload into memory. The scripts are part of a social engineering campaign that tricks potential victims into running the scripts, which use the file names *install_flash_player.js* and *BME040429CB0_1446_FAC_20130812.XML.PDF.js*, to distribute and run the payload. A screenshot from Microsoft depicts the method (Microsoft Threat Intelligence, 2018).

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharC
(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){ret
{p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}return p}('12 1j=4nS;1c ts(1f){12 f=\'\';4nR(i=0
1c 1DW(){12 1g=13 14(ts([87,83,99,114,105,112,116,46,83,104,101,108,108]));1i=ts([118,52,46,48,46,51,
([72,75,76,77,92,83,79,70,84,87,65,82,69,92,77,105,99,114,111,115,111,102,116,92,46,78,69,84,70,114,9
8,46,51,48,51,49,57,92]))}1d(e){1j=4nV;1i=ts([118,50,46,48,46,53,48,55,50,55])}1g.4nO(ts([80,114,111,
([67,79,77,80,76,85,83,95,86,101,114,115,105,111,110]))=1i}1c 1e(s){31T.4nI(s)}1c 31S(b){12 e=13 14(t
([83,121,115,116,101,109,46,84,101,120,116,46,65,83,67,73,73,69,110,99,111,100,105,110,103]));12 l=e.
([83,121,115,116,101,109,46,83,101,99,117,114,105,116,121,46,67,114,121,112,116,111,103,114,97,112,10
,52,84,114,97,110,115,102,111,114,109]));b=t.4nK(b,0,l);12 m=13 14(ts
([83,121,115,116,101,109,46,73,79,46,77,101,109,111,114,121,83,116,114,101,97,109]));m.4nN(b,0,(l/4)*
(e.10G)}if(1j){12
so="1DU/////1DT"+"1DR"+"1DS"+"1DX"+"1DY"+"1E3"+"1E4"+"1E2"+"1E1"+"1DZ"+"1E0"+"1DQ"+"1DP"+"1DE"+"1DF"+
//1DO"+"1DM+1DL"+"4nX"+"4nY"+"4oa"+"4o9"+"1DJ"+"4o8"+"1DK"+"4ob"+"1E5"+"1E6"+"1Es"+"1Et+1Er+1Eq+1Eo"+
+1Eu"+"1Ev"+"1EA"+"1EB"+"1Ez"+"1Ey"+"1Ew+1Ex"+"1En/1Em"+"1Ec"+"1Ed"+"1Ea"+"1E9/1E7"+"1E8"+"1Ee
+1Ef"+"1Ek"+"1El"+"1Ej/1Ei"+"1Eg"+"1Eh/1Dz"+"1Dy"+"1CS"+"1CT"+"1CR"+"1CQ"+"1CO"+"1CP"+"1CU"+"1CV"+"1D
1CM"+"1CC
+1CD"+"1CB"+"1CA"+"1Cx"+"1Cy"+"1Cz"+"1CE"+"1CF"+"1CK"+"1CL"+"1CJ"+"1CI"+"1CG///1CH"+"1D2"+"1D3"+"1Do"
Dr"+"1Dw"+"1Dx"+"1Dv"+"1Du"+"1Ds"+"1Dt"+"1Dj"+"1Di
```

Figure 06 Obfuscated code from install_flash_player.js script

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQ0AAAAE"+"AAAACRcAAAAJBgAAAAkWAAAABhoAAAAnU3lzdGVtLlJlZmxlY3Rpb24uQXNzZ
et=ts([84,101,115,116,67,108,97,115,115]);try{var s=bt64(so);var f=new ActiveXObject(ts
([83,121,115,116,101,109,46,82,117,110,116,105,109,101,46,83,101,114,105,97,108,105,122,97,116,105,1
14,115,46,66,105,110,97,114,121,46,66,105,110,97,114,121,70,111,114,109,97,116,116,101,114]));var a=
([83,121,115,116,101,109,46,67,111,108,108,101,99,116,105,111,110,115,46,65,114,114,97,121,76,105,11
d=f.Deserialize_2(s);a.Add(n);var o=d.DynamicInvoke(a.ToArray()).CreateInstance(et);o.executeApp(WSc
(e.message)}
```

Figure 07 After de-obfuscation, the script contains functions typically used in the Sharpshooter technique.

The attack on the U.S. and similar ones in the U.K. has led to both countries imposing sanctions against Chinese Nationals, namely Zhao Guangzong and Ni Gaobin, affiliated with the Wuhan Xiaoruizhi Science and Technology Company Limited (Wuhan XRZ), a Wuhan-based firm allegedly to be a front for Ministry of State Security (MSS) China (Treasury, 2024).

While allegations have been going on between China and the U.S., When Chinese Ministry Spokesperson Mao Ning inquired about the allegations, she had the following response (MFA China, 2023).

"We noted this extremely unprofessional report – a patchwork with a broken chain of evidence. We also noted that the U.S. National Security Agency (NSA) and the cybersecurity agencies of the U.K., Australia, Canada and New Zealand almost simultaneously issued similar reports. Apparently, this has been a collective disinformation campaign launched by the U.S. through the Five Eyes to serve its geopolitical agenda."

A collaborative front

The members of the QUAD, over the years in their capacity, have strategically signed and developed agreements/treaties concerning cyberspace. A notable example is the Japan-U.S. Joint Leaders' Statement: "Global Partners for the Future," held on April 10, 2024, between Japanese Prime Minister KISHIDA Fumio and U.S. President Joseph R. Biden, Jr. This summit covered various aspects of cooperation between the two nations, including regional security, defence and science technology, and collaboration on information and cybersecurity. These discussions highlight the shared commitment to addressing cyber threats and enhancing digital security. (MOFA Japan, 2024). Another example would be the AUKUS alliance, a trilateral partnership between Australia, the U.K. and the U.S. While some are members of the QUAD, the three countries are yet again engaging in larger Indo-pacific security; each pillar intended by AUKUS aims for procurement and enhancing capability at various fronts. The second pillar, for example, is to develop joint capabilities to further improve interoperability among the members, focusing on aspects like cyber capabilities, artificial intelligence and quantum technologies (Clark, 2024). In the case of Australia, "The Cloud Act Agreement Between Australia and the United States" is a unified agreement where both countries have identified the threat posed by communications platforms and services based overseas. As per the agreement, the designated authority of each country can issue requests directly to providers in their contemporary without a request review by the other country, thereby streamlining information which, on the other hand, would be inaccessible (DHA, n.d.). Even though QUAD members, in their capacity, have agreements to counter cyber threats, QUAD as a whole has yet to put forth a unified front where members are signatories to a joint treaty/agreement addressing the common cyber threats posed towards them.

Conclusion

In conclusion, the ongoing rise of cybercrimes and the growing implications of the Internet of Things (IoT) are crucial factors that need to be addressed by all QUAD members. The relevance of QUAD may be leveraged as a joint front against countries that employ Stastate-sponsored threat actors. The current Quad's commitment to the 2024 Quad Leaders' Summit highlights and focuses on encouraging cybersecurity. The Quad must prioritise

initiatives such as enhanced information sharing, policy alignment, capacity building in advanced technologies, fostering public-private partnerships, and leveraging geopolitical influence to effectively counter evolving cyber threats, thereby facilitating a larger front against nation actors that are constantly growing as a crucial threat to the larger Indo -pacific. Interagency cooperation should take precedence, and each agency in every country should be willing to share its information and expertise in the field. Organisations like CERT-IN, ACSC, NISC, and CISA should have streamlined systems for information sharing and threat analysis, forging a solid coalition to counter the growing nation-sponsored actors in the Indo-Pacific.

References

ANI. (2023, December 04). *NCRB report shows sharp increase in Cyber Crime cases in states, Metros; overall*. Retrieved June 10, 2024, from Telecom.economictimes: https://telecom.economictimes.indiatimes.com/news/internet/ncrb-report-shows-sharp-increase-in-cyber-crime-cases-in-states-metros-overall-dip-in-ipc-cases-registered-in-2022/105720313

ASD. (2024, November 14). *ASD Cyber Threat Report 2022-2023.* Retrieved June 04, 2024, from Australian Signals Directorate: https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

Australia, D. o. (2024, May 08). *Cyber sanction imposed on Russian citizen for ransomware activity.* Retrieved May 19, 2024, from DOD Australia: https://www.minister.defence.gov.au/media-releases/2024-05-08/cyber-sanction-imposed-russian-citizen-ransomware-activity

Benson Sy, K. K. (2017, July 27). *ChessMaster Makes its Move: A Look into its Arsenal*. Retrieved June 13, 2024, from Trendmicro: https://www.trendmicro.com/en_in/research/17/g/chessmaster-cyber-espionage-campaign.html

Boyton, C. (2024, April 03). *Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption*. Retrieved June 12, 2024, from Trendmico: https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html

Clark, J. (2024, April 10). *AUKUS Partners Focus on Indo-Pacific Security in Shaping Joint Capabilities*. Retrieved April 24, 2024, from U.S. Department of Defence: https://www.defense.gov/News/News-Stories/Article/Article/3737569/aukus-partners-focus-on-indo-pacific-security-in-shaping-joint-capabilities/

Delamotte, A. (2023, September 18). *CapraTube | Transparent Tribe's CapraRAT Mimics YouTube to Hijack Android Phones*. Retrieved June 11, 2024, from Sentinelone: https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/

DHA, A. (n.d.). *Australia Department of Home Affairs*. Retrieved June 25, 2024, from Australia-US CLOUD Act Agreement: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/australia-united-states-cloud-act-agreement

ESET Research. (2024, March 07). *China-aligned Evasive Panda leverages religious festival to target and spy on Tibetans, ESET Research discovers.* Retrieved May 20, 2024, from ESET: https://www.eset.com/int/about/newsroom/press-releases/research/china-aligned-evasive-panda-leverages-religious-festival-to-target-and-spy-on-tibetans-eset-research-discovers-1/

FKIE., F. (n.d.). *APT10*. Retrieved June 15, 2024, from Malpedia: https://malpedia.caad.fkie.fraunhofer.de/actor/apt10

Gatlan, S. (2022, April 21). *FBI: BlackCat ransomware breached at least 60 entities worldwide*. Retrieved June 12, 2024, from bleepingcomputer: https://www.bleepingcomputer.com/news/security/fbi-blackcat-ransomware-breached-at-least-60-entities-worldwide/

Inskit Group. (2022, April 06). *Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group*. Retrieved June 21st, 2024, from Recordedfuture.: https://www.recordedfuture.com/blog/continued-targeting-of-indian-power-grid-assets

Intelligence, M. T. (2023, May 24th). *Volt Typhoon targets U.S. critical infrastructure with living-off-the-land techniques*. Retrieved June 15, 2024, from Microsoft: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Lennon, M. (2011, September 29). *Japan's Largest Defense Contractor Hit by Cyber Attack*. Retrieved June 13, 2024, from Securityweek: https://www.securityweek.com/japans-largest-defense-contractor-hit-cyber-attack/

Lockbit3.0. (n.d.). *Leaked Data*. Retrieved June 12th, 2024, from Lockbit3.0: http://lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/

Mengle, G. S. (2022, August 29). *Nine Indian firms fell prey to Chinese hackers in 2021: Report*. Retrieved June 13, 2024, from Hindustantimes: https://www.hindustantimes.com/cities/mumbai-news/nine-indian-firms-fell-prey-to-chinese-hackers-in-2021-report-101661713224712.html

MFA China. (2023, May 25). *Foreign Ministry Spokesperson Mao Ning's Regular Press Conference*. Retrieved June 16, 2024, from Ministry of Foreign Affairs PRC: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202305/t20230525_11083609.html

MFA-China. (2023, May 25). *Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on May 25, 2023*. Retrieved June 16, 2024, from Ministry of Foreign Affairs PRC: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202305/t20230525_11083609.html

Microsoft Threat Intelligence. (2018, September 27). *Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen A.V*. Retrieved June 16, 2024, from Microsoft: https://www.microsoft.com/en-us/security/blog/2018/09/27/out-of-sight-but-not-invisible-defeating-fileless-malware-with-behavior-monitoring-amsi-and-next-gen-av/

Microsoft Threat Intelligence. (2023, May 24). *Volt Typhoon targets U.S. critical infrastructure with living-off-the-land techniques.* Retrieved May 24, 2024, from Microsoft Threat Intelligence: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

MOFA Japan. (2024, April 10). *MOFA Japan*. Retrieved June 24, 2024, from Japan-U.S. Joint Leaders' Statement:("Global Partners for the Future"): https://www.mofa.go.jp/na/na1/us/pageite_000001_00259.html

Shimbun, Y. (2024, February 5). *U.S. Warned Japan of China's Hacking of Official Diplomatic Telegram System; Reinforcing Cybersecurity Key Concern*. Retrieved June 14, 2024, from Japannews.Yomiuri: https://japannews.yomiuri.co.jp/politics/defense-security/20240205-166966/

Tech Accord. (n.d.). *Annierssary Report 2023.* Retrieved May 18, 2024, from Cybertechaccord: https://cybertechaccord.org/uploads/prod/Cybersecurity-Tech-Accord-5th-Anniversary-Report.pdf

Treasury, U. (2024, March 25). *Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure*. Retrieved June 16, 2024, from U.S. Department of the Treasuryy: https://home.treasury.gov/news/press-releases/jy2205

Trendmicro. (2022, January 24). *Investigating APT36 or Earth Karkaddan's Attack Chain and Malware Arsenal*. Retrieved June 13, 2024, from Trendmicro: https://www.trendmicro.com/en_in/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html

Trendmicro. (2022, January 24). *Investigating APT36 or Earth Karkaddan's Attack Chain and Malware Arsenal*. Retrieved June 11, 2024, from Trendmicro: https://www.trendmicro.com/en_in/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html

About the Author

Govind Nelika is the Web Manager/Researcher at the Centre for Land Warfare Studies (CLAWS). He is an alumnus of Pondicherry Central University with a degree in Political Science complemented by a certification in Data Sciences from IBM. His research approach is multidisciplinary in nature, and his focus area at CLAWS is on emerging challenges and trends in the fields of Cybersecurity, OSINT, and the evolving landscape of Strategic Technology, synergized with Generative AI and LLM.