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

The Commonwealth

Funding Crime Online: Cybercrime and its Links to Organised Crime in the Caribbean

Sophie Brain[1] and Olajide Oyadeyi[2]

Abstract

The Caribbean region has seen an explosion in digital transformation, with one of the fastest growing internet populations worldwide. The accompanying growth in cyber technology has allowed for new regional and social advancements. However, the Caribbean has also become an attractive target for cybercrime due to increased economic success, a growth in online presence, combined with low levels of cyber resilience. Organised crime groups have been able to exploit these vulnerabilities by taking advantage of the internet and exploring new ways of making money online, as well as using the internet for other illicit activities such as money laundering and funding terrorism. The Caribbean remains acutely unprepared to deal with cyberattacks and the COVID-19 pandemic highlighted several instances where these weaknesses were exposed, allowing for criminal groups to make millions of dollars.

This paper therefore aims to analyse the relationship between organised crime groups and cybercrime in the Caribbean and explores the methods used by these groups to fund their activities. The concept of 'software-as-a-service' is highlighted as an enabling factor in the underground economy used by organised crime groups in the Caribbean to help facilitate cybercrime. Ransomware is discussed as one of the top security concerns in the region, often used by organised crime groups to demand payment from organisations with insufficient cyber defences. Phishing is also emphasised as a common technique used by organised crime seeking to steal user banking data, gain access to accounts and steal from victims. Digital currencies such as Bitcoin, Ethereum and Central Bank Digital Currencies, as well as the dark web, are discussed as main facilitators used to move criminal proceeds in the Caribbean. The paper also discusses what

1 Research Officer, Commonwealth Secretariat. Email: sophie.brain@hotmail.com
2 Economic Research Officer, Commonwealth Secretariat. Email: jide.oyadeyi@gmail.com / o.oyadeyi@commonwealth.int

Commonwealth Caribbean countries have done so far to combat these issues through their national cybersecurity strategies, including Jamaica's National Cybersecurity Strategy and Belize's National Cybersecurity Strategy – Towards A Secure Cyberspace 2020–2023. The activities of regional groups such as the Caribbean Community and Common Market (CARICOM) Cyber Security and Cybercrime Action Plan are highlighted. Examples of successful interventions to undermine the use of cybercrime by organised crime groups in the world's leading cybersecurity authorities are also explored.

Introduction

Cybercrime has been common since the advent of the internet. The cost of cybercrime in recent times has, however, become more pronounced. According to Cybersecurity Ventures (2022), the world was due to lose over US$7 trillion to cybercrime in 2022, after losing more than US$6 trillion in 2021. If this figure was measured as a country, cybercrime would be the third-largest economy after the US and China. However, cybercrime cannot be discussed in isolation. This is because cybercrime is linked to the level of information and communication technology (ICT) in a country, and ICT has been used as a tool to integrate different systems across sectors or countries. For instance, many entities and organisations use ICT for their basic tasks. This has made it possible for many cybercriminals to target and defraud institutions and individuals. According to Verizon's (2022) *Data Breach Report*, 82 per cent of breaches involve a human element. That is, whether by phishing, the use of stolen cards, misuse or an error, human beings play a dominant role in cybercrime today. The globalisation of markets and the interconnectedness of states, combined with reliance on ICT, calls for both developed and developing states to put into place measures to address cybercrime.

This is especially true in the Caribbean, as the region's internet penetration since the turn of the twenty-first century has been on the rise. Internet users averaged 67.4 per cent of the total population in the region in 2020 compared to 52.4 per cent worldwide (WDI 2022a). This gives more credence to the notion that increased internet usage across the Caribbean has led to the proliferation of cybercriminal activities, making the region more vulnerable to cybersecurity attacks. Despite increased awareness and attention directed towards this problem, cybercrime remains a complex issue. In 2016 for example, Jamaica lost in excess of US$77 million to cybercrime alone (Wilson-Harris, 2019). These losses have adverse effects on business revenues, the cost of operations, individuals and the government in terms of its ability to provide welfare packages across the Caribbean. Furthermore, the introduction of cryptocurrencies, a platform for trading virtual currencies, has brought about renewed vigour in regulating online activities.

Analysing the Caribbean region in the context of the global discourse on cybersecurity and cybercriminal activities is particularly important. This is due to the compounding effect cybercriminal activities may have on the countries' economies given their small

size, inherent small country characteristics and the specific vulnerabilities that they face. In comparison to the US, where a cyberattack may not significantly affect the entire economy, weak infrastructure in the Caribbean – as well as the centrality of information within governments – makes the region more vulnerable to cybersecurity breaches and cybercriminal activities, which may cause a national crisis that could affect the entire macroeconomy. Moreover, the discourse on cybercriminal activities and cybersecurity breaches is becoming a developmental issue. This is because, in the event of a breach, the affected state would witness rising economic costs. These costs would be more amplified in a small and developing country context (Wint 2003; Moore 2017). Wint (2003) opined that cybercrime tends to affect small countries more than larger countries due to the larger countries' ability to cushion the effect better at the national level compared to a smaller country. By implication, a cyberattack or breach on government infrastructure and private sector organisations would affect a small Caribbean country to a larger extent (Moore 2017).

Furthermore, the ease of doing business is of top concern to several small Caribbean states as they continue to rebuild their economies following the COVID-19 pandemic, which had a significant impact on businesses in the region (Hamilton-Davis 2023). This cannot be achieved without focusing on cybersecurity as cybercrime has implications for companies, causing increased costs as organisations incur outlays such as cybersecurity technology or expertise and insurance premiums to protect their businesses. In addition to this, high levels of cybercrime cause reputational damage as customers, and even suppliers, may feel less secure leaving their sensitive information in the hands of a company whose information technology (IT) infrastructure has been broken into, which could lead to lost revenue. Given the high economic cost of infrastructural protection from cybercrime, coupled with Caribbean small states' limited financial resources, this has caused the region to be particularly vulnerable to escalating cybercriminal activity.

It is because of these increased vulnerabilities faced by Caribbean states that this study aims at adding to the literature on cybercrime and its links to organised crime in Commonwealth Caribbean countries. The objectives of this paper are therefore to conceptualise cybercrime in the region and identify the types of crimes being carried out by organised crime groups and their impacts on Commonwealth Caribbean countries. Furthermore, the paper aims to identify ways through which cybercrime can be reduced, offering guidance to Commonwealth Caribbean countries on how this can be done.

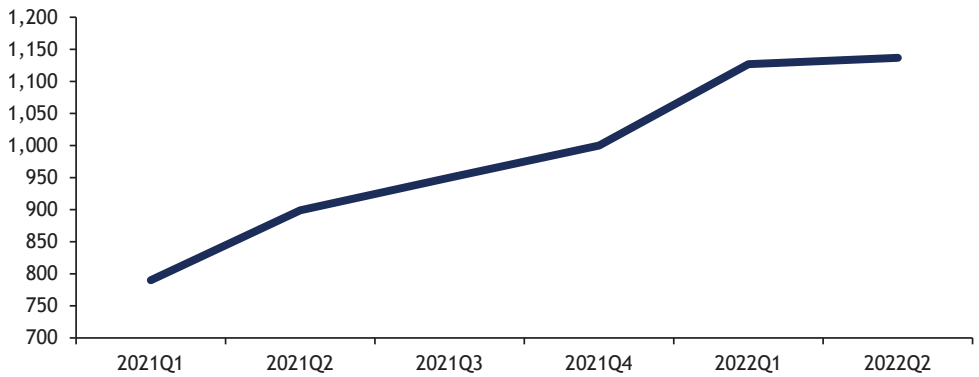
The rest of the paper is organised as follows. The next section introduces some stylised facts about global cyberattacks and links between ICT and cybercrime in the Commonwealth Caribbean countries. The section that follows explores the scope of organised crime in the Caribbean. There is then a section that discusses how organised crime groups are using cybercrime and identifies the different types of cybercrime that occur in the region. The next section discusses existing legislation and strategies used in combating cybercrime among Commonwealth Caribbean countries, while the final section identifies means by which cybersecurity can be improved and offers learning experiences from leading cybersecurity authorities.

Stylised facts

Stylised facts on cybercriminal activities across the globe

In recent times, the world has been affected by increased cyberattacks, as evidenced in Figure 1. Cybercriminal attacks per organisation grew from 899 attacks in Q2 2021 to 1,136 attacks in Q2 2022, an increase of 32 per cent year-on-year. According to Check Point Research (2022b), this has been the highest rate of weekly increase in cybercriminal activities since the introduction of the internet, leading to questions surrounding the safety of individuals, corporate organisations and governments from cybercriminals.

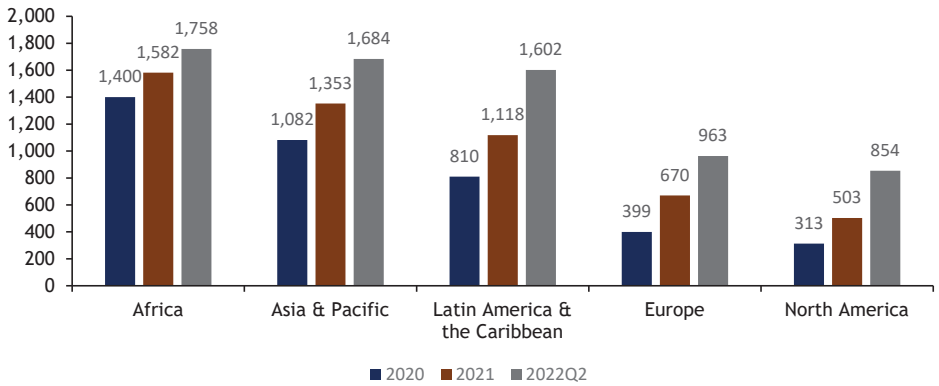
Figure 1. Global weekly cyberattacks



Source: Check Point Research 2022a

Figure 2 shows that by region, Africa has been most affected by cybercriminal activities, followed by Asia, and Latin America and the Caribbean (Check Point Research 2022a; 2022b). Looking through the data in more depth, it can be seen that between 2021 and Q2 2022 the Latin American and Caribbean region witnessed the largest increase in average weekly cybercriminal attacks per organisation (484) when compared to other regions. This therefore emphasises the importance of focusing on cybercrime in Caribbean Commonwealth countries, as cybercrimes have increased more there than in other regions.

Figure 2. Weekly cyberattacks by region



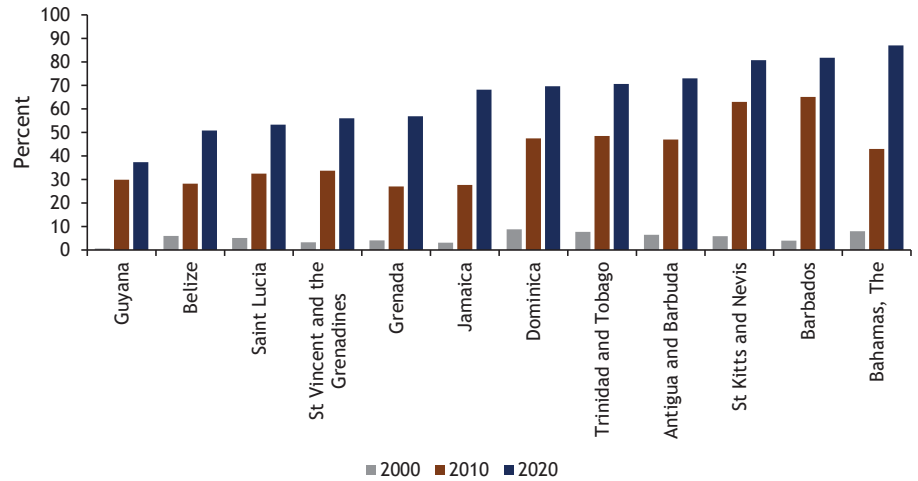
Source: Check Point Research 2022a; 2022b

Stylised facts on ICT performance and links to Cybercrime in Commonwealth Caribbean countries

Due to the proliferation of internet usage between 2000 and 2020, cybercriminals have used the opportunity to advance their illegal activities, while advances in ICT may provide a useful opportunity for the growth of illegal activities if not properly regulated. The Caribbean region has made significant strides in ICT development, especially between 2010 and 2020 – as demonstrated in Figure 3. In the year 2000, the average proportion of internet users in the Commonwealth Caribbean region stood at 5 per cent of the population, with Dominica having the highest internet usage at 9 per cent while Guyana had the least internet usage at 0.60 per cent of the population. Between 2000 and 2010, the average internet usage increased to 41 per cent, a rise of 683 per cent from the year 2000.

Between 2010 and 2020, the average number of internet users as a percentage of the Commonwealth population in the Caribbean grew by 59 per cent, from 41 per cent in 2010 to 65 per cent in 2020. Due to the rapid increase in internet use, the growth in internet penetration between 2000 and 2020 stood at 1,147.7 per cent. This growth in internet users may be ascribed primarily to a rise in internet access through mobile devices, reduced internet costs and the rise in e-commerce. This has implications for cybercriminal activities, as with faster and cheaper internet connectivity, cybercriminals have more opportunities to engage in online crime as they are able to increase their reach. These increased opportunities, paired with limited cybercrime legislation, make the region a prime target for cybercriminals.

Figure 3. Users of the internet (percentage of population)

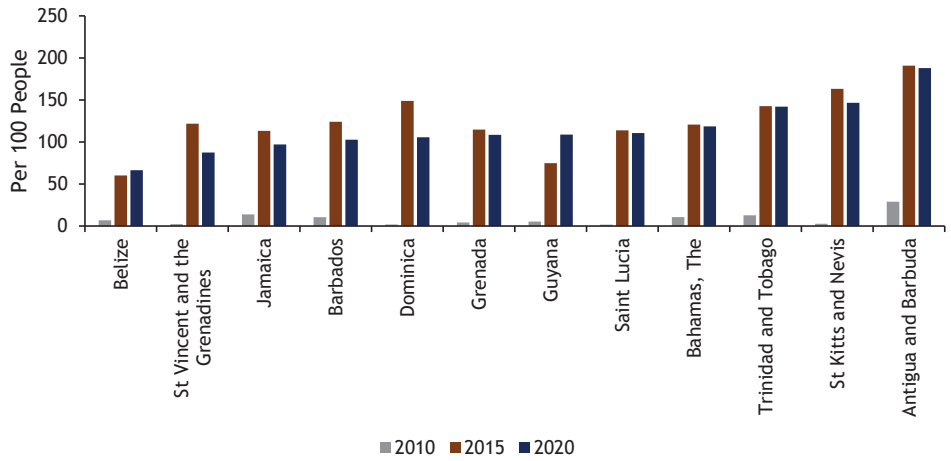


Source: World Development Indicator (WDI) 2022a

Figure 4 depicts the trend of mobile cellular subscriptions across Commonwealth countries within the Caribbean region. In 2010, the average mobile cellular subscriptions in the Caribbean region stood at 8.43 people per 100 people. At this point, Antigua and Barbuda had the highest number of mobile cellular subscriptions at 29 people per 100, while Saint Lucia had the least at 1.60 people per 100. In 2015, the average mobile cellular subscription in the Caribbean region grew by 1,372 per cent, from 8.43 people per 100 to 124.08 people per 100, given that certain individuals at that stage may have had more than one mobile phone subscription.

In 2020, the growth in the average mobile cellular subscriptions fell by 7.18 per cent, from 124.08 people per 100 in 2015 to 115.2 people per 100. This could be due to users consolidating their cellular subscriptions as costs increased. Like previous years, Antigua and Barbuda had the highest number of mobile cellular subscriptions at 187.9 people per 100, while Belize had the least number of mobile cellular subscriptions at 66.39 people per 100. From these figures, it is clear that remote connectivity is high across Commonwealth countries in the Caribbean as the average for middle-income countries is 108 per 100 and 122 per 100 for high-income countries (WDI 2022b). The reliance on mobile phones to access the internet in the Commonwealth Caribbean also has implications for cybercrime, as mobile devices tend not to have firewalls, antivirus software, encryption and other defensive mechanisms that computers do, making them more vulnerable to threats. Examples of this occurring in Caribbean Commonwealth countries will be explained in detail later in the paper.

Figure 4. Mobile cellular subscriptions (per 100 people)



Source: WDI 2022a

Table 1 shows information on secure internet servers in the Caribbean Commonwealth countries between 2010 and 2020. Data on other regions, as well as selected Commonwealth countries, were also selected for comparison. In 2010, Antigua and Barbuda had the highest number of secure internet servers at 681.6 people per1 million, while Guyana had the least number of secure internet servers at 1.3 people per 1 million. In 2020, while Guyana continued its trajectory as the country with the least secure internet servers at 61 people per 1 million, Belize significantly improved its numbers of secure internet servers and became the most secure Commonwealth country in terms of internet servers within the Caribbean.

In comparison to other regions such as the Euro Area, it is evident that Belize and Dominica performed admirably well in 2020 (see Table 2). Furthermore, their performance far outstrips the Latin America and the Caribbean region, as well as other selected advanced Commonwealth countries such as Australia, Canada and the United Kingdom. The adoption of a cybersecurity strategy in Belize may have helped improve its secure internet connections, while the Government of Dominica has made significant strides to upgrade its resilience against potential cybercrimes by partnering with international organisations to achieve its goal. These among other policies may have helped these two countries to significantly improve their secure internet connections compared to others within the region.

Although, St Kitts and Nevis is well above the Latin America and Caribbean average, with a secure internet connection of 6,223 per 1 million people, it is still far from reaching the levels of other advanced nations. On the other hand, the rest of the Commonwealth Caribbean countries are well below the Latin America and Caribbean average, as well as the World and Euro Area averages. This implies that more work needs to be done

to improve the number of secure internet connections across Antigua and Barbuda, The Bahamas, Barbados, Grenada, Guyana, Jamaica, Saint Lucia, St Vincent and the Grenadines, and Trinidad and Tobago, as this could have implications for these countries' cybersecurity.

Table 1. Secure internet servers (per 1 million people) across Commonwealth Caribbean countries

	2010	2015	2020
Antigua and Barbuda	681.6	694.7	1,245.8
Bahamas, The	366.3	1,002.1	1,261.3
Barbados	187.9	574.8	1,037.0
Belize	214.0	1,141.5	131,343.7
Dominica	42.3	266.9	46,922.5
Grenada	94.1	219.0	577.7
Guyana	1.3	27.4	61.0
Jamaica	24.2	121.4	160.4
St Kitts and Nevis	550.9	742.1	6,222.7
Saint Lucia	46.0	139.6	375.8
St Vincent and the Grenadines	18.5	119.1	126.2
Trinidad and Tobago	44.4	269.3	340.1

Source: WDI 2022a

Table 2. Secure internet servers (per 1 million people) across selected countries and regions

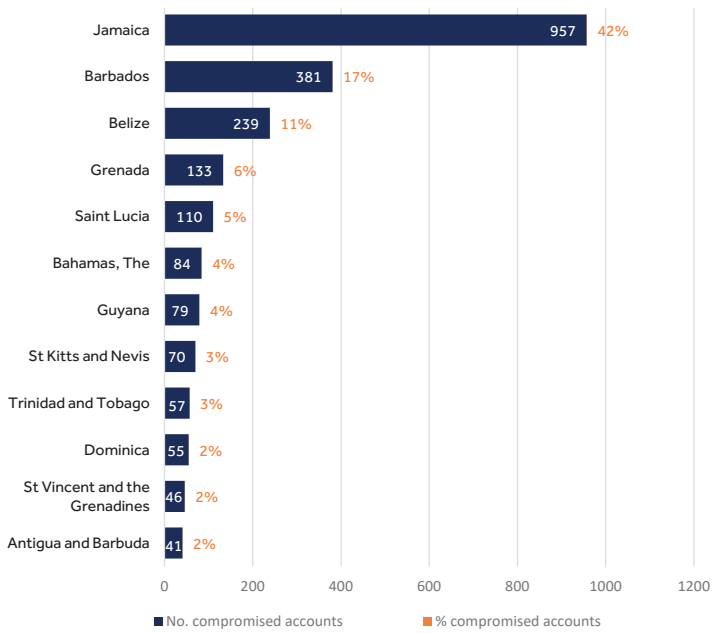
	2010	2015	2020
Euro Area	544.0	2,493.8	51,693.2
Latin America and the Caribbean	21.3	106.4	1,963.7
World	187.3	572.7	11,499.7
Australia	1,402.8	4,574.1	39,794.4
Canada	1,282.7	3,386.9	39,849.7
United Kingdom	1,315.4	4,386.3	36,379.7

Source: WDI 2022a

Due to the low levels of secure internet services across certain Commonwealth countries in the Caribbean, cybercriminals have taken advantage by developing ways of compromising emails, accounts and other online activities. Research carried out by G5 Cybersecurity (2021), as presented in Figure 5, shows that from a total of 2,252 compromised accounts across the Commonwealth countries in the Caribbean, Jamaica had the highest number of compromised accounts in 2021. This was closely followed by Barbados (17%) and Belize (11%). These figures support the relationship between the number of secure internet servers and compromised accounts as the number of secure internet servers is very low across these countries, as displayed in Table 1, since Jamaica and Barbados had 160 and 1,037 secure internet servers per 1 million people in 2020, which was relatively low when compared to advanced Commonwealth countries. However, Belize has high levels of secure internet servers, suggesting the relationship may not be so direct.

On the other hand, Antigua and Barbuda (41), St Vincent and the Grenadines (46), and Dominica (55) had the least number of compromised accounts within the Caribbean. The link between low levels of compromised accounts in this case can clearly be seen, as Dominica has relatively high numbers of secured internet servers when compared to the rest of the region. Caribbean Commonwealth countries need to be mindful when it comes to ensuring that they adequately inform individuals and businesses on securing their accounts, as this could have large economic consequences.

Figure 5. Number and percentage of compromised accounts across Commonwealth Caribbean countries in 2021



Source: G5 Cybersecurity 2021

Increased levels of internet usage, high numbers of mobile cellular subscriptions, and a lack of secure internet servers in certain Caribbean Commonwealth countries provide some insights into why cybercrime is taking place in the region and why it is likely to grow moving forward. Furthermore, the COVID-19 pandemic has acted as a great accelerator of digital transformation, with technology being at the forefront of countries' responses to the crisis. Although cybercrime was increasing and transforming before the pandemic, with a record number of people staying in their homes and relying even more on the internet for daily activities including work, education and leisure than usual, the ways for cybercriminals seeking to exploit emerging opportunities and vulnerabilities multiplied during this time (Europol 2020).

The pandemic therefore exposed the fragility of e-government services, online consumer services and education, and exacerbated the many inequalities in the system in the Commonwealth Caribbean. Cybercriminals took advantage of the crisis, since most jobs shifted operations online, and they were able to use a combination of online ransomware, phishing and other forms of cybercrime such as cryptocurrency fraud to swindle organisations, investors and individuals, further worsening this crisis. The following sections provide a more in-depth look at organised crime groups in the Caribbean and how they have used cybercrime to carry out their activities both before, during and after the COVID-19 pandemic.

Scope of organised crime in the Caribbean

Organised crime groups, which are defined in this article as groups that have as their purpose, or one of their purposes, the carrying out of criminal activities, and consist of three or more people who agree to act together to further that purpose, operate throughout the Commonwealth Caribbean. This is given its appealing geography, which allows for criminality to flourish. The Caribbean's border proximity to South America makes it both a destination and a transhipment zone for the trafficking of illicit drugs and arms to Florida, the East and Gulf Coasts of the United States (US), and to points throughout Europe and Africa (White House 2022). Large amounts of cocaine, marijuana and other drugs transit through Jamaica, Trinidad and Tobago, The Bahamas, and the Eastern Caribbean.

The influence of South America on the region has meant that foreign criminal organisations, most notably from Colombia and Mexico, feature in these countries' underworlds (Global Initiative 2020a). There is also evidence of the Italian mafia operating in The Bahamas, using the country as a trans-shipment point for cocaine trafficking. Furthermore, the ongoing political instability of the Government of Venezuela continues to generate new opportunities for organised criminal activities (White House 2022).

Street gangs are also active in much of the Caribbean region, with Jamaica reporting more than 260 gangs with nearly 4,000 members and Trinidad and Tobago identifying 95 gangs with more than 1,200 members (Katz 2015). These gangs are linked to the region's high homicide rates, with organised crime groups able to exert social control and co-opt the state in a variety of ways (InSight Crime 2018). In countries like Jamaica, for example, government sectors have established political alliances with local gangs to compensate for the state's abandonment of certain communities. Trinidad and Tobago's gangs also perform key social functions (ibid).

Given that drug trafficking is the main source of 'dirty money' in the region, both tax evasion and fraud take place as a knock-on effect of the funds from drug sales. Illicit flows are often legitimised through legal businesses such as real estate, private member clubs and banks. In addition to this, because many Caribbean countries implement liberal tax regimes while also permitting the formation of offshore companies to attract foreign investment, this allows for both shell companies to set up and tax avoidance schemes to take place. These shell companies can be used as money laundering systems to disguise the origin of illegal funds and help criminals to avoid anti-money laundering measures (Comply Advantage 2022). Ponzi and pyramid schemes also operate across the region, sometimes facilitated by army personnel and high-ranking government officials, increasing their reach (Global Initiative 2020b).

The prevalence of organised crime groups in the region has also allowed for criminal activity that goes beyond drug smuggling and arms trafficking. For example, Trinidad and Tobago is a source, transit and destination country for human trafficking. Women and girls from Venezuela, the Dominican Republic, Guyana and Colombia are vulnerable to sex trafficking in Trinidad and Tobago's brothels and clubs, while economic migrants from the Caribbean and Asia are vulnerable to domestic servitude and forced labour in the retail sector (Global Initiative 2020b).

Both fauna and flora crimes take place in the Caribbean region, with deforestation being a main issue. This is especially the case for Guyana, which is a source country for precious woods that are mainly shipped to China. Some Caribbean Commonwealth nations are also source and transit countries for the illegal trafficking of some of the world's most threatened species of fauna, including parrots, macaws, parakeets, songbirds, reptiles, arthropods and jaguars (Global Initiative 2020c). This trade in wildlife has increased significantly since the economic crisis in Venezuela, with an expanding number of traffickers identified.

The internet is a major enabler for organised crime groups' previously described activities in the Caribbean. There has been evidence that traditional organised crime groups have engaged in cybercrime and have been able to use the internet as a communication, research, logistics, marketing, recruitment, distribution and monetarisation tool (UNODC 2013; UNODC 2012). For example, organised crime groups use the dark web – encrypted online content that is not indexed by conventional search engines – for the illicit online

trade in drugs, weapons, stolen goods, stolen personal and payment card data, forged identity documents, and child abuse material (George, 2018). Furthermore, hacking – which can be defined as the unauthorised use of, or access into, computers or network resources which exploits identified security vulnerabilities in networks – individuals, small and medium-sized enterprises (SMEs), and large organisations is a low-cost, low-risk proposition for criminal groups compared to making money from more traditional forms of crime (Home Office 2013 & National Cyber Security Centre 2017).

These organised crime groups operate either partially, predominately or solely online (UNODC 2019). However, there are cases of networks that have been formed and/or operate exclusively and/or predominantly online. These changes have allowed for increased cybercrime activity to take place in the region.

How are organised crime groups using cybercrime?

As we better understand the nature of organised crime in the Caribbean, we can start to look at what implications this has for cybercrime. Cybercrime can be divided into two main areas: cyber-enabled crimes, which are traditional crimes that can be increased in scale by using computers; and cyber-dependent crimes, which can only be committed through the use of online devices.

Cyber-enabled crimes: phishing, skimming and the use of social media

As we have already established the scope of organised crime activities in the Caribbean, we will first analyse cyber-enabled crimes across the region. Cyber-enabled crimes in the Caribbean have proliferated with increased internet usage, making individuals more vulnerable to nefarious activity. Phishing, which is when a criminal attempts to lure users to counterfeit websites in hopes of acquiring private information such as usernames or passwords, has become a common occurrence across the region. We have seen evidence of this in Dominica, where in 2021 spam emails with the subject 'Important Information Regarding your NBD Account(s)' were sent to individuals masquerading as being from the National Bank of Dominica Ltd, with the goal to steal the personal information of the individuals (National Bank of Dominica 2021). Furthermore, the National Commercial Bank (NCB) of Jamaica was also hit by a phishing and smishing (a phishing cybersecurity attack carried out over mobile text messaging) scheme, where customers were asked to click on links and give up personal information. The scammers would then carry out a follow-up phone call disguised as NCB employees with requests for the token code that customers are required to input to access certain services. The scammers would then use the code to add themselves as beneficiaries on the customers' accounts and to then transfer funds (Mckenzie 2022). Skimming, which is when thieves capture credit card information from a cardholder without their knowledge, is also taking place in Trinidad and Tobago. Skimmers have established a foothold in the country, with networks in operation – usually comprising foreigners, and more specifically Venezuelans – who have access to special equipment (Superville 2021).

Online romance or social networking/dating website frauds are also common across the Commonwealth Caribbean. This usually occurs when individuals are contacted via social networking or dating sites and persuaded to part with personal information or money following a lengthy online 'relationship' (Home Office 2013). There has been evidence of this in Guyana, where the Guyana Police Force alerted citizens concerning a scam involving persons suspected of pretending to be of Nigerian nationality. This scam would usually work by the individual sending a Facebook friend request to the victim and subsequently requesting their phone number for communication via WhatsApp. As time progresses, the criminal expresses an amorous interest in the intended victim and indicates that he/she would be sending some gifts for her/him, including jewellery (Guyana Standard 2020). The victim must then pay for these gifts to be released from customs; however, the gifts never materialise (ibid). There have also been reports of romance scams in Trinidad and Tobago, with around US$300,000 lost to these scams between 2020 to 2021 (*Trinidad and Tobago Guardian* 2021).

Across the Caribbean, but specifically in Barbados and Trinidad and Tobago, there have been instances where social media is used to expand organised crime groups' operations. In Trinidad and Tobago, social media has been used in several cases to recruit victims into human trafficking, as criminals move from social media sites to chatrooms to lure individuals (Douglas 2022). Authorities in Barbados have also noted an increase in social media being used to recruit victims into human trafficking (IOM 2015). In addition to this, criminal drug networks are abusing social media to expand their reach, create new markets and target new clientele. This has been exemplified in Belize, where gang members posted video on social media showing several unlicensed and prohibited firearms; this later went viral, helping to expand the group's reach and reputation (*Breaking Belize News* 2022).

Cyber-dependent crimes: hacking, ransomware, and Central Bank Digital Currencies

Cyber-dependent crimes are primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks, such as data gathered by hacking that can then be used to commit fraud. Across the Caribbean, we have seen a range of examples where hacking has taken place. In some instances, hacking takes place to deface government websites and promote specific ideologies or messaging. This was the case for The Bahamas in 2015, which saw its Ministry of Tourism websites hacked by members of a Tunisian Islamist activist group called the 'Fallaga Team' who were attempting to promote Islamist ideology (Eleutheran News 2015). In the same year, St Vincent and the Grenadines also had its official government website hacked by the radical Islamist group the Islamic State as it posted a photograph of a man on the back of a pickup truck firing a machine gun and the headline 'Hacked by Moroccanwolf – Islamic State' (CARICOM 2015). In 2019, Trinidad and Tobago government websites, including those belonging to the Ministry of National Security, the Immigration Division and the Attorney General's Office, were also hacked (Popplewell 2019). The hacker,

known as 'VandaTheGod', is Brazilian based and known for posting political messages. In this instance, he called the Government of Trinidad and Tobago corrupt and tried to make citizens hold the government accountable for its actions.

In some cases, hacking occurs and is then followed by a ransomware attack. These ransomwares attacks arise when hackers freeze access by victims to their data, either by locking the system's screen or by locking the users' files until a ransom is paid. This was the case in both Jamaica and Trinidad and Tobago, when the Massy Stores and Massy Distribution companies were hacked in 2022 and it was confirmed they were then victims of a ransomware attack. Five months after the attack, 17 gigabytes of data were dumped on the internet by cybercriminal group, Hive Ransomware, including personal information such as the names, addresses, taxpayer registration numbers, and signatures of Massy employees and contractors (Barrett 2022). The result of this data-dump was customers, employees, suppliers and the wider financial sector were then easy targets for hackers and fraudsters engaged in identity theft (ibid). In 2020, Ansa McAl, the Caribbean's biggest conglomerate, was also held hostage by a ransomware attack by criminal cybergang REvil in both Trinidad and Tobago and Barbados (Bridglal 2020). The criminal cybergang then released 12.9 gigabytes of Ansa's data, allegedly because the company refused to pay a ransom (ibid).

Both the hacking of Massy and Ansa McAl highlight how cybercrime is developing in the Caribbean region. The groups involved in the attack are ransomware-as-a-service (RaaS) or software-as-a-service (SaaS) operations, which is a business model between ransomware operators and affiliates in which the affiliates pay to launch ransomware attacks developed by operators. This means that individuals or groups both inside and outside the Caribbean who want to carry out cyberattacks no longer need to develop their own cyber skills, as these can be outsourced. Individuals or groups wanting to cause damage can now find hackers through the dark web and vice versa. These types of ransomware attacks could also be a sign that state-sponsored operations are becoming more frequent in the region, as nation-states seek to exploit Caribbean countries' vulnerabilities or gather intelligence.

Cryptocurrencies, which are a digital means of exchange that use cryptography for security, are increasingly used to make purchases across the world (Kurmi 2022). However, cryptocurrencies such as Bitcoin and Ethereum, are also used to move criminal proceeds. An example is the Mexican cartels, including the Jalisco New Generation Cartel and the Sinaloa Cartel, which use Bitcoin to launder money. These gangs typically split their illicit cash into small amounts and deposit them in various bank accounts, a technique known as 'smurfing' (Oré 2020). They then use those accounts to buy a series of small amounts of Bitcoin online, obscuring the origin of the money and allowing them to pay associates elsewhere in the world (ibid). With countries in the Caribbean being relatively open to cryptocurrencies, such as St Kitts and Nevis implementing legislation to

make crypto transactions easier, there are risks that these loopholes could be exploited by organised crime groups to launder money and carry out illegal goods transactions across the region.

The rise of cryptocurrencies in the region will also facilitate the use of the dark web, as transactions typically take place using digital currencies (George 2018). In the past, we have seen cartels exploring the dark web to locate buyers for large-scale cocaine shipments, while Central American gangs have used these sites to advertise their willingness to help with cross-border trafficking (ibid). Given the different types of criminal activity taking place in the region, there is a high chance the dark web is being used to facilitate organised criminal activities.

Caribbean central banks have also been active in exploring Central Bank Digital Currencies (CBDCs), with three launched so far in the region. These CBDCs are the digital form of a country's fiat currency and are similar to cryptocurrencies as they are digital tokens (BIS 2021). However, these CBDCs are issued by central banks and are not privately owned, in contrast to cryptocurrency. Nonetheless, there are still risks when it comes to cybersecurity and financial crime as although the central banks issue the currencies, they use third party infrastructure and software – which could potentially open the door to fraud and illicit payments. This will drive cybercriminals to seek ways to steal and abuse monetary systems as these CBDCs are further implemented across the region.

The impact of COVID-19 on cybercrime activities

The COVID-19 crisis accelerated changes that were already underway in the criminal economy, especially online. Industry data from all over the world showed meteoric rises in internet usage, 50 to 60 per cent higher, from 2020 to 2021 (Reitano and Shaw, 2021). Without increased cyber surveillance, criminals used the COVID-19 crisis to bombard individuals and businesses with misinformation, distribute malware, and conduct phishing attacks and scams (ibid).

There is clear evidence that the COVID-19 pandemic had implications for cybercrime activities in the Caribbean. The prevalence of a social media scam that involved the impersonation of government ministers in Grenada was a prime example of this issue. The scam consisted of offering COVID-19 assistance packages, ranging from US$30,000 to US$2 million, under the guise of being a government minister and declaring that to qualify, persons were expected to pay fees ranging from US$550 to US$50,000 (Wong 2021). The data breach of Jamaica's JamCOVID app, which left exposed quarantine orders for more than half-a-million travellers to the island, is another example of the lack of preparedness of Caribbean governments as the pandemic accelerated internet usage without accompanying security measures (Whittaker 2021). Several regional security experts have warned that the region is underprepared for cyberattacks as criminals continue to capitalise on the digital transformation that has taken place since the pandemic (ibid).

As we have seen, Caribbean Commonwealth countries are experiencing and are likely to experience more sophisticated and advanced types of cybercrime in the coming years. To be able to combat these issues, strong national cybercrime strategies will be needed, coupled with both adequate cybercrime legislation and suitable cybercrime prevention programmes. What Caribbean countries have done so far in this area will be explored in the following section.

Measures put in place to reduce cybercrime in the Caribbean

National cybercrime measures are still not widespread in the Caribbean, which makes fighting cybercrime a daunting task. As technology advances, cybercriminals will come up with more sophisticated ways of defrauding people and businesses – making cybercrime reduction strategies a crucial part of government policy.

Globally, several policies have already been put in place to reduce the effects of cybercrime. This is exemplified through the Budapest Convention on Cybercrime, which is the first international treaty seeking to address internet and computer cybercrime by harmonising national laws, improving investigative techniques and increasing co-operation among nations (Council of Europe 2022a). As Caribbean Commonwealth countries continue to move to a more digital space, it will be crucial that more emphasis is placed on the cybercrime policies that are currently in place, as well as ensuring that leaders in cybercrime policy in the region are able to pass down their learning to other countries with less developed cybercrime policies.

Commonwealth countries with a cybersecurity strategy

Some Commonwealth countries in the Caribbean have already implemented cybersecurity strategies to help fight cybercrime. For instance, Jamaica has the National Cybersecurity Strategy, developed in 2015; Trinidad and Tobago has a National Cybersecurity Strategy, developed in 2012; and Belize has its National Cybersecurity Strategy – Towards A Secure Cyberspace 2020–2023. These countries have all instituted cybersecurity strategies to strengthen technical measures, improve legal and regulatory frameworks, and raise public awareness, as well as implementing education campaigns to help ensure the confidence of citizens in cyberspace. These three countries are therefore ahead of other Commonwealth Caribbean states due to their creation of national policies and plans on cybercrime, as these documented plans help to provide a structure towards achieving the goal or objectives of protecting their nations against cyberattacks.

Jamaica's cybersecurity strategy focuses on establishing a framework built around public education and awareness, human resource and capacity building, legal and regulatory reforms within the legislative landscape, and technical measures to support resilient cybersecurity in the country. As a result, Jamaica's strategy represents a high-level

approach to cybersecurity by establishing a set of national objectives and priorities that must be met within a specific timeframe. Leadership, the protection of fundamental rights and freedoms, innovation and business development, risk management, shared responsibility, and sustainable resources are among the strategy's guiding principles. Because of their interconnectedness and the shared goal of promoting a resilient Jamaican economy on all fronts, the National Cybersecurity Strategy is implemented alongside other national development plans such as its Vision 2030 – National Development Plan, National ICT Policy and National Security Policy. The country is also leading the charge to significantly improve the Caribbean's response in tackling existing and emerging cybersecurity threats, having undertaken, in 2021, a Strategic Cybersecurity Training Needs Assessment. This will serve to identify the cybersecurity knowledge and skills required to deliver and sustain strategic responses to combat malicious cyber activities across the region.

Trinidad and Tobago's cybersecurity strategy focuses on five (5) key areas: creating an appropriate governance framework for cybersecurity; developing national incident management capabilities; developing government, civil and private industry collaborative relationships that work to effectively manage cyber risk and protect cyberspace; promoting a national culture of cybersecurity consistent with United Nations General Assembly Resolutions 57/239 entitled 'Creation of a global culture of cyber security' and 58/199 entitled 'Creation of a global culture of cyber security and the protection of critical information infrastructures'; and deterring cybercrime. The strategy aims to create a secure digital environment in which all users can fully enjoy the benefits of the internet. The country believes that the strategy will create a safe, secure and resilient cyber environment based on collaboration among all key stakeholders, allowing ICT to be used for the prosperity of all.

Belize's strategy, on the other hand, is focused on creating a secure and trustworthy digital environment that will aid in the promotion of economic growth and social inclusion in the Belize economy. The strategy was developed in collaboration with the government and other key stakeholders to provide guidance on key actions to be taken to improve Belize's overall preparedness and responsiveness to cybercriminal threats. Belize recognises that cybersecurity cannot be implemented in isolation and that it must be considered in the context of other policy decisions and national initiatives, such as the National Sustainable Tourism Master Plan 2030 and the National Growth and Sustainable Development Strategy 2016–2019, among others.

It will be crucial for these three Commonwealth Caribbean countries that these strategies do not remain documents exclusively, but that implementation also takes place in order to execute these cybercrime strategies.

Commonwealth countries currently working on a cybersecurity strategy and cybercrime legislation

Antigua and Barbuda is working on plans to update the cybersecurity legislature implemented in 2013, with an emphasis on widening the scope of cybercriminal activities. The new draft on ICT policies focuses on plans to create an independent regulatory authority and regulate the ICT space for safe and secure use of the internet and protection of intellectual property. Barbados, meanwhile, initiated its Data Protection Act (2019) in March 2021 and is currently focusing on updating its cybercrime legislation in accordance with the Budapest Convention on Cybercrime. Barbados is also currently discussing a draft bill on cybercrime with support from the Octopus Project of the Council of Europe. This bill is expected to be an update to the current Computer Misuse Act established in 2005.

In the Commonwealth of Dominica, legislation on computer and computer-related crimes has been established. In 2014, the Minister for Information Technology announced that the government intended to develop a cybersecurity strategy and would seek accession to the Budapest Convention on Cybercrime. However, this national cybersecurity strategy has been in the development stages since 2014 and has yet to be enacted. Nonetheless, the Government of Dominica is making significant strides to upgrade its resilience against potential cybercrimes by partnering with international organisations to achieve its goals. Grenada created a National Cyber Security Incident Response Team in 2022, with the aim of advising and supporting the government and the population on cyber-dependent crimes. Despite Grenada having an Electronic Crimes Bill, established in 2013 and reformed in 2016 and 2017, it is yet to develop a national cybersecurity strategy.

Other countries – such as St Vincent and the Grenadines (St Vincent and the Grenadines Cybercrime Act, 2016), Saint Lucia (Computer Misuse Act, 2008) and others listed in Table 3 – have cybercrime acts but are yet to proceed with discussions on national cybercrime strategies. With all Caribbean Commonwealth countries having implemented some form of cybercrime legislation, this demonstrates the willingness of these countries to tackle cybercrime across jurisdictions. A summary of cybercrime laws implemented in the Commonwealth Caribbean is presented in Table 3.

Table 3. Cybercrime laws in the Caribbean Commonwealth region

Caribbean country	Cybercrime laws
Antigua and Barbuda	Electronic Crimes Act, 2018
Bahamas, The	Computer Misuse Act (CMA), 2003
Barbados	Computer Misuse Act, 2005
Belize	Computer Misuse Act, 1996
Dominica	Computer And Computer Related Crimes Act, 2005
Grenada	Electronic Crimes Act, 2013
Guyana	Cyber Crime Act, 2018
Jamaica	Cybercrimes Act, 2015
St Kitts and Nevis	Electronic Crimes Act, 2009
Saint Lucia	Computer Misuse Act, Cap 8.14
St Vincent and the Grenadines	St Vincent and the Grenadines Cybercrime Act, 2016
Trinidad and Tobago	The Computer Misuse Act, 2000

Source: G5 Cybersecurity 2021

At the regional level, the Caribbean Community and Common Market (CARICOM) established an Implementation Agency for Crime and Security (IMPACS) in July 2006 and released its inaugural Cyber Security and Cybercrime Action Plan (CCSCAP). The action plan seeks to address the cybersecurity vulnerabilities in each participating Caribbean country and to establish a practical, harmonised standard of practices, systems and expertise for cybersecurity. Furthermore, it aims to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of cybercrime to take place. In 2019, IMPACS's objectives were given a boost when it secured funding from the European Union (EU) to undertake a 'Capacity Development' project across CARICOM nations. However, at the time of writing there had yet to be any public information concerning the success of CCSCAP within the Caribbean region.

Furthermore, the World Bank instituted the World Bank Caribbean Digital Transformation Project 2020–2026 to improve cybersecurity, data protection and privacy by reviewing and updating regional and national cybersecurity regulations and legislations. Finally, the Council of Europe held a conference on Cybercrime Strategies and Policies in 2019, with the aim of encouraging Caribbean countries to ratify the Budapest Convention in order for countries' legislation to be consistent with international cybercrime law.

The future of cybercrime strategies in the Caribbean

Following the expansion of the internet, an increase in broadband technologies and continued economic advancements, cybercrime has increased rapidly across the Caribbean region. The rise of cybercriminal activity can be attributed to increased levels of connectivity, remote working, reliance on technology and automation, which mean the risk of attacks is rising rapidly. This, coupled with an increasingly professionalised, specialised and collaborative underground supply chain of cybercriminals, suggests that growth in cyber criminality is likely to increase across the Caribbean. In order to limit the danger posed by cybersecurity issues and digitally enabled crime in the region, initiatives must focus on addressing the threats and vulnerabilities these states face. This should include improving technical standards and infrastructure, fostering national and regional regulations that would enforce penalties on cybercrime offenders, improving public awareness, and increasing both regional and international co-operation. To be able to achieve this, co-operation between key stakeholders is necessary. Given the multisectoral and cross/multinational impacts of cybercrime, an effective response to the issue will require collaboration at the cross-sectoral, bilateral and multinational levels. A discussion of the role of key stakeholders in fighting cybercrime across these different areas going forward is therefore provided below. Lessons learnt from other regions are also provided.

Government and the police

The role of government in the Caribbean Commonwealth is predominantly to provide both a legislative and regulatory environment that protects businesses and citizens from cybercrime. This includes collaboration on legislation at the international level to allow for harmonised legislation for cross-border, international crimes that need an international response. This is especially crucial in the Caribbean, given the interconnected nature of cybercrimes across the region. Furthermore, legislation can also consider criminalising specific types of cybercrime that have caused problems at the national or regional levels to demonstrate the legislator's willingness to address the issue (Global Action on Cybercrime 2019). This legislation also needs to be sufficiently abstract so that it is able to endure over time as cybercriminals evolve their operations. This way of creating regulation has been exemplified in Jamaica, as its legal and regulatory framework aims to carry out periodic reviews of existing laws to ensure parity with the dynamic nature of cybercrimes.

It is also crucial that Caribbean governments invest in institutions that permit action against cyberthreats, such as funding towards the development of remedial and preventative measures. This includes the police in the Caribbean, as they play a key role in cybersecurity. However, this will require new skills and competencies that extend well beyond those needed for traditional policing. Training will be essential for the police to maintain pace with evolving areas of cybercrime and capacity building in this respect will be crucial. This could take place at the regional level, given the limited resources of

certain Commonwealth Caribbean countries as well as the overlap of many types of cybercrime across the region. Such training has already taken place, with a collaboration between the Commonwealth Secretariat and the Caribbean Community Implementation Agency for Crime and Security providing a four-day training session in Barbados to teach Caribbean police and legal experts how to use electronic evidence in cybercrime cases (Commonwealth Secretariat 2016).

The private sector

Given the limited resources of Caribbean Commonwealth countries, the private sector can also play a role in mitigating the impacts of cybercrime. Overall, the private sector in the region must protect itself and its clients from threats by ensuring basic cybersecurity measures are in place. Furthermore, in the Caribbean context, because attacks usually have an impact at the regional level, making sure several governments work together to ensure the best possible sharing of knowledge among all countries on the types of evidence that can be provided by the private sector will be crucial. The creation of private–public co-operative forums and joint tasks force initiatives will also provide robust preventative and response measures to cybercrime in the region. In addition to this, it would be worthwhile for private sector companies to adhere to international best practice standards, such as ISO/IEC 27032, as well as establish an industry co-regulatory approach such as the development of industry standards in relation to mandatory cyber-hygiene practices.

Although there is reference to ensuring the private sector is involved in cybersecurity across Caribbean countries within national cyber security strategies, the implementation of this seems to be lacking. However, one country leading the way in this area is The Bahamas, which has seen top IT professionals across a range of sectors participate in the government's first national cybersecurity assessment session, helping to provide a unique perspective on cybercrime issues (Eyewitness News 2021).

Prevention strategies from citizens and civil society

The involvement of citizens and civil society will also be crucial in combatting cybercrime going forward. Ultimately, citizens will be the ones who are the victims of cybercrime as not only will they suffer directly from these crimes, but also from the loss of income due to the closure of companies and lost opportunities and investments if the Caribbean is not seen as a place where business can take place safely. Citizens who have been victimised are also able to fully understand these cybercrimes and can therefore provide a unique perspective when it comes to carrying out public awareness campaigns or establishing prevention strategies in collaboration with civil society. This is increasingly important, given the high levels of digitally connected citizens across the Caribbean region. Consideration should also be given to the use of sensitisation sessions for different age

groups: for example, cyberbullying and social media safety for schools, online business safety for micro and small and medium-sized enterprises (MSMEs) and sole traders online, as well as general online safety for members of the public.

Evidence of collaboration between governments, civil society and citizens around cybercrime has already been seen in Belize, where a cross-section of national stakeholders worked together in order to develop the National Cybersecurity Strategy, 2020–2023 (Council of Europe 2022b).

International partners

Across the Caribbean, we have seen examples of successful cybercrime strategies and interventions, highlighting the importance of international partnerships in this area as Caribbean states can learn from each other. Furthermore, evidence has shown throughout this paper that in some cases, cybercrimes can be interconnected at the regional level, making a further case for international co-operation. The harmonisation of laws, co-ordinated investigative techniques, and improved access and collaboration with respect to electronic evidence are some of the ways that Caribbean countries will be able to improve this co-operation to reduce cybercrime. The CARICOM Cyber Security and Cybercrime Action Plan is an excellent example of this co-operation at the regional level as a co-ordinated framework has been created, helping to avoid duplication of effort in reducing cybersecurity issues and to disseminate lessons learnt from larger, or more technically mature, countries to smaller states. It may also be worthwhile considering greater enforcement of cross-border co-operation through mutual legal assistance treaties between different Caribbean states. Finally, the involvement of Caribbean Commonwealth states in the current international discourse at the UN level within the Open-Ended Working Group (OEWG) on the use of ICTs could be a crucial way to ensure that Caribbean countries are actively involved in developing rules, norms and principles of responsible behaviour in this area and helping them to understand the extent of potential threats in the sphere of information security.

We have also seen evidence of cyberattacks in the Caribbean being carried out far beyond its regional borders and therefore co-operation further afield is necessary. Cybercriminals will often seek out victims in a different jurisdiction to where they are based to reduce the evidence against them being readily available. Going forward, as technologies improve, these types of cyberattacks will also become easier to carry out. The US, the EU and the United Kingdom (UK) have already provided international support and capacity building by hosting, in collaboration with several Caribbean countries, cyber capacity workshops and legislation working groups to help strengthen cybercrime policies.

Lessons learnt: Five Eyes

As we have established, collaboration with international partners is essential for Caribbean Commonwealth countries to be able to tackle cybercrime effectively. In addition, although Caribbean governments do not have equivalent resources to those

of advanced states, there are still lessons that can be learnt from their approaches and interventions to allow for maximum impact. This is especially the case for 'Five Eyes', which is an intelligence alliance between the world's five leading cybersecurity authorities, Australia, Canada, New Zealand, the UK, and the US. Their forward-thinking cyber strategies can help Caribbean states develop long-term policies to address cybersecurity challenges in the future.

The first lesson from these strategies is the extensive research that went into developing them, including extensive public consultation processes that included a diverse range of stakeholders such as academics, technology experts and business leaders, to name a few. For example, Public Safety Canada received more than 2,000 comment submissions for the development of its 2019–2024 Cyber Security Strategy (Public Safety Canada 2019). Second, the importance of protecting critical national infrastructure is also highlighted as a priority throughout all five cybersecurity strategies. This is especially highlighted in New Zealand's cybersecurity strategy, given several attacks against critical infrastructure that were a result of hacking tools becoming more accessible and public services being moved online. Finally, identifying key threat groups such as nation-states, foreign state-sponsored actors and proxy actors will help towards ensuring adequate measures are put in place before attacks occur. The UK has highlighted this in its cyber strategy, suggesting that as cyber warfare is to become an essential part of armed conflicts, a country's defence capabilities need to match this trend.

Learning from these countries and understanding these future trends will be essential for Caribbean Commonwealth countries to remain resilient in the face of growing cyberattacks.

Conclusion

If Caribbean Commonwealth countries do not take adequate measures to protect themselves and their citizens from cybercrime, the impact is likely to be large. As discussed, cybercrime tends to affect small countries more than larger countries due to the larger countries' ability to cushion the effect better at the national level compared to a smaller state, making Caribbean Commonwealth countries particularly vulnerable.

This is especially true given the increased levels of internet usage, high levels of mobile cellular subscriptions and a lack of secure internet servers in certain Caribbean Commonwealth countries, which all contribute to cybersecurity risks. Organised crime groups in the region have already started to exploit these developments through a range of methods. These include cyber-enabled crimes such as phishing, skimming and the use of social media, but also cyber-dependent crime including hacking, ransomware and through Central Bank Digital Currencies. The COVID-19 crisis has accelerated changes that were already underway in the online criminal economy, with implications for cybercrime activities in the Caribbean.

To address these issues, some Commonwealth countries have already put in place measures to curb cybercriminal activity. Jamaica, Trinidad and Tobago, and Belize have setup national cybersecurity strategies, aiming to improve legal and regulatory frameworks, strengthen technical measures and raise public awareness. All Caribbean Commonwealth countries have some form of cybercrime law, demonstrating their willingness to tackle cybercrime across jurisdictions. At the regional level, CARICOM IMPACS has brought together Caribbean nations to address cybersecurity vulnerabilities and establish practical, harmonised standards of practices, systems and expertise for cybersecurity.

For Caribbean Commonwealth countries to ensure they continue to be protected in the face of increasing cybercrime threats, building on current initiatives will be necessary. This includes ensuring that governments collaborate on legislation at the international level to allow for harmonised legislation for cross-border, international crimes that need an international response. Furthermore, training will be essential if police forces are to be able to keep up with evolving areas of cybercrime. Given the limited resources of Caribbean Commonwealth countries, the private sector can also play a role in mitigating the impacts of cybercrime by ensuring knowledge sharing of evidence takes place at the regional level. The involvement of citizens and civil society will also be crucial going forward, as citizens who have been victimised are able to fully understand these crimes and can therefore provide a unique perspective and establish prevention strategies in collaboration with civil society. Finally, international partnerships will be necessary for Caribbean Commonwealth states, as this will allow countries to learn from one another while at the same time helping to combat cybercrime at the regional level.

Finally, to ensure Caribbean Commonwealth countries are forward looking in their approaches, it is important for them to pay attention to leading cybersecurity authorities, such as Five Eyes, for lessons learnt and guidance. This will mean that Caribbean countries' strategies are prepared for the long term and that they continue to adapt and innovate to protect and promote their cyberspaces.

References

Barrett, L (2022), 'Massy's ransomware attack exposes consumers and companies', eSponsored, Jamaica Gleaner, available at: https://jamaica-gleaner.com/article/esponsored/20221017/massys-ransomware-attack-exposes-consumers-and-companies (accessed 15 August 2022).

Bank of International Settlements (2021), 'BIS Innovation Hub work on central bank digital currency (CBDC)', available at: www.bis.org/about/bisih/topics/cbdc.htm (accessed 15 August 2022).

Breaking Belize News (2022), 'Fines and suspended sentences for men who pled guilty to making gang video', Belize News and Opinion, available at: www.breakingbelizenews.com/2022/10/12/fines-and-suspended-sentences-for-men-who-pled-guilty-to-making-gang-video/ (accessed 3 October 2022).

Bridglal, C (2020), 'Ansa McAl IT systems recovery "largely complete" after hack attack', *Trinidad and Tobago Newsday*, available at: https://newsday.co.tt/2020/10/27/ansa-mcal-it-systems-recovery-largely-complete-after-hack-attack/ (accessed 20 October 2022).

Caribbean Community (CARICOM) (2015), 'St Lucia tightens cyber security after hacking of SVG site', available at: https://caricom.org/st-lucia-tightens-cyber-security-after-hacking-of-svg-site/ (accessed 15 August 2022).

Check Point Research (2022a), 'Cyber Attacks Increased 50% Year over Year', available at: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ (accessed 15 August 2022).

Check Point Research (2022b), 'Weekly Cyber Attacks increased by 32% Year-Over-Year; 1 out of 40 organizations impacted by Ransomware', available at: https://blog.checkpoint.com/2022/07/26/check-point-research-weekly-cyber-attacks-increased-by-32-year-over-year-1-out-of-40-organizations-impacted-by-ransomware-2/ (accessed 15 August 2022).

Commonwealth Secretariat (2016), 'Commonwealth cybercrime experts in Barbados call for robust cybersecurity', The Commonwealth, available at: https://thecommonwealth.org/news/commonwealth-cybercrime-experts-barbados-call-robust-cybersecurity (accessed 3 October 2022).

Comply Advantage (2022), 'AML In The Caribbean: UBOs and Shell Companies', available at: https://complyadvantage.com/insights/aml-carribbean-ubos-shell-companies/ (accessed 20 October 2022).

Council of Europe (2022a), 'The Budapest Convention', Cybercrime, available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 3 November 2022).

Council of Europe (2022b), 'Status regarding Budapest Convention', available at: www.coe.int/ru/web/octopus/-/belize?inheritRedirect=true (accessed 3 October 2022).

Cybersecurity Ventures (2022), *Boardroom Cybersecurity 2022 Report*, available at: https://cybersecurityventures.com/boardroom-cybersecurity-report/ (accessed 15 August 2022).

Douglas, S (2022), 'Cox: Human traffickers target youngsters on social media', *Trinidad and Tobago Newsday*, PBJ Learning, available at: https://pbjlearning.com/2022/09/07/cox-human-traffickers-target-youngsters-on-social-media-trinidad-and-tobago-newsday/ (accessed 3 October 2022).

Eleutheran News (2015), 'Ministry of Tourism updates on the hacking of bahamas.com', available at: https://eleutheranews.com/?p=4719 (accessed 20 October 2022).

Europol (2020), 'Catching the virus: cybercrime, disinformation and the COVID-19 pandemic', 3 April, 3, available at: www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_class="•-No-break">pandemic_0.pdf (accessed 3 November 2022).

Eyewitness News (2021), 'Top IT professionals participate in govt's first-ever national cybersecurity assessment session', Eyewitness News, available at: https://ewnews.com/top-it-professionals-participate-in-govts-first-ever-national-cybersecurity-assessment-session (accessed 15 August 2022).

G5 Cybersecurity (2021), *2021 Caribbean Cyber Security and Privacy (CSPR) Report*, available at: https://g5cybersecurity.com/downloads/reports/G5CS-2021-Caribbean-Cyber-Security-and-Privacy-Report-CSPR.pdf (accessed 15 August 2022).

George, J (2018), 'Organized Crime and Cyber Crime in Latin America and the Caribbean', available at: www.linkedin.com/pulse/organized-crime-cyber-latin-america-caribbean-jaevon-george-bsc/?trk=articles_directory (accessed 15 August 2022).

Global Action on Cybercrime (2019), Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community, available at: https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c (accessed 15 August 2022).

Global Initiative (2020a), Global Organized Crime Index – Jamaica, available at: https://ocindex.net/assets/downloads/english/ocindex_profile_jamaica.pdf (accessed 3 November 2022).

Global Initiative (2020b), Global Organized Crime Index – Trinidad and Tobago, available at: https://ocindex.net/assets/downloads/english/ocindex_profile_trinidad_and_tobago.pdf (accessed 3 November 2022).

Global Initiative (2020c), Global Organized Crime Index – Dominica, available at: https://ocindex.net/assets/downloads/english/ocindex_profile_guyana.pdf (accessed 3 November 2022).

Guyana Standard (2020), 'Police warn of online scam targeting women', available at: www.guyanastandard.com/2020/11/26/police-warn-of-online-scam-targeting-women/ (accessed 20 October 2022).

Hamilton-Davis, R (2023), 'Amcham: Crime, ease of doing business among top concerns', *Trinidad and Tobago Newsday*, available at: https://newsday.co.tt/2023/01/19/amcham-crime-ease-of-doing-business-among-top-concerns/ (accessed 3 November 2022).

Home Office (2013), 'Cyber-dependent crimes', chapter 1 in *Cyber crime: A review of the evidence Research Report 75*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf (accessed 15 August 2022).

InSight Crime (2018), 'Caribbean Profile', InSight Crime, available at: https://insightcrime.org/caribbean-organized-crime-news/caribbean/ (accessed 18 October 2022).

International Organization for Migration (IOM) (2015), *Exploratory Assessment of Trafficking in Persons in the Caribbean Region: The Bahamas, Barbados, Guyana, Jamaica, The Netherlands Antilles, St. Lucia, Suriname and Trinidad and Tobago,* second edition, available at: https://publications.iom.int/system/files/pdf/exploratory_assessment2.pdf (accessed 15 August 2022).

Katz, C (2015), *An Introduction to the Gang Problem in the Caribbean*, available at: www.researchgate.net/publication/282981024_An_Introduction_to_the_Gang_Problem_in_the_Caribbean (accessed 15 August 2022).

Kurmi, S (2022), 'Investing In Cryptocurrency', Forbes Advisor UK, available at: www.forbes.com/uk/advisor/investing/cryptocurrency/ (accessed 3 November 2022).

Mckenzie, R (2022), 'Suspects arrested in connection with $45 million theft at JMMB', Sleek Jamaica Media, available at: https://sleekjamaica.com/suspects-arrested-in-connection-with-45-million-theft-at-jmmb/ (accessed 3 November 2022).

Moore, M (2017), *Cybersecurity Breaches and Issues Surrounding Online Threat Protection*, a volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, IGI Global, USA.

National Bank of Dominica (2021), 'Statement on SPAM Emails', National Bank of Dominica Ltd, available at: https://nbdominica.com/statement-on-spam-emails/ (accessed 24 October 2022).

National Cyber Security Centre (2017), 'Cybercrime – understanding the online business model', available at: www.ncsc.gov.uk/files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf (accessed 15 August 2022).

Oré, D (2020), 'Latin American crime cartels turn to cryptocurrencies for money laundering', US, available at: www.reuters.com/article/mexico-bitcoin-insight-idUSKBN28I1KD (accessed 15 August 2022).

Popplewell, G (2019), 'Guy Fawkes makes cameo appearance on hacked Trinidad and Tobago government websites', *Global Voices*, available at: https://globalvoices.org/2019/07/26/guy-fawkes-makes-cameo-appearance-on-hacked-trinidad-and-tobago-government-websites/ (accessed 20 October 2022).

Public Safety Canada (2019), National Cyber Security Strategy, available at: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf (accessed 3 October 2022).

Reitano, T and M Shaw (2021), *Criminal Contagion: How Mafias, Gangsters and Scammers Profit from a Pandemic*, Hurst Publishers, United Kingdom.

Superville, S (2021), 'Bank card skimming concern for cybersecurity in Trinidad and Tobago', *Trinidad and Tobago Newsday*, available at: https://newsday.co.tt/2021/10/24/bank-card-skimming-concern-for-cybersecurity-in-trinidad-and-tobago/ (accessed 3 October 2022).

Trinidad and Tobago Guardian (2021), 'FIUTT detects $2.3 million loss from victims of romance scams', available at: https://guardian.co.tt/news/fiutt-detects-23-million-loss-from-victims-of-romance-scams-6.2.1379265.39b80d75c7 (accessed 15 August 2022).

UN Office on Drugs and Crime (UNODC) (2012), 'Digest of Organized Crime Cases: A compilation of cases with commentaries and lessons learned', available at: www.unodc.org/documents/organized-crime/EnglishDigest_Final301012_30102012.pdf (accessed 15 August 2022).

UNODC (2013), 'Draft Comprehensive Study on Cybercrime', available at: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 15 August 2022).

UNODC (2019), 'Organized Crime / Cybercrime Module 13 Key Issues: Criminal Groups Engaging in Cyber Organized Crime', available at: www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html (accessed 15 August 2022).

Verizon (2022), *Verizon's 2022 Data Breach Investigations Report*, available at: www.verizon.com/business/resources/reports/dbir/ (accessed 15 August 2022).

World Development Indicators (WDI) (2022a), World Development Indicators (WDI), International Bank for Reconstruction and Development/The World Bank, Washington, DC, available at: https://databank.worldbank.org/source/world-development-indicators

WDI (2022b), 'Internet Penetration Over Time', available at: https://databank.worldbank.org/Internet-Penetration-over-time/id/3bdec3cd (accessed 15 August 2022).

White House (2022), National Drug Control Strategy Caribbean Border Counternarcotics Strategy, available at: www.whitehouse.gov/wp-content/uploads/2022/04/Caribbean-Border-Counter-Narcotics-2022Strategy.pdf (accessed 18 October 2022).

Whittaker, Z (2021), 'How Jamaica failed to handle its JamCOVID scandal', available at: https://techcrunch.com/2021/04/03/jamaica-jamcovid-amber-group/?guccounter=1 (accessed 18 October 2022).

Wint, A (2003), *Competitiveness in Small Developing Economies*, UWI Press, Kingston.

Wilson-Harris, N (2019). 'Cyber thieves run rampant - Jamaica suffering billions in losses from online crime', Jamaica Gleaner, available at: https://jamaica-gleaner.com/article/lead-stories/20190630/cyber-thieves-run-rampant-jamaica-suffering-billions-losses-online (accessed 22 February 2023).

Wong, M (2021), 'Grenadians urged not to fall for COVID assistance scams online', Loop News, available at: https://caribbean.loopnews.com/content/grenadians-urged-not-fall-covid-assistance-scams-online (accessed 20 October 2022)