

E-Journal of Humanities, Arts and

Social Sciences (EHASS)

ISSN – Online 2720-7722 | Print 2821-8949 Volume 4 Issue 3 – March 2023 pp 276-286 Available online at: https://noyam.org/journals/ehass/ DOI : https://doi.org/10.38159/ehass.2023438

Promoting the Cyber Wellness of Internet Users in Papua New Guinea



Olugbenga Adedayo Ige¹

¹ Papua New Guinea National Research Institute [PNGNRI], Port Moresby, Papua New Guinea.

ABSTRACT

In Papua New Guinea, there are concerns that the increase in internet accessibility has led to a rise in criminal activities in cyberspace. This paper identifies activities that constitute crimes in the cyberspace of Papua New Guinea. The main prongs of facilitating cyber wellness of Internet users are discussed to inform policy-making in Papua New Guinea. This paper provides guidance to policymakers, public health specialists, education and counselling psychologists, school teachers, educational researchers, and non-governmental organisations on cosmopolitan strategies for promoting cyber wellness in Papua New Guinea and the Pacific Islands in general.

Keywords: Cyber wellness, Cyber health, Mental health, Papua New Guinea, Cybersecurity, Cybercrimes, Cyberspace.

Correspondence Olugbenga Adedayo Ige Email: Olugbenga.Ige@pngnri.org

Publication History Received 24th November, 2022 Accepted 27th February, 2023 Published online 17th March, 2023

INTRODUCTION

Crimes in different nations of the world were occurring in the physical spaces during the analog era. These occurrences were subjected to the criminal codes that were promulgated in that era. The advancement of ICT and other related communication capabilities, most especially the Internet that powered the third industrial revolution, created a space that permits or empowers individuals to import their non-conforming behaviours in the physical space to this space. The evolution of cyberspace created new loci of criminal activities that have confounded the law enforcement apparatuses of developed and developing nations of the world. The inability of law enforcement agents to unravel crimes committed on the Internet has portrayed them in a negative light to a cross-section of the citizenry in all these nations of the world.

Unfortunately, most members of the public in developing nations have failed to realise that the technical nature of cybercrimes makes them transnational crimes that cannot be resolved with an e-intelligence gathering that could span months.¹ These are unlike conventional crimes committed in the physical space that could potentially be unravelled by crime detectors in a short period of time. The technicalities inherent in crimes committed in cyberspace and the ubiquity of information and public security led the Papua New Guinea (PNG) Government to promulgate the Cybercrime Act that was drafted in 2011, launched in October 2015, passed by the PNG Parliament in September 2016, and adopted on 13 December 2016. It is affirmed that the promulgated cybercrime law constitutes major ramifications for the functions of the Internet in the Papua New Guinean society.² This research

¹ United Nations Office on Drugs and Crimes, "Obstacles to Cybercrime Investigations: Cybercrime Module 5 Key Issues," March 2019, https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.

² Kasek Galgal, "Developing PNG's Cybercrime Policy: Local Contexts, Global Best Practice," March 16, 2017, https://www.lowyinstitute.org/the-interpreter/developing-png-s-cybercrime-policy-local-contexts-global-best-practice.

analyses The Federal Bureau of Investigation 2021's Internet crime report and policy documents on cybercrimes in Papua New to *unpack behaviours that constitute cybercrimes in Papua New Guinea, and suggest cosmopolitan approaches that Papua New Guinea can adopt to ensure the cyber wellbeing of its citizenry in the cyberspace.* The study unpacks acts that constitute crimes that impact cyber wellness in Papua New Guinea. It also draws Inferences from international crime reports and relevant policy documents on global approaches that Papua New Guinea can adopt to combat cybercrimes. In light of the foregoing, this review answers these research questions:

Research Question 1: What Constitutes Crimes in the Cyberspace in Papua New Guinea?

Research Question Two: What are the cosmopolitan approaches that Papua New Guinea can adopt to ensure the cyber wellbeing of Papua New Guineans in cyberspace?

The research adopts a systematic approach to thematically review the 2021 IC3 report and the Papua New Guinean cybercrime code act 2016 to answer the two research questions answered in this study.

LITERATURE REVIEW

Cyber Wellness

Before the emergence of the Internet, the concept 'of wellness' was a popular term in the physical space that describes activities related to holistic health or the general well-being of human beings at different geographical locales. The advent of the Internet led to the use of terms such as cybersecurity (cyber + security), cyberhealth (cyber + health), cyberspace (cyber + space), and cyber victimization (cyber + victimization). All these words or concepts that were popularised in the analog era became fused with the concept 'cyber' to provide more information on the virtual nature of traditional concepts such as 'security', 'health', 'space', and a host of other popular terms such as cyber wargaming, and cyber conflicts reported by Colbert et al.³

In the analog era, the concept was 'wargaming'. However, the era revolutionised by the Internet created the concept 'cyber wargaming', and 'cyber conflict'. Cyber wargame is a scenario that involves the regular employees of an organisation that plays roles in computer-based (most times human-based) simulation of a cyber attack and responses to it.⁴ On the other hand, cyber conflicts are designed around problems of an adversarial mold/nature that are usually solved by the adoption of game-theoretic models or simulations known as 'wargames' that are not synonymous with those in military practice.

The Council of Europe describes cyber wellness as the positive well-being of Internet users, and the understanding of online behaviours and consciousness of the channels of protection available to a user in cyberspace.⁵ In Singapore, the concept of cyber wellness has gained momentum as the Ministry of Education has designed the cyber wellness framework to guide schools in planning their cyber wellness programme.⁶ The Singaporean Ministry of Education affirms that cyber wellness is the positive well-being of Internet users, and it entails an understanding of risks inherent in harmful online behaviours, and the personalised techniques of protecting oneself and other users of the Internet from such online behaviours.⁷

³ Edward J.M. Colbert, Alexander Kott, and Lawrence P Knachel, "The Game-Theoretic Model and Experimental Investigation of Cyber Wargaming," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 17, no. 1 (January 31, 2020): 21–38, https://doi.org/10.1177/1548512918795061.

⁴ Colbert, Kott, and Knachel, "The Game-Theoretic Model and Experimental Investigation of Cyber Wargaming."

⁵ The Council of Europe, "Initiatives, Policies, Strategies - Cyberviolence," 2022, accessed November 5, 2022. https://www.coe.int/en/web/cyberviolence/initiatives-policies-strategies.

⁶ Singapore The Ministry of Education, "MOE Cyber Wellness Framework - Cyber Wellness in BV," 2010, accessed 5 November 2022. https://sites.google.com/a/bedokviewsec.edu.sg/cyber-wellness-in-bv/moe-cyber-wellness-framework.
⁷ The Ministry of Education, "MOE Cyber Wellness Framework - Cyber Wellness in BV."



Sense – Think – Act Process

Sense: Identify the possible risks of harmful behaviours online and learn how to protect oneself

Think: Analyse, evaluate and reflect on the online situation based on the three CW principles

Act: Translate understanding into actions so as to be safe and have a positive presence online

Figure 1 presents the Singaporean model and explanations of what constitutes cyber wellness. Source: <u>Cyber Wellness (moe.edu.sg)</u>

In this study, the author defines cyber wellness as the psychological and social well-being of users in cyberspace.

METHODOLOGY

Data Extraction

The data and information presented in this study were taken from the 2021 Internet crime report and the policy document relating to cybercrime in Papua New Guinea. These documents were qualitatively analysed to answer the research questions raised for the study.

Data Analysis

The data reported in the 2021 IC3 report and the Papua New Guinean cybercrime code act 2016 were thematically analysed to answer the two research questions in this study. Thematic analysis was appropriate for the study because the data analysed to answer the research questions emanate from the text. The thematic analysis method is a veritable method to analyse studies that the data are embedded in written texts and spoken words.⁸

In analysing the information and data presented in the 2021 Internet crime report and the cybercrime code act 2016, the researcher:

- Critically read the international report compiled by the Federal Bureau of Investigation on acts that were inimical to the well-being of Internet users and noted the trends inherent in the data presented.
- The relevant themes and information that answer the research questions were critically identified.
- The researcher made sense of the relevant themes and data presented in the report and policy documents to infer and project the global best approach to combat cybercrimes and enhance the well-being of Internet users in cyberspace.

⁸ Bunmi Isaiah Omodan and Olugbenga A. Ige, "University Students' Perceptions of Curriculum Content Delivery During COVID-19 New Normal in South Africa," *Qualitative Research in Education* 10, no. 2 (June 28, 2021): 204, https://doi.org/10.17583/qre.2021.7446.

Ethical Considerations

• This study did not collect data from human participants. The data reported in the 2021 Internet crime report and the Papua New Guinean cybercrime code act 2016 are documents that were analysed in this study.⁹

FINDINGS AND DISCUSSION

Research Question 1: What Constitutes Crimes in the Cyberspace in Papua New Guinea? What Constitutes Crimes in the Cyberspace?

Crimes committed in cyberspace are generally known as 'cybercrimes'. Phillips et al. state that the synonymous terminologies for cybercrimes are: cyberspace crime, computer crime, computer-related crime, electronic crime, e-crime, technology-enabled crime, and high-tech crime. ¹⁰ Other terminologies that have evolved in the developing nations in Africa on cybercrime are 'Yahoo Yahoo' and 'Yahoo Plus' (i.e., Scammers using voodoo or customary charms and incantations to support or facilitate criminal activities in cyberspace). ¹¹

Another relevant definition to this discourse that would educate the members of the public that have inadequate knowledge of the intricacies of cybercrimes in Papua New Guinea was provided by Maras.¹² Maras states that cybercrime is different from traditional crime because it exceeds physical or geographical boundaries and is carried out with less effort, greater ease and at much greater speed than traditional crimes. This definition by Maras alludes to the frustration experienced by citizens that were scammed and police investigators on incidences of crimes in many nations of the world.

What Constitutes Crimes in the Cyberspace in Papua New Guinea?

Payne asserts that there is no universally acceptable definition of cybercrime at the moment. This notwithstanding there are generally accepted definitions of cybercrime due to transnational criminal code variations.¹³ Phillips et al. asserts that criminal behaviours in cyberspace comprise a diverse set of offences and harmful behaviours, while EUROPOL classified cybercrimes into two basic strands namely: cyber-dependent and cyber-enabled crimes.¹⁴ EUROPOL defines cyber-dependent crime as "basically any crime that is committed using computers, computer networks or other related Information and Communication Technologies (ICTs)."¹⁵

The Internet is the primary channel for committing and spreading malware, hacking to steal sensitive personal or industry data, and denial of service attacks to facilitate reputation, and financial-related damages.¹⁶ On the other hand, cyber-enabled crimes refer to traditionally-occurring crimes

⁹ The Papua New Guinea Government, "Cybercrime Code Act 2016," 2016,

https://www.nicta.gov.pg/regulatory/internet/cybercrime-cybersecurity/.

¹⁰ Kirsty Phillips et al., "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," *Forensic Sciences* 2, no. 2 (April 16, 2022): 379–98, https://doi.org/10.3390/forensicsci2020028.

¹¹ Peter Adewale Amosun, Olugbenga Adedayo Ige, and Kim-Kwang Raymond Choo, "Impact of a Participatory Cyber Crime Prevention Programme on Secondary School Students' Attainment in Crime Prevention Concepts in Civic Education and Social Studies," *Education and Information Technologies* 20, no. 3 (September 10, 2015): 505–18, https://doi.org/10.1007/s10639-013-9298-0.

¹² Marie-Helen Maras, *Computer Forensics: Cybercriminals, Laws and Evidence*, Second edition. (Jones and Bartlett Publishing, 2014).

¹³ Brian K. Payne, "Defining Cybercrime," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Cham: Springer International Publishing, 2020), 3–25, https://doi.org/10.1007/978-3-319-78440-3_1.

¹⁴ Phillips et al., "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies."

¹⁵ European Cybercrime Centre [EC3] EUROPOL, "Internet Organized Crime Threat Assessment [IOCTA]," 2018, https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.

¹⁶ United Nations Office on Drugs and Crimes, "University Module Series: Cybercrime Teaching Guide.," 2019, https://www.unodc.org/e4j/en/cybercrime/teaching-guide/index.html.

facilitated by the Internet and digital technologies.¹⁷ From the provisions of the Cybercrime Code Act 2016, there are four divisions of activities that constitute cybercrimes in Papua New Guinea:¹⁸

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

Research Question Two: What are the cosmopolitan approaches that Papua New Guinea can adopt to ensure the cyber wellbeing of Papua New Guineans in cyberspace?

Cosmopolitan Approaches to Cybercrime Prevention in Papua New Guinea

• Building the Capacity of the Royal PNG Constabulary Cybercrime Unit

In Papua New Guinea, law enforcement services are provided to the citizenry by RPNGC i.e. a part of the PNG Government's law and justice sector.¹⁹ The RPNGC has a functional but young cybercrime unit (including Airport Police Unit) saddled with the responsibility of investigating and enforcing

¹⁷ The Papua New Guinea Government, "Cybercrime Code Act 2016."

¹⁸ The Federal Bureau of Investigation, "Internet Crime Report," 2021,

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

¹⁹ Interpol, "How INTERPOL Supports Papua New Guinea to Tackle International Crime," accessed March 7, 2023, https://www.interpol.int/en/Who-we-are/Member-countries/Asia-South-Pacific/PAPUA-NEW-GUINEA.

cybercrime-related laws and regulations in Papua New Guinea.²⁰ The capacity of the policemen in the cybercrime unit needs to be built to understand the cosmopolitan challenges of curbing the menace of cybercrimes from the spate of current cybercriminal activities reported in Australia. The Federal Bureau of Investigation reported that Australia has about 2,204 victims of cybercrimes.²¹ The data released by the Federal Bureau of Investigation makes Australia the third among countries whose citizens are most vulnerable to cyber scammers after the United States, Canada, and India. The security dogwatch such as Interpol opines that Papua New Guinea is situated on maritime and air crossroads between Asia and the South Pacific. Interpol reasoned that the geographic location of Papua New Guinea to Australia makes her attractive to transnational organized crime gangsters.²² 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).

• Cyber Police Portal Papua New Guinea

These countries have specialised agencies that attend to incidences of cybercrime besides the National Police: United States, United Kingdom, Canada, India, Australia, and France. 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 her 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, it is advised that the Papua New Guinean government should not wait for incidences of cybercrimes to escalate before establishing a specialised or independent agency to enforce cybercrimes laws in Papua New Guinea. 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.²³

²⁰ The National, "Cybercrime Unit Set up at Airport Police Station," August 21, 2019, https://www.thenational.com.pg/cybercrime-unit-set-up-at-airport-police-station/.

²¹ The Federal Bureau of Investigation, "Internet Crime Report."

²² Interpol, "How INTERPOL Supports Papua New Guinea to Tackle International Crime."

²³ The National, "Cybercrime Unit Set up at Airport Police Station."





• Constitute The Papua New Guinean Recovery Asset Team

This concept is adapted from the United States Internet Crime Complaint Center [IC³].²⁵ This approach would enable the Papua New Guinean Cyber Crime Unit to equipoise communication with the financial institutions in Papua New Guinea and assist Royal Papua New Guinea Constabulary (RPNGC) to freeze funds for Papua New Guineans who make transfers to local accounts or accounts domiciled in the nations located in Pacific Islands under fraudulent premises. The model is presented in Figure 3:

²⁴ Figure 2 list the top 20 countries by the number of total victims as compared to the United States. The specific number of victims for each country is listed in ascending order to the right of the graph.

²⁵ Federal Bureau of Investigation, "Internet Crime Complaint Center (IC3)," accessed November 5, 2022, https://www.ic3.gov/.



Figure 3: The Adapted Recovery Asset Model Team RAT Model²⁶ Source: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

To adapt the Recovery Asset Model developed by the National White Collar Crime Center in Papua New Guinea. The PNG Government will establish the Papua New Guinea Cyber Crime Complaint Center (PNGCCC) that will receive the complaints of victims of cyber crimes in Papua New Guinea and other countries in the Pacific Islands. The International Computer and Information Scientists will be consulted to develop the "Automated triage through the RPNGC Database", and saddle "PNGCCC Analysts" to assign the complaints received to PNGCCC field officers and field offices for action. The "PNGCCC Analysts" are given higher level security clearance to notify the financial institutions to block funds or repatriate the proceeds of cyber and Internet crimes after scrutinizing the complaint. The Royal Papua New Guinea Recovery Asset (PNGRAT) model will act as an electronic liaison between RPNGC and financial institutions supporting statistical and investigative analyses.

School-Community Based Educational Interventions

In most nations of the world especially in the Pacific Islands, researchers have overlooked 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. To educate school children and the community populace in Papua New Guinea, the cybercrime related themes and means of the crimes should be infused into school curricula for Social Science and Information and Communication Technology.

²⁶ 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).



*Figure 4. Community Action Model Source: Susana H. Lavery, et.al.*²⁷

Another veritable approach is to build the capacity of the teeming school children and the local communities in Papua New Guinea using the Community Action Model (CAM).²⁸

To operate the educational intervention with the Community Action Model (CAM), researchers or facilitators may 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 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.

²⁷ Susana Hennessey Lavery et al., "The Community Action Model: A Community-Driven Model Designed to Address Disparities in Health," *American Journal of Public Health* 95, no. 4 (2005): 611–16.

²⁸ Olugbenga Adedayo Ige, "School-Based Cybersecurity Education Programme for Schoolchildren in South Africa! A Timely Call from Bloemfontein," *Universal Journal of Educational Research* 8, no. 6 (June 2020): 2710–16, https://doi.org/10.13189/ujer.2020.080656.

School-Community Counselling Centres

The government should institutionalise the rehabilitation of victims of cybercrimes. One of the primary difficulties in rehabilitating victims of cybercrimes is the unavailability of sufficiently trained educational psychologists to address the psychologically related problems associated with this new locus of criminal activity effectively. Another dimension to cyber wellness is that it is inclusive of sexuality and sexual health.²⁹

The RPNGC should refer anyone that has reported to the cybercrime unit of loss of valuables in the cyberspace for counselling to enable overcome psychological trauma associated with these unsavoury cyber occurrences.

CONCLUSION

This article provides important insights into cosmopolitan strategies for preventing cybercrimes in Papua New Guinea. The country has done well by promulgating laws to tackle incidences of cybercrimes to enable the PNG government to guarantee the cyber wellness of its citizenry. However, the RPNGC must realise that the current law enforcement structure, though good cannot tackle 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 her staff, creating modern information and intelligence collection electronic platforms to tackle the menace of cybercrimes efficiently and sustainably in Papua New Guinea. The RPNGC should consider using educational strategies or approaches to orientate the PNG citizenry on the ills of cybercrimes, and the channels of protection available to Papua New Guineans venturing into cyberspace in any country of the world. The philosophical ideas presented in this paper would assist the RPNGC, policymakers, and educational researchers to improve on the current structure of enforcing cybersecurity laws in Papua New Guinea. This paper also has the potential to guide the Papua New Guinea government in amending laws on cybercrimes and creating cosmopolitan cyber police that could become a model to other nations in the Pacific Islands.

BIBLIOGRAPHY

- Adedayo Ige, Olugbenga. "School-Based Cybersecurity Education Programme for Schoolchildren in South Africa! A Timely Call from Bloemfontein." *Universal Journal of Educational Research* 8, no. 6 (June 2020): 2710–16. https://doi.org/10.13189/ujer.2020.080656.
- Amosun, Peter Adewale, Olugbenga Adedayo Ige, and Kim-Kwang Raymond Choo. "Impact of a Participatory Cyber Crime Prevention Programme on Secondary School Students' Attainment in Crime Prevention Concepts in Civic Education and Social Studies." *Education and Information Technologies* 20, no. 3 (September 10, 2015): 505–18. https://doi.org/10.1007/s10639-013-9298-0.
- Colbert, Edward JM, Alexander Kott, and Lawrence P Knachel. "The Game-Theoretic Model and Experimental Investigation of Cyber Wargaming." *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 17, no. 1 (January 31, 2020): 21–38. https://doi.org/10.1177/1548512918795061.
- Emelianchik-Key, Kelly, Adriana Labarta, and Taylor Irvine. "Understanding Education in Sexuality Counseling from the Lens of Trainees: A Critical Examination and Call for Increased Attention and Training." *Journal of Counseling Sexology & Sexual Wellness: Research, Practice, and Education*, January 9, 2022, 70–81. https://doi.org/10.34296/03021057.
- European Cybercrime Centre [EC3] EUROPOL. "Internet Organized Crime Threat Assessment [IOCTA]," 2018. https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.

²⁹ Kelly Emelianchik-Key, Adriana Labarta and Taylor Irvine, "Understanding Education in Sexuality Counseling from the Lens of Trainees: A Critical Examination and Call for Increased Attention and Training," *Journal of Counseling Sexology & Sexual Wellness: Research, Practice, and Education*, January 9, 2022, 70–81, https://doi.org/10.34296/03021057.

- Federal Bureau of Investigation. "Internet Crime Complaint Center (IC3)." Accessed November 5, 2022. https://www.ic3.gov/.
- Galgal, Kasek. "Developing PNG's Cybercrime Policy: Local Contexts, Global Best Practice," March 16, 2017. https://www.lowyinstitute.org/the-interpreter/developing-png-s-cybercrimepolicy-local-contexts-global-best-practice.
- Hennessey Lavery, Susana, Mele Lau Smith, Alma Avila Esparza, Alyonik Hrushow, Melinda Moore, and Diane F Reed. "The Community Action Model: A Community-Driven Model Designed to Address Disparities in Health." *American Journal of Public Health* 95, no. 4 (2005): 611–16.
- Interpol. "How INTERPOL Supports Papua New Guinea to Tackle International Crime." Accessed November 5, 2022. https://www.interpol.int/en/Who-we-are/Member-countries/Asia-South-Pacific/PAPUA-NEW-GUINEA.

Maras, Marie-Helen. Computer Forensics: Cybercriminals, Laws and Evidence, 2014.

- Omodan, Bunmi Isaiah, and Olugbenga A Ige. "University Students' Perceptions of Curriculum Content Delivery During COVID-19 New Normal in South Africa." *Qualitative Research in Education* 10, no. 2 (June 28, 2021): 204. https://doi.org/10.17583/qre.2021.7446.
- Payne, Brian K. "Defining Cybercrime." In *The Palgrave Handbook of International Cybercrime* and Cyberdeviance, 3–25. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-319-78440-3_1.
- Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic Sciences* 2, no. 2 (April 16, 2022): 379–98. https://doi.org/10.3390/forensicsci2020028.
- The Council of Europe. "Initiatives, Policies, Strategies Cyberviolence," 2022.
- https://www.coe.int/en/web/cyberviolence/initiatives-policies-strategies.
- The Federal Bureau of Investigation. "Internet Crime Report," 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- The Ministry of Education, Singapore. "MOE Cyber Wellness Framework Cyber Wellness in BV," 2010. https://sites.google.com/a/bedokviewsec.edu.sg/cyber-wellness-in-bv/moe-cyber-wellness-framework.
- The National. "Cybercrime Unit Set up at Airport Police Station," August 21, 2019. https://www.thenational.com.pg/cybercrime-unit-set-up-at-airport-police-station/.
- The Papua New Guinea Government. "Cybercrime Code Act 2016," 2016.
- https://www.nicta.gov.pg/regulatory/internet/cybercrime-cybersecurity/.
- United Nations Office on Drugs and Crimes. "Obstacles to Cybercrime Investigations: Cybercrime Module 5 Key Issues," March 2019. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.

—. "University Module Series: Cybercrime Teaching Guide.," 2019.

https://www.unodc.org/e4j/en/cybercrime/teaching-guide/index.html.

ABOUT AUTHOR

Dr. Olugbenga Adedayo Ige is a Senior Research Fellow and Program Leader of National Security and International Relations Research Program [NSIRRP] at the Papua New Guinea National Research Institute [PNGNRI], Port Moresby, Papua New Guinea.