SALUS JOURNAL

Volume 10, Number 2 (2022)
ISSN: 2202-5677

Cybercrime Policing in the Lagos State Command of the Nigeria Police Force

Usman A. Ojedokun and Samson I. Oshilaja

ABSTRACT

The criminality of cybercriminals operating in Nigeria has significantly expanded from the initially dominant cyber fraud to include other categories of cybercrime. Although the Nigerian Government has tried to contain the problem, there is a shortage of scholarly information on the specific role of the Nigeria Police Force in fighting this form of crime. Given this, the central objective of this study was to investigate cybercrime policing in the Lagos State Command of the Nigeria Police Force. It was exploratory and cross-sectional in design. . Data were sourced from 27 purposively selected police personnel using in-depth and key-informant interviews. The results showed that the Lagos State Police Command routinely handled different cases of cybercrime. However, exposure to professional training in cybercrime policing skills was restricted to certain categories of officers. Although different internal and external strategies were being used by the Police Command to combat cybercrime, the overall effectiveness of its personnel was being hampered by multiple operational challenges.

Keywords: *Cybercrime, Cybercriminals, Online Criminality, Policing, Lagos State Police, Command, Nigeria Police Force*

INTRODUCTION

Globally, cybercrime has emerged as one of the dominant crimes confronting many police organisations (Collier et al., 2022; Whelan & Harkin, 2019; Harkin et al., 2018; Wall & Williams, 2013) as criminals are increasingly using the Internet to commit a host of crimes, such as fraud, child pornography, drug trafficking, economic crime, and hate crimes (Cross & Blackshaw, 2015; Awan & Blakemore, 2012). Although the policing profession has always been evolving, the technological advancements witnessed in the past 20 years have accelerated that change and dramatically altered the landscape of crime (Police Executive Research Forum, 2014).

Volume 10, Number 2 (2022)
ISSN: 2202-5677

In Nigeria, the nature, dimension, and magnitude of cybercrime has expanded significantly in the last two decades (Ojedokun & Ilori, 2021; Punch, 2015). The activities of cybercriminals operating in the country have metamorphosed from the initially dominant online fraud to include other categories of cybercrime such as cyber bullying, cyber stalking, distributed denial of service (DDoS) attacks, identity theft, intellectual property theft, hacking, malware distribution, phreaking, revenge pornography, and software piracy (Adebayo & Ojedokun, 2018; Oyenuga, 2014). For instance, the official website of the Independent National Electoral Commission (INEC) was hacked by a group known as the Nigerian Cyber Army, in the build-up to the 2015 general elections (Alade, 2015). Also, a report by Kaspersky Protection Technologies indicates that over 9,000 people in Nigeria suffered malware attacks launched by cybercriminals in 2019 alone (Adepetun, 2020; Umeh, 2020).

The intensity, scope, and multisectoral deleterious impacts of cybercrime make it expedient to understand how the police force as the primary responder to crime events and the principal enforcer of the law in Nigeria is addressing it. Although the Nigerian Government has tried to contain the problem of cybercrime through the 2015 enactment of the Nigerian Cybercrime Act, by establishing the Nigerian Cyber Crime Working Group, and by signing a Memorandum of Understanding with Microsoft Corporation among others, there is a dearth of scholarly information on the specific role of the Nigeria Police Force as a law enforcement agency in fighting this form of crime.

The pervasiveness of different forms of cybercrime is a new addition to the burden of the Nigeria Police Force, an agency whose effectiveness in tackling offline crimes has been consistently rated average (Ojedokun, 2021; Adebayo & Ojo, 2009). Moreover, the high digital divide and skills gap in the use of information and communication technology currently existing among Nigerians may also inhibit the capability of police officials to adequately investigate and prosecute cybercrime cases (Peters & Ojedokun, 2019; Obayelu & Ogunlade, 2006). Furthermore, the fact that some non-financially motivated forms of cybercrime such as revenge pornography, cyber stalking, hate crime, and malware distribution are increasingly becoming pervasive (Adepetun, 2020; Aderinto & Ojedokun, 2017; This Day (2016) clearly indicates that relying solely on the Economic and Financial Crimes Commission (EFCC), a specialised government agency established in 2003, to tackle financial crimes in Nigeria including cybercrime, is inadequate. Therefore, it becomes important to examine the level of preparedness and operational strategies of the Nigeria Police Force in combating cybercrime. Against this background, the central objective of this study was to investigate cybercrime policing in the Lagos State Command of the Nigeria Police Force.

LITERATURE REVIEW

Volume 10, Number 2 (2022)
ISSN: 2202-5677

The growth of cyber technologies has significantly increased the workload of police personnel across the globe (Ndubueze & Igbo, 2014). Wall and Williams (2013) submit that cybercrime has become a part of the national security strategies of many countries, such as the United Kingdom, Australia, the Netherlands, and the United States of America. Harkin et al. (2018) mention that many state police organisations in Australia have responded to the threat of cybercrime by developing specialist units. However, Dupont (2017) claims that despite the increasing recognition of the social and economic costs of cybercrime, it seems evident that the main beneficiaries of the increased public-sector funding to promote cyber security have been security and intelligence agencies rather than local police organisations.

Holt and Bossler (2015) state that cybercrime poses unique challenges to domestic and international law enforcement agencies because cybercriminals have the technical capacities to transcend spatial and temporal boundaries while also widening their victim pool to include all individuals with access to the Internet. Equally, Harkin et al. (2018) posit that the pervasiveness of cyber-enabled or cyber-facilitated crimes means that police officers must be ready to confront its growing relevance and the increasing public demands to respond to cyber offending. Furthermore, they argue that cybercrime will inevitably become an element of all policing as cyber is now crucial to the facilitation of different forms of crimes.

Whelan and Harkin (2019) say that the extent to which police organisations have adequately understood and prioritised cybercrimes and their level of expertise in dealing with cyber offences have always generated serious debates. The Police Executive Research Forum (2014) submits that local police agencies have not had adequate time to be fully prepared to identify their role in preventing and investigating cybercrime because it developed very quickly. Koziarski and Lee (2020) assert that adequate cybercrime training is paramount in ensuring that any police-led approach to cybercrime is properly executed. However, Holt and Lee (2019) and Bossler and Holt (2012) have separately linked police agencies' ineffectiveness at fighting cybercrime to factors such as their inability to acquire the necessary technological equipment essential for conducting adequate investigations, insufficient training, and difficulty in retaining officers who possess appropriate skills to combat cybercrime. Willits and Nowacki (2016) state that the institutional legitimacy of the police as an effective first responder will be negatively affected if law enforcement responses to cybercrime do not improve.

METHODOLOGY

This research was exploratory and cross-sectional in design. It was cross-sectional in the sense that data were collected from different individuals at a single point in time. The Lagos State Police Command was the main focus – it is among the 36 State Police Commands of the Nigeria Police Force. The command headquarters

Volume 10, Number 2 (2022)
ISSN: 2202-5677

is located at Ikeja in the Lagos metropolis. This Police Command is primarily responsible for law enforcement and crime prevention in Lagos State. It is administered by a Commissioner of Police supported by Deputy Commissioners of Police and Assistant Commissioners. Although this Police Command did not have a special anti-cybercrime unit when this study was conducted, its selection was deemed appropriate because Lagos State is among the widely recognised major hubs of cybercrime in Nigeria (Ndubueze & Igbo, 2014). Therefore, the opinions of police personnel of the command on policing cybercrime were considered apt and important for a study of this nature. Both female and male police officials serving at the Lagos State Police Command of the Nigeria Police Force constituted the study population. The researchers had no prior personal relationship with the police officers who were involved in this study. Rather, access to respondents was made possible because the official request to conduct the research in the Police Command was granted by the Lagos State Commissioner of Police.

Data were principally elicited through the combination of two qualitative methods – in-depth and key-informant interviews. Regarding the procedure used for data collection, written permission was first sought from the office of the Commissioner of Police of Lagos State. After the request was granted, the researchers were directed to the Area 'M' Police Command and the State Criminal Investigation and Intelligence Department because of its strategic importance in cybercrime policing in Lagos State, Nigeria. However, due to many bureaucratic bottlenecks and difficulties in gaining access to potential respondents at Area 'M', data were exclusively sourced from police officials serving at the State Intelligence Bureau, the Administrative Unit and the General Duty Section of the State Criminal Investigation and Intelligence Department. At this location, different interview sessions were held with police officials belonging to the cadres of Assistant Inspector, Assistant Superintendent, Inspector, Sergeant, and Superintendent. Specifically, key informant interviews were conducted with two Assistant Superintendents of Police because of their seniority and years of professional experience, while 25 in-depth interviews were held with police officials belonging to other ranks. The purposive sampling technique was used to select respondents as they were chosen based on their knowledge and work-related experience on cybercrime policing. Some of the questions that respondents were asked during the interviews were: What can you say about the pervasiveness of cybercrime in Lagos State? What are the procedures being employed in policing cybercrime in Lagos State? How is the Lagos State Police Command responding to reported cases of cybercrime? How are the reported cases of cybercrime handled by the Police Command? What are the specialised training programs that are available to police officers in the Lagos State Police Command with regard to cybercrime policing? What are the challenges associated with cybercrime policing in Lagos State? What do you think can be done to enhance cybercrime policing in Lagos State? All interviews were conducted with the aid of a voice recorder and field notes.

Volume 10, Number 2 (2022)
ISSN: 2202-5677

At the analysis stage, the elicited data were subjected to manual content analysis. The procedure essentially involved a painstaking transcription, detailed description, and careful interpretation of the generated data using the deductive approach. More specifically, data were thematically analysed, explored, and interpreted in line with the aforementioned study objective to tease out the emerging patterns. In addition, the verbatim quotations of some of the important responses given by the respondents during the interviews were done to further ensure the lucidity of discourse.

ETHICAL CONSIDERATIONS

International research ethics standards were carefully adhered to throughout this study. Ethical approval was granted by the Department of Sociology, University of Ibadan, Nigeria before the study was carried out. Also, the permission of the Lagos State Commissioner of Police was sought and obtained before the start of fieldwork. Also, the consent of each respondent was sought and obtained before theyy participated in the study. The objective of the research was carefully explained to participants and they were also informed of their right to voluntary participation and to withdraw from the study at any time they deemed necessary.

RESULTS AND DISCUSSION

In this section, the major results from the study are presented and discussed along these themes: the types of cybercrime commonly reported to the Lagos State Police Command, the response of the Lagos State Police Command to cybercrime cases, training of police personnel on cybercrime policing in Lagos State Police Command, strategies being used by the Lagos State Police Command to address cybercrime, and challenges confronting the Lagos State Police Command in cybercrime policing.

Types of Cybercrime Commonly Reported to the Lagos State Police Command

Information was sought on the types of cybercrime commonly reported to the Lagos State Police Command to gauge the involvement of police officials in the investigation and handling of such crimes. The outcome of the interviews revealed that personnel of the Command routinely received complaints from victims of different forms of cybercrime. In one of the in-depth interview sessions conducted, a respondent said:

> ATM/debit card and online money transfer fraud involving the use of clone and dummy cards to extort money from victims' bank accounts are the forms of cybercrime commonly reported to us. There was a case I handled which was reported at my Command in which a call was put through to the victim that her ATM card had expired and that she should

Volume 10, Number 2 (2022)
ISSN: 2202-5677

> forward an SMS containing her bank details to a particular number that was sent to her. In less than ten minutes, her bank account was emptied by cybercriminals. (IDI/male/40 years/Yoruba)

A respondent also explained:

> I think hacking, online harassment, online banking fraud and identity theft are the most reported cases of cybercrime in Lagos State. We have had a case of a criminal hacking into a victim's phone to extract the victim's bank details which was later used for stealing money from his bank account. We later apprehended the offender by tracking his phone number and by also arresting a soft target (who was a person closely related to the suspect) who led us directly to him. That was how we succeeded on that particular case. (IDI/male/28 years/Yoruba)

Another key-informant described the situation this way:

> Cases of cybercrime that are commonly reported to us are basically ATM scam and identity theft/impersonation. These online bandits sometimes do extract or copy people's information including pictures, and then create a social media account or sometimes even hack into their victim's social media account. They will then begin sending incriminating messages contrary to the intent of the original owner of such an account. Sometimes they can ask the victim's online contacts to send some money to them because they are in an emergency situation or in desperate need of money. There was a particular case where a fraudster used the picture of a popular pastor to open a Facebook account and ventured into defrauding people both locally and internationally. After series of investigation and tracking, the suspect agreed to come forward after one of our men pretended to be a follower who needed special prayers. When he arrived, he was arrested and later prosecuted. (KII/male/55 years/Edo)

The submissions of these respondents indicate that different cases of financially-motivated and non-financially motivated cybercrimes including those bordering on ATM/debit card fraud, cyber bullying, cyber harassment, hacking, identity theft, online impersonation, and online money transfer fraud were the ones commonly reported to and handled by police officials at the Lagos State Police Command.

Response of the Lagos State Police Command to Cybercrime Cases

The intensity and scope of cybercrime are increasingly compelling law enforcement agencies in different parts of the world to innovate different institutional frameworks to tackle it (Whelan & Harkin, 2019; Wall & Williams, 2013). Therefore, it was

Volume 10, Number 2 (2022)
ISSN: 2202-5677

considered important to investigate the response of the Lagos State Police Command to cybercrime cases. The respondents gave different opinions. One of the key-informants interviewed stated:

> Yes, there are different units that handle cybercrime in the Lagos State Police Command such as the Special Anti-Robbery Squad, Special Task Force and the Special Fraud Unit. However, I believe the Anti-Robbery Squad handles most of the cases from the point of receiving such reports to investigating, arresting and prosecuting of suspects. (KII/male/55 years/Edo)

Another key-informant responded to the question this way:

> Yes, there are some of police units that are arresting and prosecuting suspects of cybercrime. They are also recovering stolen belongings where possible. Sometimes, they are responsible for tracking and intercepting cybercriminals from carrying out further attacks or damages. (KII/female/30 years/Yoruba)

One of the interviewees said:

> There is no dedicated unit to cybercrime in the Lagos State Police Command. However, the investigation unit of the Police Command and the Divisional Command handle reported cybercrime cases and investigations. (IDI/male/Inspector/45 years/Igbo)

A respondent also mentioned:

> Well, I will not say that there is a specialised unit that is solely dedicated to cybercrime. However, there are different means that are being adopted to monitor and handle cybercrime. When investigating a cybercrime case, the Nigeria Police do make use of some agents in the community to gather information and monitor the activities of suspects. These agents could be civilians or sometimes undercover police officers. This assignment could be handled by the Investigation Department or sometimes by the Special Anti-Robbery Squad (SARS). (KII/male/55 years/Edo)

It is clear from the submissions of the key-informants and the interviewees that cybercrime and cybercriminal cases were mainly being investigated and handled in the Lagos State Police Command by some special police detachments such as the Special Anti-Robbery Squad, the Special Task Force Unit, and the Special Fraud Unit.

Volume 10, Number 2 (2022)
ISSN: 2202-5677

Training of Police Personnel in the Lagos State Police Command on Cybercrime Policing

Training is among the major factors contributing to the effectiveness and service delivery capacity of police agencies and personnel. Thus, respondents were probed on professional training available to police personnel in the Lagos State Police Command on cybercrime policing. All the respondents interviewed confirmed that training on cybercrime policing was occasionally organised by their Command for police officials. One of the key-informants interviewed said:

> Yes, training on cybercrime policing is only available for officers in the special squad unit. There are some courses that they undergo to educate them on the current trends in cybercrime. It does not usually include every section because of lack of fund. Except one wants to sponsor oneself. The Nigeria Police does not sponsor officers for further education. Sometimes, we do hold preliminary lectures at the Area Command, but these are not enough. We were manually taught on ways of interrogating cybercriminals in Lagos. For instance, if a suspect is being intercepted and police officers check his or her phone. We were trained to check their phone contact to see if they have lot of foreign contacts. In a case where there are many foreign numbers in a suspect's phone, he or she would be asked to establish a genuine relationship with such contacts and the failure to do so would lead to his/her arrest. This is what most police squads use nowadays. (KII/male/55 years/Edo)

A respondent also mentioned:

> Yes, there are some specialised training programs that are available to police officers on cybercrime. We have the anti-fraud training course and we also received training on the modus operandi of cybercriminals. (IDI/female/33 years/Yoruba)

However, a respondent asserted:

> No, I have not attended any training on cybercrime and the reason is because I have not been enlisted to participate due to my educational qualification. (IDI/female/30 years/Igbo)

Another participant gave a similar response:

> No, I have never been part of any training because it is only senior ranking officers that are usually considered first because one's level of education is an important criterion in the selection for participation in such trainings. (IDI/male/28 years/Yoruba)

Volume 10, Number 2 (2022)
ISSN: 2202-5677

An officer who had participated in one of the organised training programs said:

> Yes, I have attended trainings on cybercrime policing. It was a conference which enabled officers build their investigative skills on crime generally, which also includes cybercrime. The training was conducted in Abuja. (IDI/female/35 years/Yoruba)

The above narratives point to the fact that the Lagos State Police Command is exposing certain categories of its personnel to some professional training programs on cybercrime policing by educating and equipping them regarding current trends in cybercrime, the modes of operation of cybercriminals, and the professional skills essential for interrogating cybercriminals. However, this professional training was restricted to senior police officers and personnel with higher educational qualifications.

Strategies Used by the Lagos State Police Command to Address Cybercrime

Operational strategy is among the major determinants of the success of any law enforcement agency. Therefore, it was deemed necessary to investigate the strategies used by police officials of the Lagos State Police Command to tackle cybercrime. The findings revealed that different strategies were being used by the Command to address cybercrime. In one of the interviews, a respondent stated:

> The Lagos State Government and the Police are doing their best to fight cybercrime by introducing different measures, some of which include organising public enlightenment and education for the purpose of detailing the antics of fraudsters and maintaining a stringent stance by ensuring that those arrested are prosecuted to serve as deterrent to others. (IDI/male/35 years/Yoruba)

In the words of another respondent:

> The State Command is employing the use of technologies that could be deployed to tackle cybercrime, such as tracking and intercepting devices. These are the ways through which police officials are monitoring and tracking down locations of cybercriminals. (IDI/female/30 years/Igbo)

A key-informant also mentioned this:

> Cybercrime is an international crime that cuts across borders. Therefore, the Nigeria Police Force is partnering with some international organisations like the CIA, FBI and the Metropolitan Police in tracking and arresting cybercriminals. (KII/male/55 years/Edo)

Volume 10, Number 2 (2022)
ISSN: 2202-5677

Another participant asserted:

> The Nigerian Police Force usually exchanges confidential details and information regarding cybercrime with relevant international agencies such as FBI and INTERPOL. (IDI/male/40 years/Yoruba)

It can be gleaned from the submissions of the respondents that the Lagos State Police Command is adopting different strategies to tackle cybercrime. Specifically, the strategies being used by the Command included conducting public enlightenment about the antics of cyberfraudsters, prosecuting cybercrime suspects, conducting surveillance in parts of Lagos State that are notorious for the activities of cybercriminals, using tracking and intercepting devices, and collaborating with relevant international law enforcement agencies such as the FBI, CIA, INTERPOL, and Metropolitan Police.

Challenges Confronting the Lagos State Police Command in Cybercrime Policing

The online environment where cybercriminals operate and their mode of operations are strikingly different from those of criminals perpetrating offline crimes. Therefore, information was gathered on the major challenges confronting the officials of the Lagos State Police Command in investigating cybercrime. All the respondents interviewed agreed they were confronted by different challenges while investigating cybercrime cases. A typical response that was given by nearly all participants was captured this way:

> A major challenge facing us as regards cybercrime policing is lack of equipment. Specifically, the technologies we have are obsolete and cannot be employed for efficient investigation. Another challenge is that social media platforms are also providing opportunities for cybercriminals to facilitate cybercrime. (IDI/male/45 years/Yoruba)

A respondent also described the situation this way:

> A problem that I discovered is the lack of database on people, culprits and cybercrimes. It is so hard to investigate this form of crime efficiently without proper digitisation. There are also financial issues when it comes to training of people and the acquisition of equipment and devices necessary for surveillance and investigation. (IDI/male/28 years/Yoruba)

In the opinion of another interviewee:

> I believe one of the unrated challenges is our bad judicial system that usually frees these culprits when political figures interfere in a case.

Volume 10, Number 2 (2022)
ISSN: 2202-5677

> Another one is the inadequate devices and equipment that can be used to carry out serious and effective investigation. (IDI/male/31 years/Edo)

A respondent also claimed:

> Most times, there is this uncooperative attitude of some of our financial houses (inadequate synergy with financial institutions). Also, funds are not available to support and/or train police officers. Investigation process equally requires the use of certain equipment and these are not usually readily available. (IDI/male/45 years/ Hausa)

Another insight was given by one of the key-informants:

> Another challenge is that at times when officers conducted their investigations and get fruitful result, some superior authorities and political figures do get involved and interrupt the process of charging suspect(s) to court. Thereby, rendering the whole investigation and interrogation ineffective. The Lagos Police Command is doing it best despite the lack of essential machineries and equipment. I am proud to say police officers are using their brains and intellect to detect crime and make arrest. When police officers do their best on cases and then such cases are being cancelled because of the network of culprits to some highly influential people in society or even in the police, this act drains our motivation to combat crime generally. (KII/male/55 years/Edo)

The above assertions of the respondents show the cybercrime policing efforts of the Lagos State Police Command are being hampered by multiple institutional and non-institutional challenges such as the lack of relevant equipment for effective crime investigation, the lack of a database of cybercriminals, an inefficient judicial system, political interference in police investigations, the uncooperative attitude of some financial houses, and the low reportage of cybercrime incidents by victims.

DISCUSSION OF FINDINGS

Regarding the types of cybercrime that are commonly reported to the Lagos State Police Command, the study established that ATM/debit card fraud, cyber bullying, cyber harassment, hacking, identity theft, online impersonation, and online money transfer fraud were the types of cybercrime that were commonly handled by the Police Command. A major deduction that can be made from this finding is that there is a high demand and expectations on police officers in Lagos regarding cybercrime as both financially and non-financially motivated cases of cybercrime are increasingly being brought to their attention by victims. This finding is supported by

Volume 10, Number 2 (2022)
ISSN: 2202-5677

Harkin et al. (2018) who found that the pervasiveness of cyber-enabled or cyber-facilitated crimes means that police officers must be ready to confront its growing relevance and the increasing public demands to respond to cyber offending.

The response of the Lagos State Police Command to cybercrime indicated that such cases were being handled by different police detachments, such as the Special Anti-Robbery Squad, the Special Task Force Unit, and the Special Fraud Unit. A major implication of this finding is that the approach of the Police Command to handling cybercrime is not wholly different from its response to offline crimes, as these police units were originally set up to fight traditional crimes such as armed robbery, fraud cases, and kidnapping. This finding corroborates the position of Whelan and Harkin (2019) that the extent to which police organisations have adequately understood and prioritised cybercrimes and their level of expertise in dealing with cyber offences have been generating serious debates.

It was also established in the study that though police personnel of the Lagos State Command were being exposed to professional training in cybercrime policing, the opportunity to enhance vocational skills was limited to some categories of police officials. The restriction of training programs on cybercrime policing to certain categories of officers may be due to the perennial paucity of funds facing the Nigeria Police Force (Ojedokun, 2021; Adebayo & Ojo, 2009. This result supports the observation of Dupont (2017) that despite the increasing recognition of the social and economic costs of cybercrime, the main beneficiaries of the increased public-sector funding to promote cyber security have been security and intelligence agencies rather than local police organisations.

Furthermore, findings on the operational strategies of the Lagos State Police Command showed that this law enforcement department recognised the intensity, scope, and devastating consequences of cybercrime and the threat that activities of cybercriminals pose to legitimate users of cyber space. Thus, it has put in place multiple strategies to combat the crime while also collaborating with other relevant stakeholders in cybercrime policing. This finding is in line with Willits and Nowacki (2016) that many police agencies are developing new strategies to combat the devastating impacts of cybercrime. Also, the fact that the Lagos State Police Command in its effort at policing cybercrime is being confronted by different institutional and non-institutional challenges may negatively affect the overall job performance and service-delivery capacity of its police personnel as it concerns the fighting of cybercrime and the detection, investigation, and prosecution of cybercriminals. Indeed, studies conducted elsewhere have linked the ineffectiveness of police agencies at fighting cybercrime to factors such as their inability to acquire necessary technologies that are essential for conducting adequate police investigations, insufficient training, and the difficulty of retaining officers who possess the appropriate skills to combat cybercrime (Holt & Lee, 2019; Koziarski & Lee, 2020; Bossler & Holt, 2012).

Volume 10, Number 2 (2022)
ISSN: 2202-5677

CONCLUSION

This study was primarily interested in understanding cybercrime policing in the Lagos State Police Command of the Nigeria Police Force. It was established that the major types of cybercrimes being handled by officials of the Command were ATM/debit card fraud, bullying, hacking, identity theft, online impersonation, and fraudulent online money transfers. The approach of the Police Command to handling cybercrime is not wholly different from its response to offline crimes. Professional training programs on cybercrime policing are restricted to certain categories of police officers. The Lagos State Police Command had developed multiple strategies for combating cybercrime. However, its cybercrime policing effort is still being hampered by various challenges.

Therefore, to effectively tackle cybercrime, it is imperative for the Lagos State Police Command to set-up a specialised unit that will be responsible for investigating and prosecuting cybercrime cases. This step is necessary because the current practice of the Command, which essentially involves assigning cybercrime cases to police units focusing on real space crimes, is unsustainable and less result oriented. The evolving nature of cybercrime and transnational mode of operations of cybercriminals require the services of specially trained and highly skilled police officials in cybercrime policing. Similarly, the Federal Government of Nigeria should make adequate funds available to the Nigeria Police Force to enable it to procure essential equipment and technologies such as relevant software applications and digital forensic tools that are needed by its State Commands for cybercrime policing, investigations of cybercriminal cases, and the collection of electronic evidence. Also, the police organisation should be financially empowered to enable it to periodically sponsor or organise professional training programs on cybercrime policing for its personnel to improve their overall service delivery capacity. Equally, it is important for the Lagos State Police Command to innovate some institutional frameworks through which it can better collaborate with relevant stakeholders such as victims of cybercrime, judicial officials, and staff of financial institutions in the investigation and prosecution of cybercriminals. Finally, the Nigeria Police Force should adequately protect and provide necessary support for its personnel who are handling cases of cybercrime to encourage them to remain resolute and unwavering in the face of likely intimidation that may be directed at them by powerful individuals wishing to interfere in their investigations.

Volume 10, Number 2 (2022)
ISSN: 2202-5677

About the authors:

Usman A. Ojedokun, PhD *is a lecturer at the Department of Sociology, University of Ibadan, Ibadan, Nigeria. He majors in the area of Criminology and Victimology. His core research areas of focus include: crime prevention and law enforcement, policing and police studies, violence, gender and cultural studies. He has worked and published extensively in these areas. His recently co-edited book, Criminal Justice System in Nigeria, funded by the Tertiary Education Trust Fund (TETFUND) was published in June, 2022. Twitter handle: @kunleojedokun.*

Samson I. Oshilaja *is a postgraduate student at the Department of Sociology, University of Ibadan, Ibadan, Nigeria.*

Volume 10, Number 2 (2022)
ISSN: 2202-5677

REFERENCES

Adebayo, H. B., & Ojedokun, U. A. (2018). Trajectories of University of Ibadan undergraduates' exposure to cyber pornography. *Journal of Social, Behavioral, and Health Sciences*, *12*(1), 140–152. doi:10.5590/JSBHS.2018.12.1.10

Adebayo, P. F., & Ojo, O. E. (2009). The challenges of effective policing as measure of controlling the phenomenon of police corruption in Nigeria today. *International NGO Journal*, *4*(3), 70–75.

Adepetun, A. (2020, January 31). 9, 000 suffer from malware attacks in Nigeria. *The Guardian*. Retrieved from https://guardian.ng/business-services/9000-suffer-fresh-malware-attacks-in-nigeria/

Aderinto, A. A., & Ojedokun, U. A. (2017). Cyber underground economy in Nigeria. In Philip Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 219–228). Ahmadu Bello University Press, Limited, Zaria.

Alade, A. (2015, March 28). INEC website hacked. *Vanguard*. Retrieved from https://www.vanguardngr.com/2015/03/inec-website-hacked/

Awan, I., & Blakemore, B. (2012). *Policing cyber hate, cyber threats and cyber terrorism*. Oxon: Routledge.

Bossler, A., & Holt, T. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management 35*(1), 165–181.

Collier, B., Thomas, R. C., Hutchings, A., & Chua, T. (2022). Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing & Society*, *32*(1), 103–124. doi: 10.1080/10439463.2021.1883608

Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing: A Journal of Policy and Practice*, *9*(2), 119–128.

Dupont, B. (2017). Bots, cops and corporations: On the limits of enforcements and the promise of polycentric regulation and as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97–116.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, *19*(6), 519–536. doi.10.1080/15614263.2018.1507889

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge, New York, NY.

Holt, T. J., & Lee, J. R. (2019). *Policing cybercrime through law enforcement and industry mechanisms*. The Oxford Handbook of Cyberpsychology.

Volume 10, Number 2 (2022)
ISSN: 2202-5677

Koziarski, J., & Lee, J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*, 43(1), 198–211. doi: 10.1108/PIJPSM-07-2019-0107

Ndubueze, P. N., & Igbo, E. U. M. (2014). Third parties and cyber-crime policing in Nigeria: Some reflections. *Policing: A Journal of Policy and Practice*, *8*(1), 59–68. doi:10.1093/police/pat034

Obayelu, A. E., & Ogunlade, I. (2006). Analysis of the uses of information and communication technology for gender empowerment and sustainable poverty alleviation in Nigeria. *International Journal of Education and Development Using Information and Communication Technology*, *2*(3), 45–69.

Ojedokun, U. A. (2021). COVID-19 pandemic lockdown enforcement: Strategies of the Nigeria Police Force and lessons for the future. *Salus Journal – Law Enforcement, National Security and Emergency Management*, *9*(2), 16–26.

Ojedokun, U. A., & Ilori, A. A. (2021). Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria. *International Journal of Criminal Justice*, *3*, 1–24.

Oyenuga, S. A. (2014). Information and communication technologies and crime in Nigeria. In A. A. Aderinto (Ed.), *Deviance and social control – An African perspective* (pp. 73–99). Ibadan: Ibadan University Press.

Peters, S. E., & Ojedokun, U. A. (2019). Social media utilization for policing and crime prevention in Lagos, Nigeria. *Journal of Social, Behavioral, and Health Sciences*, *13*(1), 11. doi:10.5590/JSBHS.2019.13.1.10

Police Executive Research Forum. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime*. Police Executive Research Forum.

Punch. (2015, July 14). Cybercriminals use carbanak malware to defraud banks – Experts. Retrieved from http://www.punchng.com/business/technology/cybercriminals-use-carbanak-malware-to-defraud-banks-experts/

This Day. (2016, April 16). Nigeria loses over N127bn annually through cybercrime. Retrieved from https://www.thisdaylive.com/index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime/

Umeh, J. (2020, February 5). Cyber security: 9, 000 Nigerians attacked by malware in 2019. *Vanguard*. Retrieved from https://www.vanguardngr.com/2020/02/cyber-security-9-000-nigerians-attacked-by-malware-in-2019/

Wall, D., & Williams, M. L. (2013). Policing cybercrime: Networked and social media technologies and the challenges for policing. *Policing & Society*, *23*(4), 409–412.

Volume 10, Number 2 (2022)
ISSN: 2202-5677

Whelan, C., & Harkin, D. (2019). Civilianizing specialist units: Reflections on the policing of cyber-crime. *Criminology & Criminal Justice*, Doi: 10.1177/1748895819874866.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies*, *29*(2), 105–124. doi:10.1080/1478601X.2016.1170282