THE NATIONAL RESEARCH INSTITUTE
PAPUA NEW GUINEA

SPOTLIGHT

STRATEGIES FOR COMBATING CYBERCRIMES IN PAPUA NEW GUINEA

Olugbenga Ige

Volume 16, Issue 1
www.pngnri.org

Key Points

- The development of internet created a new scene of criminal activity that targets computer or uses computer network device to operate (cybercrime).
- Activities associated with cybercrimes in Papua New Guinea (PNG) include offences related to the integrity of data and electronic systems or devices, computer-related offences and content-related offences.
- The capacity of Royal PNG Constabulary Cybercrime Unit must be enlarged to address cybercrime issues.
- Cybercrimes can be addressed using the Cyber Police Portal PNG and the PNG Recovery Asset Team.
- Bottom-up educational interventions have the potential to promote cybersecurity in PNG.

inquire
inform
influence

January 2023

THE NATIONAL RESEARCH INSTITUTE
PAPUA NEW GUINEA

SPOTLIGHT
January 2023

STRATEGIES FOR COMBATING CYBERCRIMES IN PAPUA NEW GUINEA

By Olugbenga Ige

In the recent past, most crimes occurred in the physical environment or space. These occurrences were subjected to the criminal codes that were promulgated during that period. The advancement of Information and Communications Technology (ICT) and other related communication capabilities, especially the internet that powered the third industrial revolution, created a space that provides some people with the opportunities to engage in ICT related crimes known as 'cybercrime'. The increased use of ICT by people created different new forms of criminal activities that have been a challenge for the law enforcement agencies in different countries; unlike the traditional crimes committed that can be unravelled by crime detectors in a short period of time. The technicalities inherent in crimes committed via the internet, that is cyberspace and the essential nature of information and public security, made the Government of Papua New Guinea (GoPNG) to promulgate the *Cybercrime Act 2016*. The cybercrime law is the main document being used for regulating the use of the internet in the country (Galgal, 2017). This article provides highlights on the multi-faceted nature of cybercrimes.

What is cybercrime?

Cybercrime is any criminal activity that targets or uses a computer, a computer network or a related network device to operate (Kaspersky, 2022). It can also be referred to as cyberspace crime, computer crime, computer-related crime, electronic crime, e-crime, technology-enabled crime or high-tech crime (Philips et al., 2022). Another terminology that has evolved in the developing nations in Africa on cybercrime are 'Yahoo Yahoo' (Ige, 2020) and 'Yahoo Plus' (i.e., Scammers using voodoo or customary charms and incantations to support or facilitate criminal activities in the cyberspace).

The cybercrime is often committed by cybercriminals or hackers with the primary aim of making money. However, some of the hackers operate to destroy computers or associated networks. Cybercrime operates in a collection of all information systems known as cyberspace (Zhang et al., 2015). Unlike the traditional crimes such as burglary and car theft that operates in a local environment, cybercrimes are global and can have strong impacts on different countries (Anderson et al., 2013). Cybercrime exceeds physical or geographical boundaries and is carried out with less effort, greater ease and at much greater speed than traditional crimes (Maras, 2014). For instance, cyberattacks on the Vanuatu Government Broadband Network on 6 November 2022 have disabled the websites of the Pacific island's parliament, police and prime minister's office, brought down the email system, intranet and online databases of schools, hospitals and paralysed other emergency services of government's department to the citizenry with the cyberhackers demanding ransom that the Vanuatu government has turned down (BBC, 2022). Furthermore, these cyberattacks on Vanuatu's government internet servers has incapacitated about 315,000 residents across several islands struggling to finalise important tasks like tax payment, invoicing bills and procuring licences and travel documents (BBC, 2022). Thus, there is a need to ensure the security of cyberspace.

Types of cybercrime

Cybercrimes can be classified into two basic strands: crime committed using computers, computer networks or other related ICTs, and crime that targets computers using viruses to damage the computers and associated device (EUROPOL, 2018). According to Kaspersky (2022), there are several types of cybercrime, which include the following:

- Email and internet fraud
- Theft of personal information (identity fraud)
- Theft of credit/debit card data or financial information
- Theft and sale of corporate data
- Demand money from victims as a ransom to prevent a threatened attack
- Access of government or company data by hackers (cyberespionage)
- Interfering with ICT systems to compromise a network
- Infringement of copyrights
- Soliciting, producing or processing child pornography online
- Illegal gambling in the cyberspace
- Selling of illegal items online

Components of cybercrime in PNG

According to the PNG *Cybercrime Code Act* 2016, there are four divisions of activities that constitute cybercrimes in the country (Government of Papua New Guinea, 2016). The four divisions and activities are the following:

Division 1: Offences related to the integrity of data and electronic systems or devices

- Unauthorised access or hacking
- Illegal interception
- Data interference
- System interference
- Data espionage
- Illegally remaining

Division 2: Computer-related offences

- Electronic fraud
- Electronic forgery
- Electronic gambling or lottery by a child
- Identity theft
- Illegal devices

Division 3: Content-related offences

- Pornography
- Child pornography
- Child online grooming
- Animal pornography
- Defamatory publication
- Cyber bullying
- Cyber harassment
- Cyber extortion
- Unlawful disclosure
- Spam

Division 4: Other offences

- Cyber attack
- Online copyright infringement
- Online trademark infringement
- Patent and industrial designs infringement
- Unlawful advertising

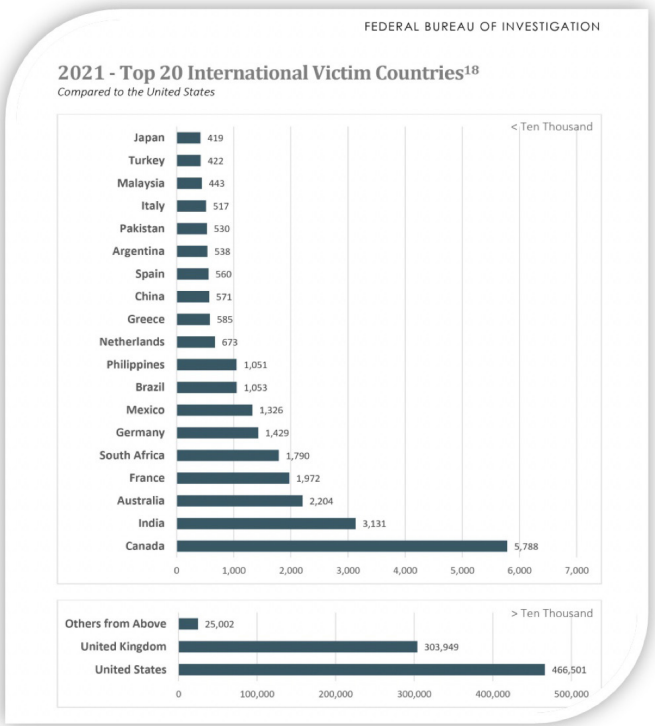
Approaches to cybercrime prevention in PNG

- **Building the capacity of Royal PNG Constabulary (RPNGC) Cybercrime Unit**

In PNG, law enforcement services are provided to the citizenry by RPNGC, that is, a part of PNG Government's law and justice sector. The RPNGC has a functional but young cybercrime unit (including Airport Police Unit) saddled with the responsibility of investigating and enforcing cybercrime-related laws and regulations in PNG. The capacity of the police in the cybercrime unit needs to be strengthened to understand the universal challenges of curbing the menace of cybercrimes from the spate of current cybercriminal activities reported in Australia (Figure 1). The 2021's Internet crime report confirms that Australia has about 2,204 victims of cybercrime. The data released by the Federal Bureau of Investigation makes Australia the third among countries whose citizens are most vulnerable to cyber scammers after United States, Canada, and India.

The security watchdog such as Interpol reported that PNG is situated on maritime and air crossroads between Asia and the South Pacific. The Interpol reasoned that the geographic location of the country to Australia makes it attractive to transnational organised crime gangsters (INTERPOL, 2023). It was on this note that the policemen saddled with cybercrime-related investigations would immensely benefit from capacity building programmes facilitated by policemen at the National White Collar Crime Center in the United States, Cyber Police in India, Economic and Financial Crimes Commission (EFCC) in Nigeria, National Cybercrime Coordination Centre (NC3) in Canada, the Australian Federal Police, Action Fraud in the United Kingdom, and the French Expert Center Against Cybercrime (CECyF).

Figure 1: 2021 - Top 20 International Victim Countries compared to the United States



*The charts list the top 20 countries by number of total victims as compared to the United States. The specific number of victims for each country is listed in descending order to the right of the graph.

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

- **Cyber Police Portal PNG**

The United States, United Kingdom, Canada, India, Australia, and France have specialised agencies that attend to incidences of cybercrime beside the National Police. In South Africa, the responsibility of enforcing the Cybercrimes Act 19 of 2022 rests with the South African Police Service (SAPS), but with a dedicated cybercrime awareness portal that has

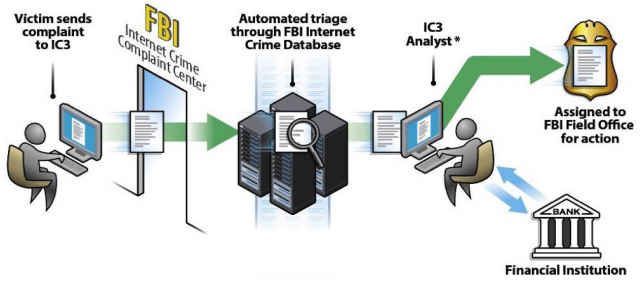
local and international resources to educate its citizenry. To effectively tackle the incidences of cybercrimes in Papua New Guinea, university researchers and the government should support the RPNGC to design "Cybercrime.org.pg", or "ReportCyber.gov.pg". However, PNG should not wait for incidences of cybercrimes to escalate before establishing a specialised or an independent agency to enforce cybercrime laws in the country.

In the meantime, a dedicated cybercrime portal administered by the RPNGC will complement the manual or traditional means of reporting cybercrime offenders at the Airport Police Station, 7–Mile, where the new special unit on cybercrime is located.

- **Constitute The Papua New Guinean Recovery Asset Team**

This concept is adapted from the United States Internet Crime Complaint Center [IC3] (Figure 2). This approach would enable PNG Cyber Crime Unit to balance communication with the financial institutions in the country, and assist RPNGC to freeze funds for Papua New Guinean that makes transfers to local accounts or accounts domiciled in the nations located in Pacific Islands under fraudulent premises. The model is presented in Figure 2:

Figure 2: The Adapted Recovery Asset Model Team (RAT Model)



* If these criteria are met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, PNGRAT contacts the appropriate RPNGC field office(s).
Source: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

The PNGRAT will act as an electronic liaison between RPNGC and financial institutions supporting statistical and investigative analyses.

- **School-Community Based Educational Interventions**

In some countries, researchers often overlook the necessity of supporting the technical programs, encryptions, or firewalls designed by computer experts with "EDUCATION" since human beings are at the centre or end users of these technical-related solutions. In order to educate school children and community populace in PNG, the cybercrime-related themes and means of the crimes should be infused into school curricula for Social Science and Information and Communication Technology. Another veritable approach is to build the capacity of the teeming school children and the local communities in PNG using the Community Action Model (CAM) (Ige, 2020, p.2713) shown in Figure 3. To operate the educational intervention with the CAM, researchers or facilitators are to follow these steps:

- Train the participants on collaborating to solve social problems. Name the issue as "Cybercrime". Choose the area of focus from Divisions 1, 2, 3, or 4 of the *Cybercrime Code Act* 2016.
- Support the selected members of the community or school to define, identify and engage to diagnose common crimes that are committed by residents in the cyberspace or those cybercrimes that the members of the selected community or schools are vulnerable to.
- The members of the selected local community or school should analyse the outcomes of their group diagnoses of the problem of "cybercrimes".
- At this stage, the members of the selected local community or school will select participatory activities to stop the identified cybercrimes.
- The local channels or school channels of maintaining and enforcing the foci of action selected from the *Cybercrime Code Act* 2016 are identified and sustained or reinforced.

Figure 3. Community Action Model

Source: Lavery et al. (2005).

Conclusion

This article provides insights on the strategy that can be used to address cybercrimes in PNG. The country has done well by promulgating laws for addressing incidences of cybercrimes

to enable the PNG Government guarantee the cyber well-being of its citizens. However, it is important for the RPNGC to understand that the current law enforcement structure, though good but may not be able to address organised cybercrimes and large-scale internet fraud in its current form. This research is a timely call to the RPNGC to take further administrative and legal initiatives to expand the structure of cybercrime prevention by building the capacity of its staff, creating modern information and intelligence collection electronic platforms to address the menace of cybercrimes in the country. The RPNGC should consider using educational approaches to orientate the PNG citizenry on the ills of cybercrimes and the channels of protection available to PNG residents venturing into the cyberspace in any country of the world. The ideas presented in this article will assist the RPNGC, policy makers, and researchers to improve on the current structure of enforcing cybersecurity laws in PNG. This paper will also serve as a guide for Government of PNG when considering revising policies and strategies related to cybercrimes and creating cosmopolitan cyber police that can become a model to other nations in the Pacific Islands.

References

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T., & Savage, S. (2013). *Measuring the Cost of Cybercrime*. In: Böhme, R. (eds) *The Economics of Information Security and Privacy*. Pp 265-300. Springer, Berlin, Germany.

BBC (2022). Vanuatu: Hackers strand Pacific island government for over a week. British Broadcasting Corporation (BBC). https://www.bbc.com/news/world-asia-63632129 Accessed 20 November 2022.

European Cybercrime Centre [EC3] EUROPOL. (2018). *Internet organized crime threat assessment* [IOCTA]. Accessed 25 October 2022 at https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Galgal, K. (16 March 2017). *Developing PNG's cybercrime policy: Local contexts, global best practice*. Accessed 25 October 2022 at https://www.lowyinstitute.org/the-interpreter/developing-png-s-cybercrime-policy-local-contexts-global-best-practice.

Government of Papua New Guinea (2016). The National Cyber-crime Code Act issued in 2016. Government of Papua New Guinea, Port Moresby. https://www.parliament.gov.pg/index.php/bills-and-legislation/view/cybercrime-code-act-2016 Accessed 30 January 2022.

Ige, O.A. (2020). School-based Cybersecurity Education Programme for schoolchildren in South Africa! A Timely Call from Bloemfontein. *Universal Journal of Educational Research,* 8(6), 2710 – 2716. http://dx.doi.org/10.13189/ujer.2020.080656.

INTERPOL (2023). How INTERPOL supports Papua New Guinea to tackle international crime.https://www.interpol.int/en/Who-we-are/Member-countries/Asia-South-Pacific/PAPUA-NEW-GUINEA Accessed 30 January 2023.

Kaspersky (2022). *What is cybercrime? How to protect yourself from cybercrime*. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime. Accessed on 23 November 2022.

Lavery, S.H, Smith, M.L., Esporza, A.A., Hrushow. A., Moore, M., & Reed, D.F. (2005). The community action model: *A community-driven model designed to address disparities in health. Am J Public Health,* 95(4), 611-616.

Maras, M.H. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence*. Second edition. Jones and Bartlett.

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., & Aiken, M.P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 2(2), 379-398. MDPI AG. http://dx.doi.org/10.3390/forensicsci2020028.

The Papua New Guinea Government. (2016). *Cybercrime Code Act 2016*. Retrieved 4 November 2022 https://www.nicta.gov.pg/regulatory/internet/cybercrime-cybersecurity/

Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Lin, J. (2015). Survey on cyberspace security. *Sci. China Inf. Sci*. 58, 1-43 (2015).

About the Author

Olugbenga Ige is a Senior Research Fellow, Building Safer Communities Research Program at the PNG National Research Institute. His research interests include cybersecurity education, social sciences education, ICT in education, gender studies, society and culture, and community-based research.

Acknowledgements

The author would like to thank the Federal Bureau of Investigation (FBI) and National White Collar Crime Center (IC3) for providing the data used in this study at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf