ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

The Commonwealth

Cybercrime in the Asia-Pacific Region: A Case Study of Commonwealth APAC Countries

Olajide O. Oyadeyi[1], Oluwadamilola Adeola Oyadeyi[2] and Rofiat Omolola Bello[3]

Abstract

The Asia-Pacific (APAC) region has witnessed a digital transformation in the past decade. There have been many factors behind this shift, including technological breakthroughs, heightened internet accessibility, evolving consumer patterns and efforts by governmental bodies and enterprises to embrace digital solutions. The region has also become a target for cybercrime as a result of its economic potential, expanding internet presence and comparatively inadequate levels of cyber-resilience. This article discusses the susceptibility of APAC to cyberattacks as well as the way recent events have exacerbated its vulnerability, leading to a need to enhance cyber-resilience within the region.

In response to such attacks, there has been a concerted emphasis on bolstering cybersecurity, fostering collaboration among law enforcement agencies and enacting regulatory measures to address cybercrime and related illicit online activity at both international and regional levels. This has entailed the co-operation of governmental bodies, law enforcement entities, financial institutions, technology corporations and international establishments in enhancing cybersecurity measures, exchanging information on potential threats and implementing more stringent regulations to reduce organised criminal activities in the era of digitalisation. Efforts to mitigate cyber-vulnerabilities are continuously evolving and may vary across different countries within the APAC region. In light of the dynamic nature of the threat landscape, ongoing collaboration and proactive actions to foster cyber-resilience and effectively combat cybercriminal activities are vital.

The relatively large surge in cybercriminal activities in APAC compared with other regions presents considerable obstacles for cybersecurity, law enforcement and the broader security environment in the region. There is a need for a

1 Imperial College Business School. Email: jide.oyadeyi@gmail.com
2 PhD candidate, University of Ibadan, Nigeria. Email: dami.oyadeyi@gmail.com.
3 Oxford Brookes University. Email: orb.bello@gmail.com.

comprehensive strategy encompassing the reinforcement of cybersecurity protocols, the augmentation of law enforcement capacities, the facilitation of international collaboration and the elevation of public consciousness regarding the perils associated with cybercrime.

1. Introduction

The Asia-Pacific (APAC) region has witnessed a digital transformation in the past decade. There have been a number of factors behind this shift, including technological breakthroughs, heightened internet accessibility, evolving consumer patterns and the efforts of governmental bodies and enterprises to embrace digital solutions. On the downside, these innovations have also played a key role in increasing cybercriminal activities in the region.

According to Cybersecurity Ventures (2023), the global cost of cybercrime may rise to US$9.5 trillion in 2024. If not appropriately mitigated, it may rise to 10.5 trillion by 2025 (Cybersecurity Ventures, 2022). If cybercrime were a country, it would have the world's third-largest economy behind the USA and China (ibid.). As cybercriminals do not publicise their operations, for obvious reasons, these estimates are based on recent trends and the exposure of corporations, governments, individuals and businesses to different kinds of cyberattacks.

The APAC region has not been spared from these attacks. The region has become an appealing target for cybercrime owing to its economic potential, expanding internet presence and comparatively inadequate levels of cyber-resilience. APAC was the most attacked of all regions in 2022, accounting for roughly 31 per cent of global cyberattacks (Positive Technologies, 2023). Furthermore, the first quarter of 2023 saw cybercriminal activities globally increase by a staggering 1,835 per cent year on year, with APAC bearing the brunt (Check Point Research, 2023). On average, there were 1,835 new cyber-assaults per organization every week in APAC, far above the global average of 1,248. As a result, the potential for cybercriminal activities in APAC is huge, with a potential cost of roughly US$3.3 trillion by 2025 if we take into account the 31 per cent of global cyberattacks attributed to the region and the potential cost of cybercrime of $10.5 trillion by 2025 (ibid.). Indeed, the APAC region has been called the new 'ground zero' for cybercriminal activities (Gullapali, 2023).

The connection between organised crime groups and cybercrime in the APAC region is complex. Organised crime attackers have been quick to recognise the potential for leveraging the digital domain to facilitate the expansion of their operations.

Questions arise about factors contributing to this increase in cyberattacks in the APAC region and the steps that must be taken to counteract the impending danger they

pose. Within this, it is of use to study recent cybersecurity attacks in APAC; we use the Commonwealth countries in the region to ascertain what can be done to mitigate the risks of attacks and improve cyber-resilience and recovery.

If these trends are not taken seriously, there may be further harm as the number of cyber-users increases. For instance, the growing presence of the Metaverse represents a new opportunity for abuse. The use of chatbots, artificial intelligence (AI) and machine learning (ML) in research and analytics (ChatGPT) holds a great deal of potential but these tools also generate vulnerability, since hackers may employ AI tools for sophisticated assaults. Moreover, deepfakes and other malicious bots are already in use, while the Russian invasion of Ukraine has exposed the vulnerability of critical infrastructure to nation-state threats, such as an increase in distributed denial of service (DDoS) assaults on websites and infrastructure (DDI, 2023). A major example of this has been the hacking of a Ukrainian satellite, which has further shown that countries and governments with highly secretive and covert activities are vulnerable to cyber threats and cyberattacks (ibid.).

In essence, this article analyses the susceptibility of the Commonwealth APAC region to cyberattacks and how recent events such as the COVID-19 pandemic and the proliferation of AI and chatbots may exacerbate this vulnerability. The pandemic-related transition to remote working has amplified online engagement and escalated cybercriminal endeavours. The article also aims to suggest ways of enhancing cyber-resilience within the region.

The focus of this article on the Commonwealth countries within APAC is justified by the increasing convergence between internet usage, internet proliferation and cybercriminal activities in the region. This connection is presenting considerable obstacles for cybersecurity, law enforcement and the broader security environment in the APAC region. Addressing it will necessitate a comprehensive strategy encompassing the reinforcement of cybersecurity protocols, the augmentation of law enforcement capacities, the facilitation of international collaboration and the elevation of public consciousness regarding the perils associated with cybercrime and its connection with other criminal activities.

The article first looks into the context behind cybercrime in the APAC region; the situation post-COVID in terms of the proliferation of cybercrime in the region; the pros and cons of the potential use of AI in cybersecurity; cybersecurity initiatives and strategies in the Commonwealth APAC region; and options for policy consideration.

2. The context of cybercrime in the APAC region

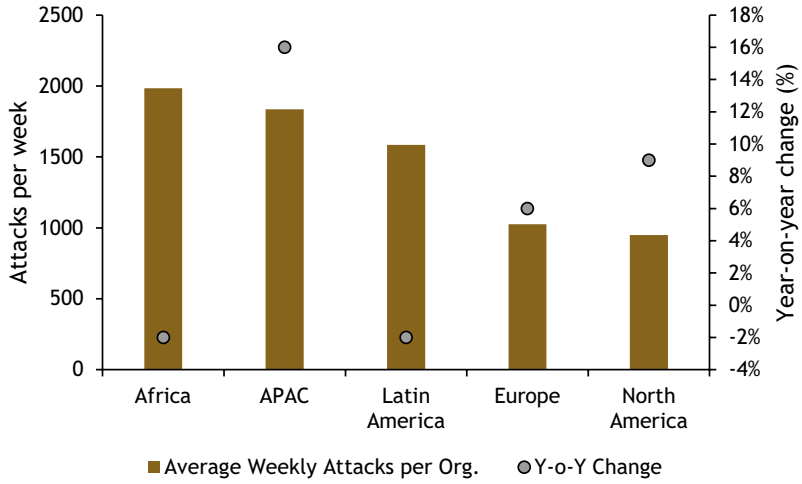
This section provides statistics to support the focus of the article on cyber-vulnerability in the APAC region.

2.1 Average rate of weekly cyberattacks in the APAC region

Even though the African region has the highest average of weekly cyberattacks, Figure 1 shows that the year-on-year percentage change was highest in the APAC region in the first quarter of 2023. This implies that the rate of increase in average weekly cyberattacks in the APAC region was well above that in every other region. For context, the chart also shows that, while it may seem that the African region had the highest number of average weekly attacks, this figure has reduced compared with what it was in the same period of the previous year based on the data collected.

There are a few reasons given for this increasing trend in the APAC region: the trojanising of the 3CXDesktop app for a supply chain attack, the use of ChatGPT for code generation that can help less-skilled threat actors launch cyberattacks without effort, the leveraging of the critical unauthorised remote code exploitation (RCE), and the vulnerability in the Microsoft Message Queuing (MSMQ) service (Gullipalli, 2023).

Figure 1. Average weekly cyberattacks per organisation, by region, Q1 2023

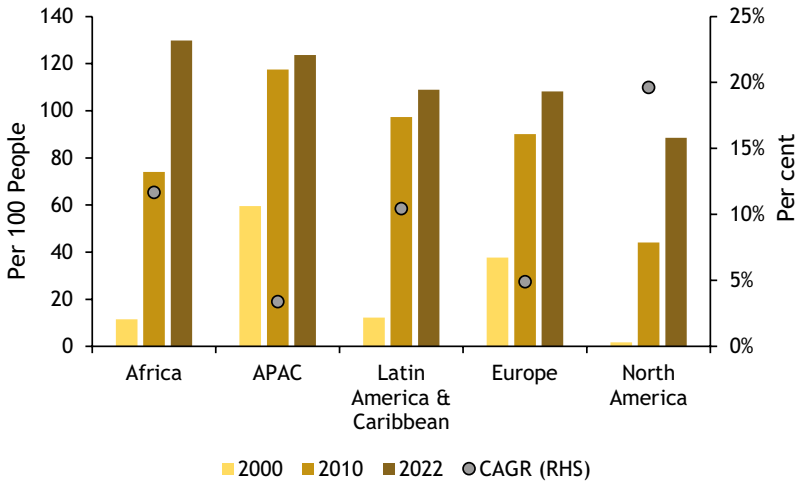


Source: Check Point Research (2023).

2.2 Mobile cellular subscriptions and links to cybercriminal activities

The increase in mobile cellular subscriptions may have contributed to the rise in global cybercriminal activities. Figure 2 reveals that mobile cellular subscriptions expanded significantly in the five regions between 2000 and 2022, with the highest compound annual growth rate (CAGR) found in North America. The results also show that the APAC region had the highest number of mobile cellular subscriptions (per 100 people) in 2010, showing the rising trend in internet activities in the region. However, Africa had the largest

Figure 2. Mobile cellular subscriptions by region (per 100 people)



Source: World Development Indicators 2023.

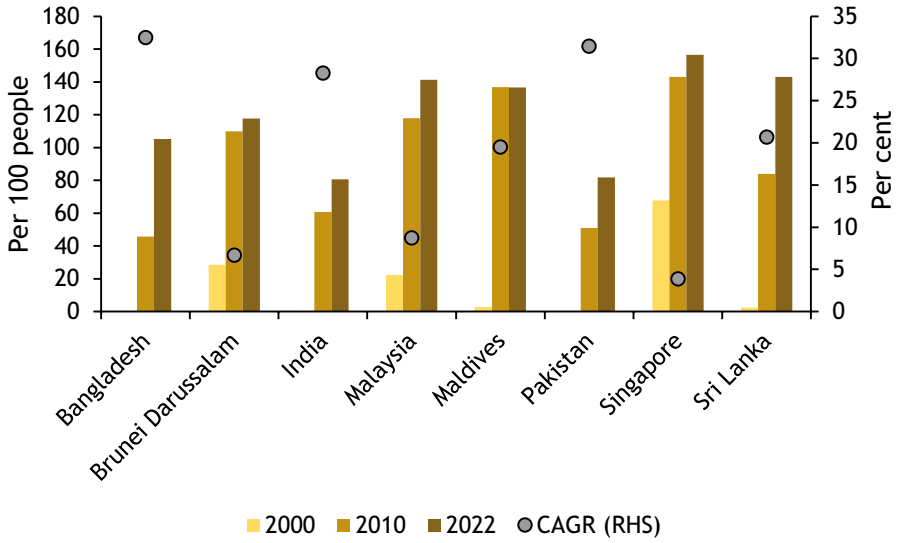
number in 2022, at an average of roughly 130 per 100 people, slightly higher than the APAC region's 124 per 100 people.

The number of mobile cellular subscriptions shown in Figure 2 is likely linked to the average weekly cyberattacks in Figure 1. For example, Africa has the largest number of mobile cellular subscriptions per 100 people, as presented in Figure 2, and at the same time the largest average number of weekly cyberattacks, as shown in Figure 1. This implies that the rise in mobile cellular subscriptions may have led to the rise in weekly cyberattacks, with the APAC region suffering a large chunk of these.

Figures 3 and 4 take the analysis a step further by comparing the Commonwealth APAC countries' performance in terms of their cellular subscriptions over the internet. Interestingly, the findings demonstrate that, even though Singapore has the highest number of mobile cellular subscriptions per 100 people among the Commonwealth Asian countries (Figure 3), the gap is not as wide as we might think: the other Commonwealth countries in the region closed the gap over the 22-year period. As a result, Bangladesh and Pakistan had the highest CAGR in mobile cellular subscriptions per 100 people between 2000 and 2022 and Singapore had the lowest. Nevertheless, the data show that all the countries have embraced connectivity through the use of mobile phones and gadgets to gain access to the internet. Reasons for this include the reduced cost of internet subscriptions on mobile devices, more individuals embracing mobile usage across different age groups and a rise in e-commerce (Brain and Oyadeyi, 2023).

The Commonwealth Pacific region has also witnessed a surge in mobile cellular subscriptions. Figure 4 shows that New Zealand, Australia and Fiji had the highest number of mobile cellular subscriptions per 100 people and Papua New Guinea and Kiribati the lowest.

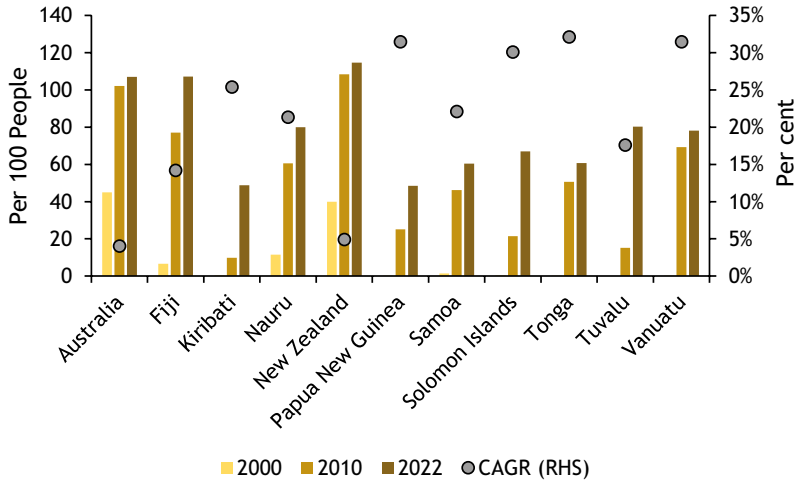
Figure 3. Mobile cellular subscriptions among Commonwealth Asian countries (per 100 people)



Source: World Development Indicators 2023.

In general, these findings imply that the Commonwealth APAC region is making significant strides in its use of mobile cellular subscriptions whether for good or for bad reasons. 'Good' reasons include the fast-paced development in information and communication technology (ICT) and 'bad' reasons include the potential for

Figure 4. Mobile cellular subscriptions among Commonwealth Pacific countries (per 100 people)



Source: World Development Indicators 2023.

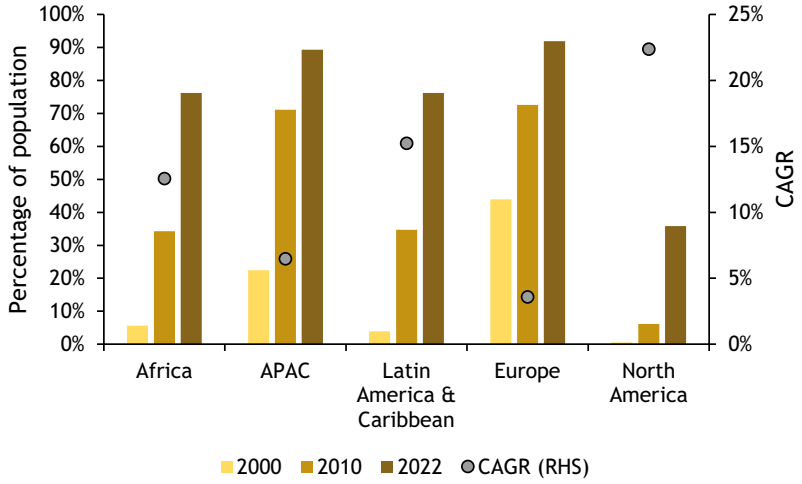
cybercriminals to use such subscriptions to access the internet and target their victims, unlike in the early 2000s, when such activities were performed only using desktops and laptops. Now, with a mobile, cybercriminals can easily access victims to defraud.

Therefore, cybercrime is a particular concern in the Commonwealth APAC region because of the prevalence of internet access on mobile phones. Unlike PCs, mobile phones often lack protective measures like firewalls, antivirus software, encryption and so forth. These heightened possibilities, coupled with the region's inadequate legal framework for cybercrime, make it a prominent target for cybercriminals and their activities.

2.3 Internet penetration and links to cybercriminal activities

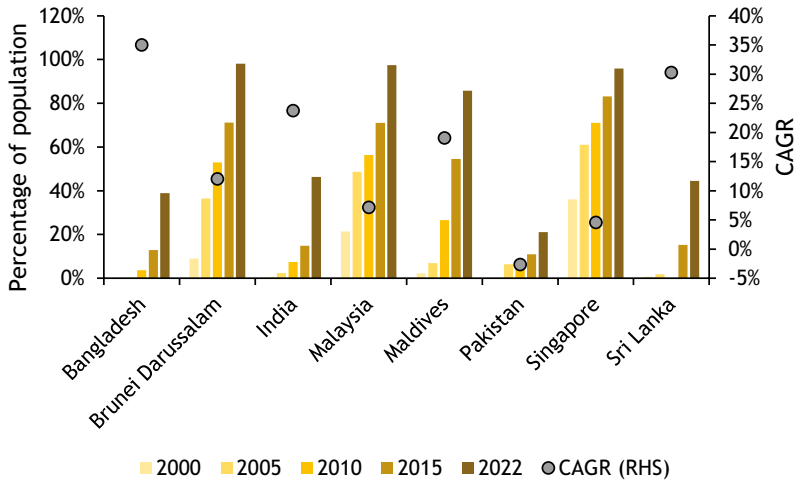
The proliferation of digital technology in the Commonwealth APAC region has resulted in heightened connectivity and a growing dependence on digital infrastructure (Runde et al., 2020). The level of internet penetration within the APAC region ranks high; only Europe rivals (or ranks higher than) the APAC region when it comes to internet use as a percentage of the population. In figures, roughly 89 per cent of the population in the APAC region uses the internet, which is the second highest internet penetration use, beneath only Europe, which has roughly 92 per cent usage. This shows that ICT development within the region is advanced and has been higher than in most other regions except Europe. Weak legislation on cybercriminal activities has also potentially helped cybercriminal activities over the internet proliferate: Figure 1 shows that the region sees the highest number of average weekly cyberattacks globally.

Figure 5. Individuals using the internet by region (% of population, and compound annual growth rate [CAGR])



Source: World Development Indicators 2023.

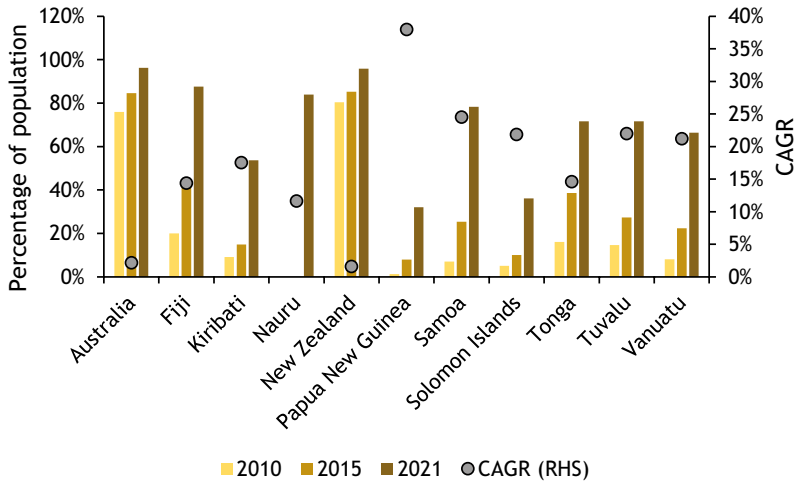
Figure 6. Individuals using the internet in Commonwealth Asian countries (% of population, and compound annual growth rate [CAGR])



Source: World Development Indicators 2023.

In 2022, Brunei Darussalam, Malaysia and Singapore had the highest share of people using the internet in Commonwealth Asia, at 98, 97 and 96 per cent of the population, respectively (Figure 6). The figures were the lowest in India (46 per cent), Bangladesh (39 per cent) and Pakistan (21 per cent). Therefore, from Figure 6, we can see that Brunei Darussalam, Malaysia, Singapore, and Maldives, are the key driving forces behind the

Figure 7. Individuals using the internet in Commonwealth Pacific countries (% of population, and compound annual growth rate [CAGR])



Source: World Development Indicators 2023.

Commonwealth Asian region's internet penetration of 89 per cent in Asia as illustrated in Figure 5.

Figure 7 shows internet penetration as a share of the population in Commonwealth Pacific countries. Australia (96.2 per cent), New Zealand (95.9 per cent) and Fiji (88 per cent) have the highest rate and Kiribati (54 per cent), Solomon Islands (36 per cent) and Papua New Guinea (32 per cent) had the lowest in 2021.

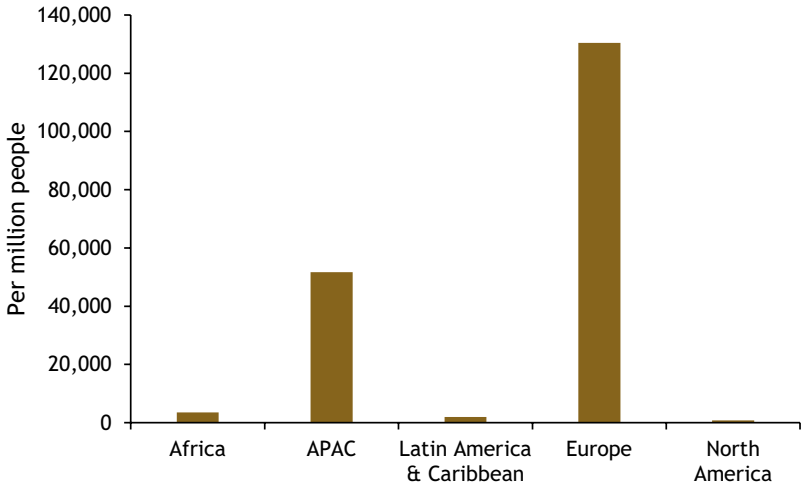
2.4 Internet server security and links to cybercriminal activities

Figure 8 shows how successful each region has been in enforcing stringent cybercrime policies. Europe has the most secure internet users in the world. That is, for every 1 million people, 130,402 persons have secure access to the internet or roughly 13 per cent of the population. This rate is low but still the highest of all regions. Europe's position may be linked to the high presence of cybercriminal laws and regulations, as well as stringent penalties for anyone caught engaging in cybercriminal activities.

The APAC region comes in second at roughly 52,000 secure internet users per 1 million people or roughly 5.2 per cent of the population in the region. However, many of the countries driving these numbers are not Commonwealth APAC countries (Table 1). Finally, Africa, Latin America and the Caribbean, and North America have extremely low figures per 1 million people.

Table 1 sheds more light on the information provided in Figure 8 on the APAC region. Among Commonwealth Asian countries, Singapore had the highest rate of secure

Figure 8. Secure internet servers by region (per million people)



Source: World Development Indicators 2023.

Table 1. Secure internet servers in Commonwealth APAC countries (per 1 million people)

Asian countries	2010	2015	2020	CAGR	Pacific countries	2010	2015	2020	CAGR
Bangladesh	0	2	138	92%	Australia	1,403	4,574	39,853	40%
Brunei Darussalam	40	565	15,598	81%	Fiji	14	86	259	34%
India	2	12	474	76%	Kiribati	0	9	40	20%
Malaysia	44	228	7,306	67%	Nauru	0		325	35%
Maldives	25	122	1,124	46%	New Zealand	1,389	3,921	20,509	31%
Pakistan	1	3	72	63%	Papua New Guinea	1	13	52	49%
Singapore	532	3,585	128,378	73%	Samoa	26	123	475	34%
Sri Lanka	3	21	384	60%	Solomon Islands	2	21	62	42%
					Tonga	9	104	561	51%
					Tuvalu			271	72%
					Vanuatu	41	123	359	24%

Source: World Development Indicators 2023.

internet servers in 2020, at roughly 13 per cent of the population. This was followed by Brunei Darussalam, at roughly 1.6 per cent. The rest of the Commonwealth Asian countries had a rate of less than 1 per cent, meaning that public and private organisations and investors need to put more emphasis on building secure internet servers within the region. Based on these figures, the potential for businesses that want to delve into creating a secure cyberspace is huge; likewise, the potential for cybercriminals to perpetrate their activities is also huge, as many people in Commonwealth Asian countries are not using a secure internet connection and this makes them vulnerable to cyber-scams, attacks and threats.

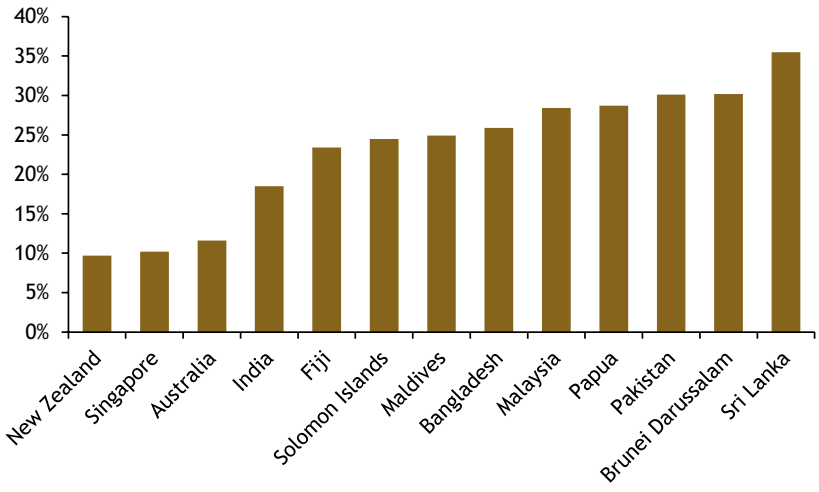
In the Commonwealth Pacific countries, only about 4 per cent of people in Australia use the internet securely, and only about 2 per cent in New Zealand. The rest of the Commonwealth countries in this region do not reach 1 per cent.

Overall, these figures highlight a huge gap in infrastructure for many Commonwealth countries and enormous susceptibility to cyberattacks.

2.5 The shadow economy and the APAC region

The underground economy can be described as all economic activities that are hidden from official authorities for monetary, regulatory and institutional reasons (Medina and Schneider, 2019). Reasons may include tax avoidance, corruption and weak institutions or regulatory frameworks. Figure 9 shows that the shadow economy is largest in Sri Lanka (35.5 per cent), Brunei Darussalam (30.2 per cent) and Pakistan (30.1 per cent). This implies that the size of the shadow economy compared with overall economic activities in these countries is huge, at over a third in Sri Lanka and at a little less than a third in Brunei

Figure 9. Shadow economy (% of GDP) in the Commonwealth APAC region



Source: Medina and Schneider (2019).

Darussalam and Pakistan. On the other hand, New Zealand (9.7 per cent), Singapore (10.2 per cent) and Australia (11.6 per cent) have the least informal economies in the Commonwealth APAC region. This points to the level of development in these countries and the high level of regulatory frameworks guiding against underground activities.

In essence, the high level of cybercriminal activities in the Commonwealth APAC region (as presented in Figure 1) may relate to the level of underground activities going on (Figure 9). This is particularly so in countries that have higher shadow economy levels and a weaker secure internet server situation (as presented in Table 1), such as Papua New Guinea, Brunei Darussalam and Pakistan, to mention a few. Consequently, a larger shadow economy is a concern for the Commonwealth APAC region, since it may aid cybercriminal activities.

3. Post-COVID situation and cybercriminal activities in the APAC region

The COVID-19 pandemic had a significant impact on the cybercrime landscape in the APAC region (Germanos and Georgiou, 2021). It led to a rise in the reliance on AI-based technologies for work, education and entertainment (Khan et al., 2022). The heightened dependence on digital technology during the pandemic engendered new prospects for cybercriminals while at the same time intensifying pre-existing susceptibilities. Consequently, there was a notable increase in cyberattacks inside the APAC region, affecting various entities both public and private organisations as well as individuals (Christine and Thinyane, 2020; Singh, 2022).

Key trends in cybercrime in the Commonwealth APAC region post-COVID include the following.

Increase in phishing and malware attacks

Phishing and malware attacks are among the most common types of cyberattacks, and they have become significantly more frequent since the pandemic (Lallie et al., 2021). Cybercriminals are using phishing emails and websites to trick individuals into revealing their personal information or clicking on malicious links (Alkhalil et al., 2021). Malware is also being used to infect devices with ransomware, which can encrypt data and demand a ransom payment. There has been a substantial increase in the occurrence of phishing attacks and data breaches among Commonwealth APAC countries. For instance, the Tasmanian education department in Australia was the victim of a cyberattack that led to the exposure of roughly 30,000 documents on the dark web, many of which contained sensitive personal information of schoolchildren. Both Australian and New Zealand citizens were victims of the Latitude Financial attack in Australia, which affected over 14 million customers. In Bangladesh, over 14 million details were breached through the Office of the Registrar General. The objectives of these attacks were not only the acquisition of financial benefits but also the deliberate disruption of vital services and the exploitation of confidential information (Smail, 2023).

Rise in ransomware attacks

The emergence of ransomware has resulted in significant monetary damage and the disruption of essential services within diverse industries (Laitinen and Armstrong-Smith, 2022). Ransomware attacks in the APAC region encompass the unauthorised penetration of computer systems or networks, wherein sensitive data is encrypted and a ransom is subsequently demanded in exchange for the provision of decryption keys (Dimitrov, 2020; Amankwah-Amoah et al., 2021; Skouby et al., 2022). The APAC region has experienced a significant rise in both the number and the severity of these attacks, especially since the pandemic. In addition, the pandemic expedited the adoption of remote work practices, which increased dependence on digital platforms (Amankwah-Amoah et al., 2021), making many firms vulnerable to ransomware attacks.

Within Commonwealth APAC countries, Australian commercial law firm HWL Ebsworth has been a victim of ransomware attacks (Smail, 2023). Singapore's Cyber Security Agency reported 8,500 cases of phishing attempts in 2022, a rise from 3,100 cases in 2021 (Chakravarti, 2023). Also, an Indian cybersecurity firm exposed plans by cybercriminals originating from Indonesia and Pakistan to disrupt the G20 summit in India using distributed denial of service (DDoS) attacks and mass defacement. According to the Centre for Strategic and International Studies (CSIS), Bangladesh shut down access to its central bank and commission website in 2023 when it received information that an Indian group was trying to hack it, similar to the hack that happened in 2016 that cost the country almost $1 billion (CSIS, 2023). A Pakistani-based hacker group infiltrated the Indian army and education sector in a wave of attacks against Indian government institutions (ibid.).

Finally, geopolitical factors have also served as potential catalysts for cyberattacks. The use of cyber-tools for purposes of disruption or espionage has been observed during Russia's war on Ukraine (Solar, 2023). Actors now utilise advanced strategies including double extortion, which involves the threat of leaking sensitive data if the ransom is not paid (Ryan, 2021). This strategy puts pressure on victims to comply.

Targeting of critical infrastructure

The deliberate targeting of critical infrastructure by cybercriminals presents an increasing danger, particularly to critical sectors of the economy, such as healthcare, electricity, transportation and telecommunications (Mizrak, 2023). The strategies cybercriminals have employed in targeting critical infrastructure have exhibited a notable enhancement in sophistication. Threat actors utilise sophisticated techniques like ransomware, supply chain attacks and zero-day exploits to infiltrate systems (Diogenes and Ozkaya, 2019; Xu et al., 2021). Incidents targeting healthcare systems pose a significant threat to patient care as they disrupt critical medical services and compromise the security of confidential patient information (Argaw et al., 2020). These disturbances not only impede prompt medical attention but also present potential long-term hazards to patient safety and confidentiality. Cyberattacks also pose significant threats to energy systems, which are crucial for providing power to urban areas and facilitating industrial operations (Zhao et al., 2021).

Commonwealth APAC region countries affected by these types of cybercriminal activities include Malaysia and Singapore, among others (Commonwealth Secretariat, 2022).

Exploitation of remote work vulnerabilities

The pandemic mandated a swift transition to telecommuting in various sectors. This sudden shift resulted in numerous organisations being exposed to potential risks, as they hastily attempted to modify their infrastructure to facilitate remote accessibility (Dwivedi et al., 2020). The transition has led to an increase in cyber-vulnerabilities, rendering organisations more prone to cyberattacks. Cybercriminals in the APAC region have exploited these vulnerabilities by utilising remote access points, specifically targeting home networks lacking security measures and employing social engineering strategies to gain unauthorised access to business systems (Aslan et al., 2023).

4. The link between AI and cybersecurity and the role of AI in building cyber-resilience

In recent years, the incorporation of AI into various digital services has experienced continuous and extensive growth. Governments around the world are currently contemplating the implementation of AI systems to assist in a multitude of endeavours, such as the identification and prediction of criminal activities (Engstrom et al., 2020). National security and intelligence organisations acknowledge the potential impacts of AI in achieving cyber-resilience and public cyber-safety (Schmidt et al., 2021). Nevertheless, if the advancement of AI technology (such as face recognition, drones and lethal autonomous weaponry) is not appropriately regulated or supervised, it presents risks to the protection of individual rights and liberties (Ala-Pietilä and Smuha, 2021).

AI and ML have promising prospects for the identification and mitigation of cyberattacks targeting essential sectors of critical infrastructure in the APAC region. Despite this, issues remain regarding its legislation, particularly for small and medium enterprises (SMEs) whose funds for cybersecurity are constrained. Cybercriminals use AI to create and carry out targeted attacks against government entities, businesses and people. Although there is currently a lack of substantial proof regarding cybercriminals possessing extensive technical knowledge in AI manipulation, they are aware of its potential for illicit and disruptive activities (Caldwell et al., 2021). The current trends in cybercrime underscore a growing dependence on the Internet of Things (IoT) for the dissemination of malware, as well as the utilisation of AI to enhance ransomware attacks (Cascavilla et al., 2021). The anticipated growth of this phenomenon is projected to coincide with the rapid proliferation of interconnected gadgets, potentially heightening the susceptibility of both businesses and individuals to cybercriminal activities.

Moreover, the emergence of deepfakes has raised substantial concerns within the realms of national politics and law enforcement, as these have the potential to facilitate

fraudulent acts using impersonation (van der Sloot and Wagensveld, 2022). According to a report by The Asset (2023), the APAC region experienced a 1,530 per cent surge in deepfake cases from 2022 to 2023 amid a growing trend in sophisticated scams and money laundering cases globally, with Commonwealth countries such as Bangladesh (5.44 per cent) and Pakistan (4.59 per cent) the biggest culprits. The report further showed that Singapore, another Commonwealth country in the region, stands out compared with many other countries in APAC, maintaining a low level of 0.89 per cent. Australia has also been able to maintain a low rate, of 2 per cent, despite increased incidents within the region. The use of deepfakes has presented law enforcement agencies with hurdles to climb as a result of the intricate legal considerations involved in cross-border investigations.

How can AI be deployed to foster cyber-resilience? AI has emerged as a pivotal tool in addressing cybersecurity threats by employing ML to monitor and track illegal and malicious activities within similar digital environments (Zeadally et al., 2020). AI-based security systems play a crucial role in distinguishing between 'good' and 'bad' behaviour but more advanced iterations can analyse vast datasets, identifying interconnected activities that may indicate suspicious behaviour by anonymous entities. The proliferation of network computers, the internet and mobile applications has led to a rise in diverse and prevalent cyberattacks, particularly through connected devices with insufficient security measures, exacerbated by the expansion of the IoT. This surge in cybercrime has highlighted the limitations of traditional 'signature-based' cybersecurity methods (Zhang et al., 2022). These conventional approaches require substantial human effort to identify risks, develop risk features and integrate threat characteristics into software, often falling short of addressing modern, complex cyberattacks, which is an area where AI can effectively be used to boost cyber-resilience.

Furthermore, the concept of CAPTCHA exemplifies the intersection between AI and cybersecurity, requiring users to identify distorted letters or images as a test to distinguish between humans and computers (Al-Maliki et al., 2023). When conventional security systems prove ineffective against evolving threats, AI-driven approaches enhance the overall security architecture, offering robust protection against a diverse range of intricate cyberattacks. Companies integrating AI into their operations witness improved business processes and financial outcomes, particularly through AI-powered cybersecurity solutions that swiftly develop data-driven security models across various domains (Allioui and Mourdi, 2023). This is because AI-based monitoring systems continuously track user behaviour, promptly identifying anomalies, providing a significant advantage in today's dynamic cybersecurity landscape (Zeadally et al., 2020). In essence, AI and ML technologies serve as effective anti-malware defences against sophisticated cybercriminal tactics such as camouflaging malware and ransomware to evade detection (Ferdous et al., 2023). These technologies enable systems to cross-reference new malware with existing databases, assess code and pre-emptively prevent potential attacks, even when malicious code is concealed within large volumes of benign or irrelevant data.

5.1 How international and national legal measures have helped combat cybercrime

One major impact of regional and national legal frameworks in the APAC region is the creation of vast awareness of the dangers of cyberattacks and the ways to mitigate such attacks. The various frameworks put in place by many of these countries have created cyber-awareness among government institutions, business owners and individual users. Australia, for example, has avenues for training in cyber-awareness on protecting emails, personal phones and online transactions (ASD, 2024). India has an incident report framework giving a duration within which cyberattacks must be reported to the appropriate agency. Cases of business email compromise (BEC) are on the rise; the case on BEC heard at the ACT Civil and Administrative Tribunal (ACAT) is one such cyberattack incident (ibid.). The Australian Court puts the responsibility on companies to protect their systems to prevent the future occurrence of BEC when dealing with clients and other businesses (Falk, 2022).

5.2 Gaps in national laws and the regional or international legal framework

The United Nations Office on Drugs and Crime noted that the Commonwealth of Independent States' CIS Agreement on Cooperation in Combating Offences Related to Computer Information of 2001 calls on countries to adopt national laws to implement the Agreement's provisions to harmonise their national cybercrime laws (UNODC, 2019). Singapore, Australia and New Zealand are some of the top Commonwealth APAC countries in terms of formulating cybersecurity strategies, establishing computer emergency response teams (CERT), creating governmental agencies and enacting laws to protect their critical information infrastructure, economy, businesses and people from incessant cyberattacks while paying attention to international frameworks such as the CIS Agreement and to UNODC, Council of Europe and EU cybersecurity policies.

The Association of Southeast Asian Nations (ASEAN) is another example of regional co-operation on cybersecurity in APAC. The focus of ASEAN is threefold: ensuring member states make provision for (i) cybersecurity incident response; (ii) CERT policy and co-ordination; and (iii) cybersecurity capacity-building (ASEAN, 2017).

There are gaps in the regional framework of ASEAN and in the national strategies of these countries (Gan, 2024). Also, the APAC region has uneven cybersecurity development (ASEAN Cyber Security Cooperation Strategy, 2021). Singapore and Australia have more legal and judicial frameworks in place than countries such as Kiribati, Solomon Islands and Tuvalu. India's cybersecurity legislation has not been updated recently, and Malaysia has unspecialised cybersecurity legislation (Positive Technologies, 2023).

Table 2. Major cyberattacks in the APAC region in 2023

Institutions	Date	Country	Affected
Tasmanian Education Department	April 2023	Australia	30,000 documents
Samsung ChatGPT incident	April 2023	APAC	Company and all Samsung users
Toyota cyberattack	May 2023	APAC	Over 2 million customers
Latitude Finance	March 2023	Australia	14 million customers
Bangladesh Registrar General cyberattack	July 2023	Bangladesh	14 million citizens
Tissupath Clinic attack	August 2023	Australia	10 years' worth of data breached

Source: Smail (2023).

5.3 Cybersecurity incidents, court judgements and sanctions

The APAC region has experienced several cyberattacks and has been labelled highly vulnerable to cybercriminal activities. The Medibank Group cyberattack of October 2022, the Optus Pty Limited cyberattack and the Costa Group cyberattack were some of the many devastating cyberattacks in the APAC region in 2022. The Medibank cyberattack led to the exposure of 9.7 million customers' data. Table 2 presents major cyberattacks occurring in the Commonwealth APAC region in 2023.

These cyberattacks have led to several sanctions. For instance, the Australian government sanctioned Aleksandr Ermakov, who was linked to the Medibank cyberattack. It has been deemed criminal for anyone to use or deal with Aleksandr Ermakov's assets, cryptocurrency wallet and ransomware payments, with a 10-year imprisonment or heavy fines imposable (Wong et al., 2024).

Australia also saw some court judgments delivered in cyberattack cases at the Federal Court and the ACAT. In 2020, the Australian Security and Investments Commission (ASIC) instituted an action against RI Advice Group at the Federal Court. The action was instituted owing to RI Advice Group's lack of documented cybersecurity measures to protect its client's information, leading to losses for its clients for six years. The company was penalised to the tune of AU$750,000, to be paid to ASIC as compensation (Falk, 2022). These sanctions have helped solidify the Australian authority's efforts in the fight against cybercriminal activities; other Commonwealth countries in the APAC region that are yet to make strong cybercriminal legislation can adopt such measures.

5.4 Relevance of regional and international co-operation in fighting cybercrime

The transnational nature of cyberthreats means regional and international co-operation play a crucial role in combating cybercrime. In the APAC region, several organisations play a crucial role in tackling cybercrime and enhancing cybersecurity (Benincasa, 2020). These include the Asia-Pacific Computer Emergency Response Team**,** Interpol Global Complex for Innovation**,** ASEAN's Cyber Capacity Programme, Asia-Pacific Telecommunity, Asia-Pacific Economic Cooperation's Telecommunications and Information Working Group, Asia-Pacific Network Information Centre, Asia-Pacific Regional Internet Governance Forum and Asia-Pacific Security Forum. These agencies foster collaboration, share expertise and promote best practices in cybersecurity (Sarowa et al., 2020). Their relevance in the APAC region in fighting cybercrime is briefly discussed in the subsections below.

Information-sharing and co-ordination

Regional organisations serve as platforms for member states to share threat intelligence, cyber-incident data and best practices in cybersecurity (Rui, 2023). By facilitating information exchange and co-ordination, they contribute to a more effective global response to cyberthreats (Sarowa et al., 2020).

Capacity-building and training

Regional organisations enhance the skills and capabilities of cybersecurity professionals in member states (Quimba and Barral, 2022). By investing in human resources development and knowledge-sharing, they contribute to building a global network of cyber-experts equipped to address evolving cyberthreats (Kumar, 2020).

Harmonisation of cyber-policies

Regional organisations work towards harmonising cybersecurity policies, standards and frameworks across member states. By promoting policy coherence and alignment on cybersecurity issues, they contribute to a more unified approach to combating cybercrime at the international level (Tien and Cheng, 2016).

Promotion of international cyber-norms

Regional organisations advocate for the adoption of international cyber-norms, principles and best practices to promote responsible behaviour in cyberspace (Herko, 2023). By endorsing global cybersecurity standards and norms, they contribute to a more secure and stable international cyber-environment (Ang, 2021).

Collaboration with international partners

Regional organisations engage in partnerships and collaborations with international entities, such as INTERPOL, the United Nations and other global organisations (Araki,

2022). In doing so, they contribute to a co-ordinated and comprehensive global response to cyberthreats (Rui, 2023).

Advocacy for cyber-resilience

Regional organisations advocate for cyber resilience and the importance of cybersecurity at the international level (Herko, 2023). By raising awareness, promoting good governance and advocating for cybersecurity measures globally, they contribute to strengthening the overall resilience of the international community against cybercrime (Slayton and Clarke, 2020).

Contribution to global cybersecurity initiatives

Regional organisations actively participate in global cybersecurity initiatives, conferences and forums to share insights, experiences and expertise on cybercrime prevention and response (Ang, 2021). In this way, they play a vital role in shaping international cybersecurity agendas and strategies (Bahuguna et al., 2020).

5.5 Challenges in enforcing legal provisions on cybercrime at the regional level

Enforcing legal provisions on cybercrime in the APAC region faces several challenges to the effective prosecution and deterrence of cybercriminal activities.

Jurisdictional issues

Cybercrimes are often transnational, making it challenging to determine jurisdiction and prosecute offenders operating across multiple jurisdictions (Quimba and Barral, 2020). Lack of clear legal frameworks for cross-border co-operation and extradition complicates the enforcement of cybercrime laws in the region (Araki, 2022).

Lack of harmonised legislation

Variations in cybercrime laws and regulations among countries in the APAC region create inconsistencies and gaps in legal frameworks (Kumar, 2021). The absence of harmonised legislation hampers international co-operation and co-ordination in combating cybercrimes effectively (Araki, 2022).

Capacity and resourcing difficulties

Many countries in the region face resource constraints, including on funding, technical expertise and specialised cybercrime units (Tien and Cheng, 2016). This hinders law enforcement agencies' ability to investigate cybercrimes, gather digital evidence and prosecute offenders (Roberts, 2022).

Technological challenges

Rapid technological advancements present challenges for law enforcement agencies in keeping pace with evolving cyberthreats (Ang, 2021). Cybercriminals often use sophisticated techniques and encryption methods to conceal their activities, making it difficult for authorities to detect and investigate effectively (Herko, 2023).

Data privacy concerns

Balancing the need for law enforcement access to digital evidence with data privacy rights poses a significant challenge in enforcing cybercrime laws (Sarowa et al., 2022). Striking a balance between investigating cybercrimes and protecting individuals' privacy rights is a complex issue that requires careful consideration and legal safeguards (Benincasa, 2020).

Cross-border co-operation

Effective enforcement of cybercrime laws requires close co-operation and information-sharing among law enforcement agencies across borders (Sarowa et al., 2022). Challenges such as differing legal systems, language barriers and cultural differences can impede seamless collaboration in combating transnational cybercrimes (Bahuguna et al., 2020).

Inadequate cybersecurity capacity-building

Building the technical capabilities and expertise of law enforcement agencies to investigate cybercrimes is essential for the effective enforcement of legal provisions (Kumar, 2021). A lack of specialised training programmes and cybercrime units in some countries hinders their ability to respond to and investigate cyber-incidents.

Difficulties in setting up public–private partnerships

Collaboration between government agencies, private sector entities and civil society organisations is crucial in combating cybercrime (Slayton and Clarke, 2020). However, establishing effective public–private partnerships and information-sharing mechanisms can be challenging owing to concerns about data protection, trust issues and differing priorities (Ang, 2021).

The need for legal framework adaptation

Cyberthreats evolve rapidly, with continuous updates and adaptations to existing legal frameworks required to address emerging challenges (Araki, 2022). The process of revising laws and regulations to keep pace with technological advancements can be slow and complex, delaying the enforcement of legal provisions on cybercrime (Kumar, 2021).

6. Efforts toward the enforcement of cybersecurity laws to build cyber-resilience

To combat cybercrime, the Commonwealth APAC countries have adopted different national strategies.

6.1 Asia region

Singapore

Singapore launched its first Cybersecurity Strategy in 2016 and updated this in 2021 to develop a vibrant cybersecurity ecosystem and grow a robust cyber talent pipeline. Singapore has laid out three pillars – 'build resilient infrastructures,' 'enable safe cyberspace' and 'enhance international cyber co-operation' – to accomplish its goals. The Cyber Security Act of 2018 is one of the laws passed to put this into action. The Cyber Security Agency (CSA) has been established to manage the establishment of a cyberthreat response team and the development of cyberspace awareness initiatives for organisations, companies and people. Other government departments receive security consultation services from CSA. Given the global nature of cybercrime, CSA actively promotes international and regional capacity-building initiatives with other nations (CSA Singapore, 2023). Cybercrime monitoring, and policy generation within existing regulatory frameworks for implementation by various financial institutions, payment platforms and the general public, is a primary function of Singapore's Monetary Authority.

Brunei Darussalam

Brunei Darussalam has formed Cyber Security Brunei (CSB). Despite being a government body, this assists both public and private entities in their fight against cybercrime. CSB raises public awareness of cybercrime, develops policies to deal with cyber-risks and plans to strengthen the national enforcement agency's enforcement capabilities (ibid.). Brunei's Computer Emergency Response and the National Digital Forensic Laboratory are the ways by which they carry out their mandate. CSB has rules and regulations pertaining to cybercrime, including the Cyber Security Order 2023 and the National Cybersecurity Framework, which provide organisations with standards, guidelines and protocols to fight cybercrime.

India

India has purposefully established a multistakeholder ecosystem to handle cybercrime. The National Cyber Security Strategy, launched in 2013, with a revamp in 2023 (in its final stages of approval) aims to help raise awareness about cybercrime, educate the public on data protection, develop strategies to prevent cyberattacks and bring those responsible to justice (Inamdar, 2023). The strategy will help agencies including the National Cybercrime Reporting Portal, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory and National Cybercrime Threat Analytics Unit.

The country's National Cyber Crime Research and Innovation Centre keeps an eye out for emerging cybercrime trends and develops strategies to combat them.

Malaysia

To ensure the safety of its critical and national information infrastructure, Malaysia established the National Cyber Security Agency (NACSA) in 2017 and created the National Cybersecurity Strategy in 2020. Its cybersecurity strategy plan spanning the years 2020–2024 is built around five main pillars: (i) efficient administration and control; (ii) increasing the robustness of law enforcement; (iii) facilitating first-rate innovation, technology, research and development, and business; (iv) improving awareness, education and capacity-building; and (iv) building international co-operation. The tenets of these pillars include legislation, awareness-raising initiatives, cyberthreat agencies and enhanced cyberattack prevention measures.

Maldives

Cybersecurity Maldives was established in 2013 with the mandate of performing security audits, assessing network threats and developing solutions for cyberthreat hunting. In addition to assisting businesses and organisations in preventing cyberattacks and safeguarding their data, it conducts penetration tests. Meanwhile, Maldives has initiated the Digital Maldives for Adaptation, Decentralisation, and Diversification Project, with cybersecurity as one of its aims. Maldives and India signed a multipronged international co-operation partnership in 2022 to fund a wide range of development initiatives, one of which is cybersecurity on the island country. Maldives and Bahrain have also signed a memorandum of understanding.

Sri Lanka

As a result of the establishment of a National Cybersecurity Agency in 2016, Sri Lanka now has a Centre for Computer Incident Response Team. The government approved the Cybersecurity Bill 2023 in July of that year. The agency will oversee the creation of cybercrime awareness, the formulation of regulatory frameworks for organisations, training and the creation of a computer incidence response team. Sri Lanka has an information and cybersecurity plan for the years 2019–2023. The country also has laws that make it a felony to commit certain types of cybercrime. Sri Lanka's legal framework for dealing with cybercrime and malevolent online actions includes the Computer Crimes Act 2007, the Payment Devices Fraud Act 2006, the Intellectual Property Act 2006, the Electronic Transaction Act 2006 and the Information and Communication Technology Act 2003.

Pakistan

Many cybercrimes and internet-related offences are punishable by law in Pakistan. A national cybersecurity policy was unveiled in July 2021. This allows for the establishment

of a national cybersecurity agency and the development of public and private sector cybersecurity rules, frameworks, processes and standards. Nevertheless, these rules remain unenforced.

Bangladesh

According to the Bangladesh Gazette 2018, the country's legal framework for dealing with cybercrimes and the prosecution of those accused of such crimes is embedded within the Digital Security Act 2018. The Bangladesh Cybersecurity Act 2023 passed into law in 2023 and supersedes the Act of 2018. Reportedly, the substance of the two Acts is the same, although they go by different names. Amnesty International (2022) has speculated that the most recent version includes language that may lead to abuses of human rights. In addition, Bangladesh has formulated its Cybersecurity Strategy 2021–2025 but it is yet to implement this.

6.2 Pacific region

Australia

Australia has changed its cybersecurity strategy, laws, agencies, structure, standards and guidelines, joining other Pacific nations in this effort. The government previously unveiled two cybersecurity plans, in 2016 and 2020. After soliciting inputs from the private sector, the government, academia and business, it then unveiled its 2023–2030 Cybersecurity Strategy, aiming to become a global leader in cybersecurity. The Australian Signals Directorate set up the Australian Cyber Security Centre in 2023 to enhance cyberattack awareness, conduct cybersecurity assessments, spread information about cybercrime reporting and recovery, and put into action many other aspects of the Australian Cybersecurity Strategy.

Vanuatu

The National Security Strategy of Vanuatu has cybersecurity as its fifth pillar. The aim is to protect cyberspace and the nation's critical information and infrastructure. Cybercriminal activities are now a crime, punishable by law, according to the Cybersecurity Act of 2021. The government has also developed the National Cybersecurity Strategy 2030, the National Harmful Digital Communication Strategy 2023 and Vanuatu National Data Protection & Privacy Policy. Vanuatu has intergovernmental programmes involving many of its agencies on training, cyberattacks and threat reporting, among others. The main agency in charge of Cybersecurity in the country is CERT Vanuatu.

Fiji

Fiji has in place the Cybercrime Act 2021. The Ministry of Information and Communication Technology is responsible for the country's cybersecurity. To strengthen the country's overall digital presence and to control and mitigate unwanted cybercriminal

activities, it oversees programmes such as Digital FIJI and many more. The country's CERT and an updated National Cybersecurity Strategy are nearing completion. To enhance its security policy, the country takes part in regional partnerships with Australia as well as other international collaborations.

Kiribati

The Ministry of Information, Communications and Transport of Kiribati prepared a national cybersecurity strategy in 2020 and enacted the Cybercrime Act in 2021. No dedicated government body has been established to carry out this plan; the ministry oversees implementation of the cybersecurity strategy.

Nauru

As a member of the Pacific Cybersecurity Operational Network, Nauru passed a law in 2015 to combat cybercrime and make it easier to prosecute those responsible. The Ministry of Information and Telecommunications is responsible for implementing cybersecurity policy.

Tonga

The Strategy and Computer Emergency Response Team in Tonga oversees the implementation of the National Cybersecurity Framework 2022. This specialist agency enforces Tonga's cybersecurity rules. Critical infrastructure operators, as well as public and private sector organisations, obtain guidance and assistance from the response team.

New Zealand

New Zealand passed the Intelligence and Security Act 2017. In addition, the country launched a cybersecurity strategy in 2019 managed by CERT New Zealand.

Papua New Guinea

In Papua New Guinea, cybersecurity matters are handled by the Department of Information and Communication Technology and other departments that are members of the National Cyber Co-ordinating Centre. There is national legislation and a cybersecurity policy in place to make cybercrime a punishable offence. An example of this is the Cybercrime Code Act 2016. Launched in 2020, the National Cybersecurity Policy 2021 details the government's cybersecurity objectives and plans to attain them.

Samoa, Solomon Islands and Tuvalu

While Samoa has a national cybersecurity strategy for 2016–2021, with SamCERT as its main cybersecurity body, it has no specialised cybercrime legislation. Solomon Islands also does not have cybercrime legislation but the government ICT Unit keeps tabs on the country's cybersecurity activities. Tuvalu does not yet have a dedicated body to

supervise cybersecurity matters; issues are handled by the Department of Information and Communication Technology under the Ministry of Justice.

7. Conclusion and recommendations

7.1 Conclusion

This article has looked in depth into cybercrime in APAC and found that the region is not as resilient to cybercriminal activities as initially thought. This is particularly the case for Commonwealth APAC countries, used as the focus for the study, although some Commonwealth countries, such as Singapore, New Zealand and Australia, are very heavy on cybersecurity initiatives that uncover and address the activities of cybercriminals and promote cyber-resilience. Our study has highlighted the context of cybercrime in the region, and within this the role that the COVID-19 pandemic has played in shifting work online, thereby exposing many organisations in the region to cyberthreats. It has also highlighted the positive and negative roles that AI may play in the fight against cybercriminal activities.

The Commonwealth APAC region needs to strengthen its resilience to and reduce the risk of cyberattacks and threats, and protect its digital infrastructure in the ever-changing landscape. Therefore, we now highlight options to build the resilience of Commonwealth APAC countries to prevent the proliferation of cybercriminal activities in the region.

7.2. Policy considerations to prevent cybercrime

Increased awareness, advocacy and education: The governments of APAC countries should fund campaigns to educate the public about the risks of cybercrime. An example of an existing awareness campaign is Singapore's Better Cyber Safe than Sorry campaign, which began with private e-commerce retailers like Shopee and supermarket chain NTUC Fairprice, and has since expanded to include instructional videos, national television advertisements and posters at most bus stops (Gullapalli, 2023). Individuals and businesses alike can benefit from increased vigilance and preparedness in the face of cybersecurity threats if they are made more aware of the risks they face and given direction on how to react (ibid.).

Improved public and private co-operation: Co-operation between cybersecurity authorities, organisations and governments may aid in the prevention of attacks and proactively address emerging threats. By working together, organisations can improve their defences in response to cyberthreats more quickly.

Creation of taskforces: Learning from the successes of countries such as Singapore, it is pertinent to establish national taskforces devoted to developing, co-ordinating and implementing comprehensive strategies and policies to successfully tackle cybercrime.

Improved government regulations: To safeguard their citizens, APAC countries should consider enacting strict and standardised cybersecurity laws. These policies can create

baselines for security, promote frequent evaluations and impose consequences for failing to comply, drawing inspiration from the practices already in place in Australia and Singapore. By establishing rules that strengthen cybersecurity resilience, APAC nations can push businesses to prioritise safety and implement best practises.

Strengthening cybersecurity governance and leadership: Organisations in the APAC region should hire skilled experts with experience in cybersecurity to senior roles and boards of directors to strengthen cybersecurity leadership and governance frameworks. Fostering a culture of responsibility and giving security measures their appropriate priority can be achieved when cybersecurity is prioritised at the highest levels of decision-making within organisations. Public and private organisations require a chief information security officer, who is given authority and a clear mandate to implement an 'intelligence-led, prevention-first cybersecurity approach' to compete on the new cyber-battlefield (Gullapalli, 2023).

Collaboration with international partners: Cybercrime is a global phenomenon, hence APAC countries need to collaborate with global partners to put an end to it. By doing this, APAC countries will enhance their defence and reduce the threats presented by cybercriminals who may operate from other countries.

Consistent expenditure on security: The public and private entities in the APAC region need to invest heavily in cyber-resilience. To remain ahead of threats and reduce their exposure to attacks, entities must invest in strong security protocols, update and patch systems regularly and undertake thorough security audits.

Responding to the misuse of AI for cybercriminal activities: To respond to the misuse of AI for cybercriminal activities, the APAC region can adopt policy initiatives like the Digital Services Act and the Regulation proposal for Artificial Intelligence Systems adopted by the EU (Schneider and Werle, 2023). Such policy will serve the purpose of creating rigorous guidelines and responsibility for risk assessments using AI services to guarantee the safe use of AI services. Other initiatives to draw lessons from include the Budapest Convention and the recent inclusion of the Second Additional Protocol to the Budapest Convention, initiated by the Council of Europe, which aims at criminalising offenders who perpetrate cybercriminal activities (Chang, 2020; Mantelero, 2022). In addition, the adoption of these initiatives will foster co-operation within the region, thereby supporting efforts to identify, investigate and prosecute cybercriminals (Velasco, 2022).

Finally, it is crucial to note that recognising that a multidimensional strategy comprising awareness, co-operation, regulation and continual improvement from all stakeholders is necessary to make APAC the least targeted region for cyberattacks. By adopting these policies and promoting a cybersecurity-aware culture, APAC can strengthen its defence against cybercriminals; safeguard its digital infrastructure, businesses and citizens from evolving threats; and reduce the associated risks. Since the threat environment is always changing, it is vital to stress the need for constant communication and preventative measures in building cyber-resilience and stopping cybercrime.

References

Ala-Pietilä, P. and N.A. Smuha (2021) 'A Framework for Global Cooperation on Artificial Intelligence and Its Governance'. *Reflections on Artificial Intelligence for Humanity* 237–265.

Alkhalil, Z., C. Hewage, L. Nawaf and I. Khan (2021) 'Phishing Attacks: A Recent Comprehensive Study and a New Anatomy'. *Frontiers in Computer Science* 3: 563060.

Allioui, H. and Y. Mourdi (2023) 'Unleashing the Potential of AI: Investigating Cutting-Edge Technologies That Are Transforming Businesses'. *International Journal of Computer Engineering and Data Science* 3(2): 1–12.

Al-Maliki, S., A. Qayyum, H. Ali et al. (2023) 'Adversarial Machine Learning for Social Good: Reframing the Adversary as an Ally'. arXiv preprint arXiv: 2310.03614.

Amankwah-Amoah, J., Z. Khan, G. Wood and G. Knight (2021) 'COVID-19 and Digitalization: The Great Acceleration'. *Journal of Business Research* 136: 602–611.

Amnesty International (2022) 'Bangladesh: Government Must Remove Draconian Provisions from the Draft Cyber Security Act'. 31 August. www.amnesty.org/en/latest/news/2023/08/bangladesh-government-must-remove-draconian-provisions-from-the-draft-cyber-security-act/

Ang, B. (2021) 'Singapore: A Leading Actor in ASEAN Cybersecurity'. In Romaniuk, S. and M. Manjikian (eds) *Routledge Companion to Global Cyber-Security Strategy*. Basingstoke: Routledge, pp. 381–391.

Araki, N. (2022) 'Report on the 34th Asia-Pacific Telecommunity Standardization Program Meeting'. *NTT Technical Review*: 81–84.

Argaw, S.T., J.R. Troncoso-Pastoriza, D. Lacey et al. (2020) 'Cybersecurity of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks'. *BMC Medical Informatics and Decision Making* 20: 1–10.

Aslan, , S.S. Aktuğ and M. Ozkan-Okay (2023) 'A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions'. *Electronics* 12(6): 1333.

Association of Southeast Asian Nations (ASEAN) Cybersecurity Cooperation Strategy (2021) 'Broadening and Deepening Cybersecurity Cooperation for a Secure and Resilient ASEAN Cyberspace, 2017–2020'. https://asean.org/wp-content/uploads/2021/08/ASEAN-Cybersecurity-Cooperation-Strategy.pdf

Australian Signals Directorate (ASD) (2024) 'Steps for Organisations to Protect their IT Environment'. www.cyber.gov.au

Bahuguna, A., R.K. Bisht and J. Pande (2020) 'Country-Level Cybersecurity Posture Assessment: Study and Analysis of Practices'. *Information Security Journal: A Global Perspective* 29(5): 250–266.

Benincasa, E. (2020) 'The Role of Regional Organizations in Building Cyber Resilience: ASEAN and the EU'. *Pacific Forum Issues & Insights* 20.

Brain, S. and O. Oyadeyi (2023) 'Funding Crime Online: Cybercrime and Its Links to Organised Crime in the Caribbean'. *Commonwealth Cybercrime Journal* 1(1): 84–110.

Caldwell, M., J.T. Andrews, T. Tanay and L.D. Griffin (2020) 'AI-Enabled Future Crime'. *Crime Science* 9(1): 1–13.

Cascavilla, G., D.A. Tamburri and W.J. van den Heuvel. (2021) 'Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review'. *Computers & Security* 105: 102258.

Chakravarti, J. (2023) 'Phishing Attacks Rise Sharply in Southeast Asia'. Bank Info Security, 27 July. www.bankinfosecurity.asia/phishing-attacks-rise-sharply-in-southeast-asia-a-22669.

Chang, L.Y. (2020) 'Legislative Frameworks against Cybercrime: The Budapest Convention and Asia'. In Holt, T. and A. Bossler (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London: Palgrave, pp. 327–343.

Check Point Research (2023) 'Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most'. 27 April. https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

Christine, D. and M. Thinyane (2020) 'Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies'. Macau: United Nations University.

Commonwealth Secretariat (2022) 'Commonwealth Experts Meet in Singapore to Explore Solutions to Increasing Cyber Risks in Asia'. 29 September. https://thecommonwealth.org/news/commonwealth-experts-meet-singapore-explore-solutions-increasing-cyber-risks-asia

Centre for Strategic and International Studies (CSIS) (nd) 'Significant Cyber Incidents'. Accessed online at: www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed 29 October 2023).

Cybersecurity Ventures (2022) '2022 Official Cybercrime Report'. https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

Cybersecurity Ventures (2023) 'Cybercrime to Cost the World $9.5 Trillion USD Annually in 2024'. www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024?utm_medium=email&utm_source=pardot&utm_campaign=autoresponder

Development Dimensions International (DDI) (2023) 'Global Leadership Forecast 2023'. www.ddiworld.com/global-leadership-forecast-2023?utm_source=google&utm_medium=display&utm_campaign=|Brand|DA|GLF23_Launch|EU|EN|&gclid=EAIaIQobChMIn6y0kfLegQMVHUf2CB2Xlw_xEAEYASAAEgLpP_D_BwE

Dimitrov, W. (2020) 'The Impact of the Advanced Technologies Over the Cyber Attacks Surface'. In Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science Online Conference: 509–518.

Diogenes, Y. and E. Ozkaya (2019) *Cybersecurity–Attack and Defense Strategies: Counter Modern Threats and Employ State-of-the-Art Tools and Techniques to Protect Your Organization against Cybercriminals*. Birmingham: Packt Publishing Ltd.

Dwivedi, Y.K., D.L. Hughes and C. Coombs (2020) 'Impact of COVID-19 Pandemic on Information Management Research and Practice: Transforming Education, Work and Life'. *International Journal of Information Management* 55: 102211.

Engstrom, D.F., D.E. Ho, C.M. Sharkey and M.F. Cuéllar (2020) 'Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies'. NYU School of Law Public Law Research Paper 20–54.

Falk, R. (2022) 'First Australian Court Judgments on Cyber Security'. AICD, 8 June. www.aicd.com.au/economic-news/world/global-risk-report/first-australian-court-judgments-on-cyber-security.html

Ferdous, J., R. Islam, A. Mahboubi and M.Z. Islam (2023) 'A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism'. *IEEE Access* 11: 121118–121141.

Gan, G.S. (2024) 'Filling the Gaps: The Story of APAC's Cyber Security Capacity Building'. Kaspersky www.kaspersky.com/about/policy-blog/filling-the-gaps-the-story-of-apacs-cyber-capacity-building

Germanos, G. and N. Georgiou (2022) 'How Did Cybercriminals "Survive" during the Pandemic?' *Urban Crime, An International Journal* 3(2): 110–123.

Gullapalli, V. (2023) 'Why Is the Asia Pacific Region a Target for Cyber Crime & What Can Be Done'. Check Point Research, 4 August. www.cybertalk.org/2023/08/04/why-is-the-asia-pacific-region-a-target-for-cyber-crime-what-can-be-done/

Herko, T. (2023) 'The INTERPOL Global Complex for Innovation in Singapore: A Personal Retrospective'. *Belügyi Szemle* 71(3. ksz): 45–55.

Inamdar, N. (2023) 'National Cyber Security Strategy 2023 to Be Released Soon'. *Hindustan Times*, 13 June www.hindustantimes.com/cities/pune-news/national-cyber-security-strategy-2023-to-be-released-soon-101686596627065.html

Khan, J.I., J. Khan, F. Ali et al. (2022) 'Artificial Intelligence and Internet of Things (AI-IoT) Technologies in Response to the COVID-19 Pandemic: A Systematic Review'. *IEEE Access* 10: 62613–62660.

Kumar, S. (2021) 'The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society'. *Journal of Cyber Policy* 6(3): 375–393.

Laitinen, M. and S. Armstrong-Smith (2022) 'Tackling Cybercrime and Ransomware Head-On: Disrupting Criminal Networks and Protecting Organisations'. *Cyber Security: A Peer-Reviewed Journal* 5(3): 190–205.

Lallie, H.S., L.A. Shepherd and J.R. Nurse (2021) 'Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic'. *Computers & Security* 105: 102248.

Malja, M. and M. October (2022) 'The Lanzarote Convention: National Action Plan for the Years 2022–2025'. http://urn.fi/URN:ISBN:978-952-00-5443-4

Mantelero, A. (2022) 'Regulating AI'. In *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. The Hague: TMC Asser Press, pp. 139–183.

Medina, L. and F. Schneider (2019) 'Shedding Light on the Shadow Economy: A Global Database and the Interaction with the Official One'. CESIFO Working Paper 7981.

Mizrak, F. (2023) 'Integrating Cybersecurity Risk Management into Strategic Management: A Comprehensive Literature Review'. *Research Journal of Business and Management* 10(3): 98–108.

Positive Technologies (2023) 'Cybersecurity Threatscape of Asia: 2022–2023'. 12 September. www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/

Quimba, F.M.A. and M.A.A. Barral (2020) 'Exploring the Feasibility of Content Analysis in Understanding International Cooperation in APEC'. PIDS Discussion Paper 2020–58.

Roberts, W. (2022) 'Role of IGF and APrIGF in reference to Libraries in Nepal'. *Access: An International Journal of Nepal Library Association* 1(1): 139–142.

Rui, W. (2023) 'ASEAN Cybersecurity Policy and China-ASEAN Cooperation' *China International Studies* 98: 55.

Runde, D.F., C.M. Savoy and O. Murphy (2020) 'Post-Pandemic Infrastructure and Digital Connectivity in the Indo-Pacific'. Brief, 2 November. Washington, DC: CSIS.

Ryan, M. (2021) *Ransomware Revolution: The Rise of a Prodigious Cyber Threat* . Berlin/Heidelberg: Springer.

Sarowa, S.K., B. Bhanot and V. Kumar (2022) 'Analysis of Cyber Attacks and Cyber Incident Patterns over APCERT Member Countries'. In 4th International Conference on Artificial Intelligence and Speech Technology (AIST): 1–6.

Schmidt, E., B. Work, S. Catz et al. (2021) 'National Security Commission on Artificial Intelligence (AI) Final Report'. https://digital.library.unt.edu/ark:/67531/metadc1851188/

Schneider, V. and R. Werle (2023) 'International Regime or Corporate Actor? The European Community in Telecommunications Policy'. In Dyson, K. and P. Humphreys (eds) *The Political Economy of Communications*. Basingstoke: Routledge, pp. 77–106.

Singh, L. (2022) 'Cyber Crime, Cyber Resilience and Security Strategy in Post Pandemic World'. *Supremo Amicus* 28(305): 1–11.

Skouby, K.E., P. Dhotre, I. Williams and K. Hiran (2022) *5G, Cybersecurity and Privacy in Developing Countries*. Boca Raton, FL: CRC Press.

Slayton, R. and B. Clarke (2020) 'Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005'. *Technology and Culture* 61(1): 173–206.

Smail, J. (2023) 'The Top 10 Data Breaches'. Cybers Security Hub, 15 September www.cshub.com/attacks/articles/the-top-10-apac-data-breaches.

Solar, C. (2023) *Cybersecurity Governance in Latin America: States, Threats, and Alliances*. Albany, NY: State University of New York Press.

The Asset (2023) 'Asia-Pacific Deepfake Incidents Surge'. 30 November. www.theasset.com/article/50495/asia-pacific-deepfake-incidents-surge

Tien, H.M. and T.J. Cheng (2016) *The Security Environment in the Asia-Pacific*. Basingstoke: Routledge.

United Nations Office on Drugs and Crime (UNODC) (nd) 'International and Regional Instruments'. E4J University Module Series. www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html

Van der Sloot, B. and Y. Wagensveld (2022) 'Deepfakes: Regulatory Challenges for the Synthetic Society'. *Computer Law & Security Review* 46: 105716.

Velasco, C. (2022) 'Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments'. *ERA Forum* 23(1) 109–126.

Wong, P., R. Marles and C. O'Neil (2024) 'Cyber Sanctions in Response to Medibank Private Cyber-attack'. Release, 23 January. www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack

Xu, L., Q. Guo, Y. Sheng et al. (2021) 'On the Resilience of Modern Power Systems: A Comprehensive Review from the Cyber-Physical Perspective'. *Renewable and Sustainable Energy Reviews* 152: 111642.

Zeadally, S., E. Adi, Z. Baig and I.A. Khan (2020) 'Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity'. *IEEE Access* 8: 23817–23837.

Zhang, Z., H. Al Hamadi, E. Damiani et al. (2022) 'Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research'. *IEEE Access* 10: 93104–93139.

Zhao, P., Z. Cao, D.D. Zeng et al. (2021) 'Cyber-Resilient Multi-Energy Management for Complex Systems'. *IEEE Transactions on Industrial Informatics* 18(3): 2144–2159.

About the authors

Dr Olajide O. Oyadeyi is a passionate economist who specialises in the economic dynamics of cybercrime to inform strategic solutions and policies in combating digital threats worldwide. He is dedicated to unravelling the economic incentives driving cybercriminal activities and developing innovative frameworks to mitigate risks and enhance cybersecurity resilience on a global scale.

Oluwadamilola A. Oyadeyi is a passionate researcher on a range of societal issues. She has served as an independent researcher and writer, contributing her expertise to publications covering a wide array of topics, from public health to energy, climate change and cybercriminal activities.

Rofiat O. Bello is a seasoned legal expert who specialises in the multifaceted legal landscape surrounding cybercrime on a global scale, adept at navigating intricate regulatory frameworks and addressing emerging challenges in cybersecurity law. Passionate about exploring the intersections of technology and jurisprudence, she is committed to advancing legal solutions that safeguard individuals and organisations against digital threats in an ever-evolving digital ecosystem.