Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 01 January-2026, Page No.-8575-8580

DOI: 10.47191/etj/v11i01.18, I.F. – 8.482

Cyber Fraud in Nigerian Banks: Trends, Regulatory Gaps, and Mitigation Strategies (2020–2025)

Chibuzor Akujobi[1], Francisa Ogwueleka[2], Gilbert Aimufua[3], Steven Bassey[4]

[1,3,4] Centre for Cyber Space Studies, Nasarawa State University Keffi, Nigeria

[2]Computer Science Department, University of Abuja-FCT, Nigeria

ABSTRACT: Cyber fraud poses a growing threat to Nigeria's banking sector, driven by rapid digitalisation, expanding electronic payment systems, and weaknesses in cybersecurity governance. Although reported fraud incidents have declined, financial losses rose sharply from ₦17.67 billion in 2023 to ₦52.26 billion in 2024, indicating increased attack sophistication. This study qualitatively reviews literature, regulatory frameworks, and major fraud cases between 2020 and 2025 to examine the drivers, impacts, and control gaps in Nigerian banks. The key challenges identified include legacy system vulnerabilities, insider collusion, weak internal controls, and regulatory enforcement gaps. The paper evaluates mitigation strategies within the context of Nigeria's evolving regulatory landscape. The findings show that regulatory and law enforcement measures alone are insufficient without strong technical controls, effective governance, staff awareness, and sustained public–private collaboration to enhance cybersecurity resilience.

KEYWORDS: cyber fraud, cybersecurity resilience, cybersecurity governance, regulatory frameworks, Nigerian Banks

1. INTRODUCTION

The Nigerian banking sector has undergone profound digital transformation over the past decade following the adoption of internet and mobile banking, Point-of-Sale (POS) systems, and other e-payment platforms. Nigeria's Central Bank has pursued a cashless policy, further incentivizing digital transactions. While these developments have increased efficiency and financial inclusion, they have also created fertile ground for cyber-enabled fraud. For example, the Central Bank of Nigeria (CBN) notes that as more customers move to electronic channels, opportunities for fraud multiply. Indeed, high-profile reports from businessday.ng indicate that cybercrime losses in Nigeria jumped from $706 million in 2022 to a projected $833 million (≈₦300 billion) in 2023. This study focuses on year 2020 to 2025 a period of intense growth in digital banking to examine how fraud trends have shifted, what major incidents have occurred, and how Nigeria's regulatory framework has responded. We utilize data from regulatory reports (CBN, NDIC, NIBSS), law enforcement (EFCC, DSS), and case journalism, supplemented by relevant academic analyses, to offer a comprehensive view of the challenges and solutions.

2, LITERATURE REVIEW

2.1 Cyber Fraud Trends (2020–2025)

The period 2020–2025 saw an unprecedented rise in fraud incidents and losses at Nigerian banks. According to the Nigeria Deposit Insurance Corporation (NDIC), fraud and forgery losses in deposit money banks were ₦5.33 billion in 2020 and jumped to ₦7.19 billion in 2021. This 34.9% increase reflected surging digital exploitation: NDIC reports show that electronic channels (mobile, internet, ATM, etc.) accounted for 88.7% of cases and 69% of losses in 2021, a notable shift from past patterns. By comparison, historical losses were lower: for example, NDIC had recorded ₦15.5 billion lost in 2018, indicating that fraud severity had grown even as overall transaction volumes expanded.

Guaranty Trust Holding Company (GTCO) noted an 84.3% surge in recorded fraud incidents in 2022 (to 27,725 events), with fraud amounts rising from ₦1.2 billion in 2021 to ₦6.4 billion in 2022. NIBSS data similarly show enormous growth in e-payments alongside rising fraud attempts. For instance, mobile money transfers hit N2.1 trillion in November 2022 and a NIBSS fraud report (cited by Nairametrics) indicated that fraud attempts on mobile banking jumped 330% in early 2020. BusinessDay reports that banks lost ₦17.67 billion to fraud in 2023, and The Guardian notes industry data estimating cumulative fraud losses of ₦52 billion in 2024 (nearly triple the 2020 total). Figure 1 illustrates this rise in reported fraud losses

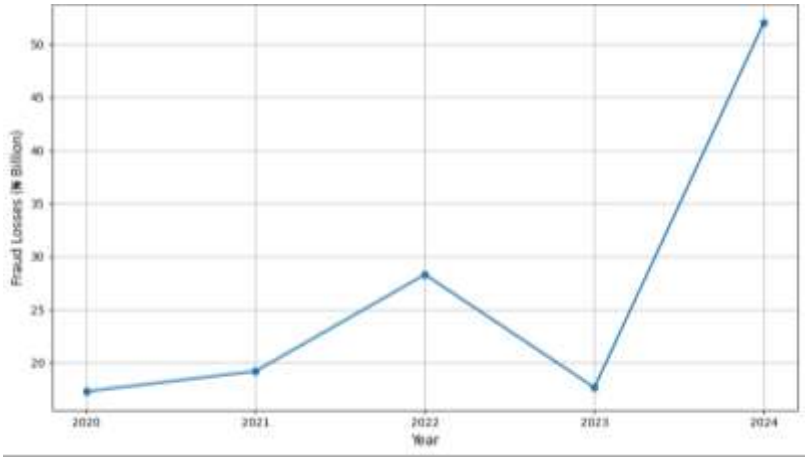

Figure: Reported Fraud Losses in Nigerian Banks(2020-2024) Source: NDIC, 2024

Electronic channels dominate 16.6% of cases were internet banking fraud (29.7% of losses) and 22.8% of cases were mobile banking fraud (20.3% of losses). In contrast, physical counters and agencies saw far fewer cases. This pattern marks a shift from historical norms where in-person fraud was larger. In 2021, ATMs still showed frequent fraud (25.4% of cases) but only 14.6% of losses. Overall, losses have been concentrated: NDIC notes that from 2020 to 2022, fraud losses soared e.g. total fraud losses climbed from ₦2.4 billion in 2020 to ₦15.15 billion in 2022 (an increase of 536%). The volume of cases also rose (fraud cases up 44.4% from 2017 to 2022.

2.2 Case Studies

A 2025 CBN fraud study found that more than 50% of bank fraud now occurs via digital platforms, with web-based and mobile fraud the largest components. Social engineering is rampant: in 2023 over 12,000 fraud cases were attributed to social engineering (phishing, vishing, impersonation). Insider participation has also grown: a Temenos survey found that roughly 70% of cyber incidents involve internal collusion at banks, and the number of bank staff implicated in fraud nearly tripled from 2021 (320 staff) to 2022 (899 staff) In short, Nigeria's banking sector is experiencing a clear acceleration in fraud: volumes, values, and sophistication of attacks are all up relative to past norms.

Table 1.1 Comparative Analysis of Selected Bank-Related Fraud Cases in Nigeria

Dimension	**Case Study 1: SIM-Swap Fraud**	**Case Study 2: Operation "Pandora's Box" (ATM Card Conspiracy)**	**Case Study 3: Fake COVID-19 Charity Scam**
Date / Timeline	August 2021	September 2020	November 2020
Financial Institutions Involved	Access Bank; First Bank of Nigeria	Multiple Nigerian banks (ATM card holders affected)	First City Monument Bank
Primary Fraud Type	SIM-swap fraud and digital account takeover	ATM card theft and organized card trafficking	Social engineering via fake online charity
Method of Fraud	Theft or acquisition of customers' SIM cards used to bypass authentication and access bank accounts	Concealment of 2,886 ATM cards and SIM cards for coordinated fraud and overseas shipment	Creation of a fake Facebook charity page linked to a fraudulent FCMB donation account
Detection / Discovery	Arrest of a suspect by Nigerian police; interrogation revealed the broader scheme	Joint raid by Nigerian Customs and the Economic and Financial Crimes Commission uncovered hoarded ATM cards	Intelligence-led investigation and manhunt by the Nigeria Police Force Intelligence Response Team
Scale and Impact	Numerous customer accounts reportedly emptied; significant financial losses	At least 10 cards confirmed stolen; thousands more prepared for fraud, indicating large-scale planned losses	Thousands of donors defrauded; exact loss figure not publicly disclosed
Key Actors Arrested	Suspected fraud syndicate members	Abubakar Ishaq (principal suspect)	Henry Ushie and accomplices

Institutional Response	Case referred to EFCC and police; funds tracing and SIM fraud controls strengthened	Suspect charged with cybercrime and money laundering; banks alerted to monitor affected accounts	Suspects charged with fraud and cybercrimes; banks advised to tighten charity account verification
Institutional Response	Case referred to EFCC and police; funds tracing and SIM fraud controls strengthened	Suspect charged with cybercrime and money laundering; banks alerted to monitor affected accounts	Suspects charged with fraud and cybercrimes; banks advised to tighten charity account verification
Regulatory / Law Enforcement Bodies Involved	EFCC; Nigeria Police	EFCC; Nigerian Customs	Nigeria Police Force
Digital Forensic Readiness Gaps Identified	Weak mobile authentication controls; poor SIM-swap prevention; reactive evidence collection	Inadequate card lifecycle monitoring; weak cross-bank intelligence sharing	Insufficient verification of special-purpose accounts; low customer fraud awareness
DFRF Implications	Need for stronger MFA, telecom–bank coordination, and proactive logging	Importance of centralized fraud intelligence, transaction monitoring, and forensic auditing	Need for policy-driven account vetting, social engineering detection, and customer education

Source: Compiled from Carnegie Endowment for International Peace (2021), EFCC (2020), and Nigeria Police Force (2020)

3. REGULATORY FRAMEWORK AND GAPS

3.1 Central Bank of Nigeria (CBN):

Nigeria has developed multiple, overlapping regulatory frameworks aimed at combating bank-related fraud; however, significant gaps remain in implementation, coordination, and enforcement. The Central Bank of Nigeria (CBN) serves as the primary banking regulator, issuing prudential regulations and consumer protection rules. In 2023, the CBN updated its Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs), mandating controls such as multi-factor authentication, intrusion detection systems, incident response planning, and compliance with emerging data protection legislation, including the Nigeria Data Protection Act (CBN, 2023). In late 2025, the CBN further released draft guidelines addressing Authorized Push Payment (APP) fraud, alongside a proposed 72-hour fraud reporting rule requiring customers to report unauthorized transactions within three days to qualify for reimbursement (Pulse Nigeria, 2025). Although these initiatives are intended to improve fraud prevention and accelerate fund recovery, their draft status limits enforceability, and the CBN's supervisory authority despite routine bank examinations and sanctions for weak controls continues to rely largely on existing statutes such as the BOFIA and the CBN Act, creating transitional enforcement gaps (CBN, 2023).

3.1.2 Nigeria Deposit Insurance Corporation (NDIC)

The Nigeria Deposit Insurance Corporation (NDIC) primarily functions as the country's deposit insurer but also plays a complementary supervisory role in monitoring bank soundness. The NDIC publishes annual fraud statistics, encourages banks to maintain fidelity insurance, and promotes stronger internal controls to mitigate fraud risks (NDIC, 2023). Although the NDIC Act empowers the Corporation to examine banks and sanction unsafe or unsound practices, it lacks criminal prosecutorial authority, and its jurisdiction is largely limited to Deposit Money Banks, excluding microfinance institutions and mobile money operators. While the NDIC has consistently highlighted systemic weaknesses such as widespread underinsurance against fraud its enforcement tools are predominantly financial, relying on fines and supervisory actions. Consequently, criminal fraud cases must be referred to the CBN or law enforcement agencies for investigation and prosecution (NDIC, 2023).

3.1.3 Economic and Financial Crimes Commission (EFCC) and DSS

At the enforcement level, the Economic and Financial Crimes Commission (EFCC) is Nigeria's lead agency for the investigation and prosecution of financial crimes and operates specialized cybercrime units that collaborate with banks on fraud detection. In recent years, the EFCC has intensified joint enforcement initiatives with the Department of State Services, including coordinated operations such as Operation Crackdown, which have resulted in notable successes, including the interception of hundreds of bank accounts linked to fraudulent activities (EFCC, 2023; The Guardian, 2023). Despite these achievements, enforcement challenges persist, as suspects frequently secure bail, evade custody, or benefit from prolonged judicial processes. Prosecution backlogs and slow case resolution continue to weaken deterrence, while the absence of a centralized national fraud bureau limits intelligence consolidation and long-term strategic coordination, despite improvements in bank–EFCC information sharing (EFCC, 2023).

3.1.4 National Information Technology Development Agency (NITDA

The National Information Technology Development Agency (NITDA) oversees national information technology and cybersecurity policy and enforces the Nigeria Data Protection Act (NDPA, 2023), giving it an indirect but increasingly important influence on the banking sector. Although NITDA is not a bank-specific regulator, its cybersecurity guidelines for critical national sectors shape banks' data governance and security architectures (NITDA, 2023). In collaboration with the Nigeria Data Protection Commission (NDPC), NITDA can sanction banks for data breaches and non-compliance, as illustrated by the ₦555.8 million fine imposed on Fidelity Bank in 2024 for privacy violations (Reuters, 2024). Nevertheless, NITDA's role in direct fraud prevention remains secondary, as its primary focus lies in data protection, privacy compliance, and cybersecurity governance rather than operational fraud investigation and prosecution (NITDA, 2023).

3.1.5 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015

3.2 Regulatory gaps and overlaps

Overall, despite the presence of multiple regulatory and enforcement bodies, Nigeria's anti-fraud framework continues to suffer from coordination challenges and overlapping mandates. The NDIC and CBN share supervisory responsibilities but rely on different enforcement mechanisms, creating inconsistencies in oversight and sanctions (NDIC, 2023; CBN, 2023). Banks have also raised concerns about unclear liability rules, particularly in cases of socially engineered fraud, where draft guidelines suggest reimbursement obligations only if customers report incidents within prescribed timelines, yet without firm statutory backing (Pulse Nigeria, 2025). Notably, Nigeria lacks a dedicated national compensation fund for fraud victims, and smaller operators such as fintech firms and third-party payment providers remain subject to fragmented oversight, under which fraud monitoring and enforcement are comparatively weak (NIBSS, 2023). In sum, while Nigeria's regulatory architecture appears comprehensive on paper, it continues to be undermined by enforcement delays, ambiguity in customer liability, and uneven coverage of emerging digital payment platforms.

4. MITIGATION STRATEGIES

4.1 Technical Controls

Banks should strengthen technical controls by deploying advanced authentication, monitoring, and security architectures to counter evolving fraud threats. Experts from INTERPOL emphasize the use of multi-factor authentication such as combining biometrics with one-time passwords (OTPs) to prevent account takeovers, alongside strong encryption for data both in transit and at rest (INTERPOL, 2022). Real-time transaction monitoring systems, increasingly powered by machine learning, can detect anomalous behavior such as sudden high-value transfers or unusual login patterns, while anti-malware solutions and intrusion detection systems should be standard across banking networks (Basel Committee on Banking Supervision [BCBS], 2021). Additional safeguards include tokenization of card data, secure application programming interfaces (APIs) for mobile and digital banking platforms, network segmentation to limit lateral movement during breaches, and regular penetration testing to proactively identify vulnerabilities (NIST, 2020).

In the context of mobile banking, closer collaboration between banks and telecommunications providers is critical to preventing SIM-swap fraud, including the introduction of dual or multi-step verification for SIM change requests (GSMA, 2021). Finally, sharing threat intelligence through collaborative platforms such as the Nigeria Electronic Fraud Forum enables early warning of emerging fraud schemes and enhances collective resilience across the financial sector (NIBSS, 2023).

4.2 Organizational Measures

Strong organizational measures are essential to complement technical controls in reducing fraud risk within banks. Robust internal governance should begin with enhanced background checks and staff due diligence, particularly for operations and other sensitive roles, in line with recommendations from the Nigeria Deposit Insurance Corporation (NDIC, 2023). The classic fraud triangle pressure, opportunity, and rationalization must be actively mitigated through structural controls such as segregation of duties, job rotation, and mandatory leave policies, which reduce opportunities for prolonged concealment of fraudulent activities (Association of Certified Fraud Examiners [ACFE], 2022). Banks should also maintain dedicated internal fraud detection and investigation units staffed with forensic accountants and analysts who conduct continuous transaction audits and internal reviews (COSO, 2017).

Comprehensive staff training is equally critical, with regular programs focused on phishing awareness, social engineering, ethical conduct, and regulatory compliance; several Nigerian banks involved in recent fraud cases have reportedly intensified ethics training and internal monitoring following major incidents (ThisDay Live, 2022). In addition, effective whistle blowing mechanisms, periodic fraud risk assessments conducted by internal audit functions or independent third parties, and sustained customer education campaigns delivered through SMS, email, and in-app alerts can significantly reduce the success rate of phishing, spoofing, and insider-enabled fraud schemes (ACFE, 2022).

4.3 Policy and Legal Measures

Strong policy and legal measures at the national level are critical for deterring fraud and improving victim protection within Nigeria's financial system. Clear and enforceable rules on fraud liability and compensation can reduce uncertainty and strengthen trust, and the Central Bank of Nigeria's

proposed 72-hour fraud reporting rule represents a positive step in this direction; however, it must be implemented with adequate consumer safeguards to avoid unfairly disadvantaging victims of sophisticated social engineering attacks (Pulse Nigeria, 2025; CBN, 2025). Regulators should also mandate the timely freezing of suspected beneficiary accounts immediately fraud is reported, supported through coordinated action involving the Nigeria Deposit Insurance Corporation and the Economic and Financial Crimes Commission (EFCC, 2023). Law enforcement effectiveness would further improve through the expansion of specialized cybercrime units equipped with modern digital forensic tools, with increased funding and training for EFCC and the Department of State Services cyber squads to accelerate investigations and prosecutions (UNODC, 2021).

In addition, public–private partnerships with cybersecurity firms and telecommunications operators can enhance the tracing of illicit transfers, particularly in cross-border fraud cases (INTERPOL, 2022). From a regulatory standpoint, the CBN, working with the Nigeria Inter-Bank Settlement System, could impose minimum fraud-reporting obligations on banks and fintechs and establish a centralized national fraud repository to improve intelligence sharing and systemic oversight (NIBSS, 2023). Finally, Nigeria's continued collaboration with INTERPOL and regional partners remains essential, as the success of coordinated joint operations such as Operation Sentinel demonstrates that sustained international cooperation can effectively dismantle complex, cross-border cyber fraud networks (INTERPOL, 2022).

5. DISCUSSION

The evidence indicates a pronounced acceleration of banking fraud in Nigeria between 2020 and 2025 compared to historical norms. While isolated fraud incidents have long existed within the banking sector, the scale and financial impact have expanded significantly alongside rapid digitalization. Fraud losses that previously amounted to low single-digit billions of naira annually have risen to tens of billions in recent years, reflecting both increased transaction volumes and the growing sophistication of fraud schemes (BusinessDay, 2024; ResearchGate, 2023). Notably, the dominant modes of fraud have shifted away from traditional practices such as currency counterfeiting and manual collusion by cashiers towards predominantly cyber-enabled threats, including phishing, malware attacks, SIM-swap fraud, and insider-assisted digital exploitation. Although this trend mirrors global developments, Nigeria's large population, uneven cyber awareness, and fragmented regulatory enforcement amplify its vulnerability.

The analysis further reveals persistent regulatory and enforcement shortcomings. Despite the existence of relatively robust legal and regulatory instruments such as the Cybercrimes (Prohibition, Prevention, etc.) Act and cybersecurity guidelines issued by the Central Bank of Nigeria implementation remains inconsistent. For example, although phishing is explicitly criminalized under Section 32 of the Cybercrimes Act, many phishing campaigns remain unpunished due to underreporting by victims, evidentiary challenges, and slow investigative processes. Similarly, the CBN's draft measures, including the proposed 72-hour fraud reporting rule, demonstrate regulatory awareness of liability and reimbursement gaps, yet their draft status limits deterrence and enforceability. Resource constraints further compound these challenges, as smaller banks and fintech firms often lack the technical capacity and funding required to fully implement advanced cybersecurity frameworks without sustained regulatory support and independent audits. While enforcement efforts by the Economic and Financial Crimes Commission and the Department of State Services have improved, the sheer volume of cyber fraud cases continues to overwhelm investigative and judicial capacity, allowing many offenders to evade meaningful sanctions. In addition, coordination among regulatory bodies particularly the CBN, the Nigeria Deposit Insurance Corporation, and the National Information Technology Development Agency remains suboptimal. Overlapping mandates and fragmented oversight weaken accountability, suggesting the potential value of a unified national cybersecurity or financial fraud coordination council involving regulators and law enforcement agencies.

Despite these challenges, there are indications of gradual progress. Industry reports and academic studies increasingly identify cyber fraud as a top systemic risk, prompting greater investment and strategic attention from banks. International collaboration has also intensified, with INTERPOL and global cybersecurity firms supporting operations against Nigerian-linked cyber fraud networks, reflecting global recognition of the threat's scale (INTERPOL, 2022). At the institutional level, many banks have begun deploying artificial intelligence driven fraud detection systems and establishing dedicated fraud operations teams. However, without sustained coordination, widespread consumer education, improved cyber hygiene, and timely regulatory updates, fraud trends are likely to continue tracking the rapid growth of digital transactions.

CONCLUSION

Between 2020 and 2025, Nigeria's banking sector experienced a marked and sustained rise in cyber fraud, posing significant risks to financial stability and public trust. Empirical evidence and documented cases show that fraud losses and incident complexity have increased well beyond historical levels, driven by pandemic-era digital adoption, expanded electronic payment channels, and increasingly sophisticated criminal techniques. Cyber-enabled fraud particularly through mobile and internet banking platforms has largely supplanted traditional fraud methods, with insider involvement emerging as a critical risk factor.

Although Nigeria's regulatory and legal framework has evolved through instruments such as the Cybercrimes Act and

enhanced cybersecurity guidelines issued by the CBN enforcement gaps persist, especially in relation to emerging fintech platforms and digital payment ecosystems. Addressing these challenges requires a comprehensive and coordinated response. Banks must strengthen technical defenses, improve internal governance, and embed continuous fraud awareness across staff and customers. Regulators, in turn, should finalize and enforce clear liability and data protection rules, enhance supervisory consistency, and deepen inter-agency coordination. Continued international cooperation, particularly through INTERPOL and regional task forces, remains essential for disrupting cross-border fraud syndicates. If implemented collectively, these measures offer a realistic pathway toward reducing cyber fraud to manageable levels, even as Nigeria's digital banking landscape continues to expand.

REFERENCES

1. Association of Certified Fraud Examiners. (2022). Occupational fraud 2022: A report to the nations. ACFE. https://www.acfe.com
2. Central Bank of Nigeria. (2023). Risk-based cybersecurity framework and guidelines for deposit money banks and payment service banks. https://www.cbn.gov.ng
3. Central Bank of Nigeria. (2025). Draft guidelines on fraud risk management and customer protection. CBN. https://www.cbn.gov.ng
4. Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. COSO. https://www.coso.org
5. Economic and Financial Crimes Commission. (2023). Annual report. https://www.efcc.gov.ng
6. GSMA. (2021). Preventing SIM swap fraud. GSMA. https://www.gsma.com
7. Institute for Security Research and Conflict Law. (2022). Cybercrime enforcement and financial fraud trends in Nigeria.
8. INTERPOL. (2022). Cyber-enabled financial crime: Global threat assessment. INTERPOL. https://www.interpol.int
9. INTERPOL. (2022). Global cybercrime operations and joint task forces. INTERPOL. https://www.interpol.int
10. Nigeria Deposit Insurance Corporation. (2023). Annual report and statement of accounts. NDIC. https://www.ndic.gov.ng
11. Nigeria Inter-Bank Settlement System. (2023). Fraud risk management and information sharing framework. https://www.nibss-plc.com.ng
12. Nigeria Inter-Bank Settlement System. (2023). Industry guidelines on fraud reporting and information sharing. NIBSS. https://www.nibss-plc.com.ng
13. National Information Technology Development Agency. (2023). National cybersecurity policy and guidelines. https://www.nitda.gov.ng
14. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). NIST. https://www.nist.gov
15. Pulse Nigeria. (2025). CBN proposes 72-hour fraud reporting rule for bank customers. https://www.pulse.ng
16. Reuters. (2024). Nigeria fines Fidelity Bank ₦555.8 million for data privacy violations. https://www.reuters.com
17. ThisDay Live. (2022). Banks tighten internal controls amid rising fraud cases. https://www.thisdaylive.com
18. United Nations Office on Drugs and Crime. (2021). Handbook on cybercrime investigations.UNODC. https://www.unodc.org