Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.149, 2025

Adjudicating Digital Laundering: Judicial Frameworks for Global Cyber-Enabled Transnational Financial Crime

Gary Kelechi Amadi*
*Nigerian Institute of Advanced Legal Studies (NIALS), Supreme Court Complex, Three Arms Zone, FCT - Abuja, Nigeria. *Email: mckellany@yahoo.com.

Abstract
Technological advancement and the fast pace of growth of digital technology and global connectivity has not just encouraged economic development, it has also led to an increase rate of cyber-enabled transnational financial crime (CTFC), presenting a challenge to global economic stability and the rule of law. Crimes like complex ransomware schemes, business email compromises, and digital currency fraud and money laundering, exploit the borderless nature of cyberspace, creating a fundamental mismatch with territorially-bound judicial systems. While existing literature often focuses on law enforcement or regulatory responses, this article addresses a critical gap by addressing the fundamental, role of the judiciary as the cornerstone for successful prosecution and global compliance. This study employs a qualitative analysis of international legal frameworks, case law, and scholarly literature to dissect the tripartite challenge facing judges: navigating jurisdictional landscapes, overcoming complex digital evidence hurdles, and enduring procedural bottlenecks in mutual legal assistance. In response, the article proposes a comprehensive framework of judicial strategies, advocating for a model shift from passive adjudication to active case management. This framework emphasizes the need for enhanced international judicial cooperation, specialized judicial training in digital forensics and emerging technologies, and interpretative strategies that harmonize legal regimes. Drawing from the context of Nigeria as a case study from the Global South, the analysis provides a grounded perspective on these universal challenges. The article concludes that empowering the judiciary with these tools is not merely an option but a requirement for closing the global enforcement gap and upholding justice in the digital age.
Keywords: Cybercrime, Cyber – enabled, Judicial - frameworks, Judiciary, Money Laundering
DOI: 10.7176/JLPG/149-11
Publication date: November 28th 2025

1. Introduction:

The digital age has transformed the global financial environment, promoting economic integration and efficiency. However, this same interconnectedness has become a tool by criminal entities, giving rise to a universal and sophisticated threat which is cyber-enabled transnational financial crime (CTFC). These crimes, which include ransomware attacks, business email compromise, and large-scale fraud schemes operating across borders, represent a fundamental challenge to the sovereignty of national legal systems and the very concept of territorial integrity.[1] The global cost of cybercrime is projected to reach an annual figure of $10.5 trillion by 2025, highlighting the high – level of the threat to economic stability worldwide.[2]

While the technological aspects of these crimes are often discussed, and law enforcement responses are frequently analyzed, a critical component of the justice pipeline remains disproportionately underdiscussed and this is the important role of the role of the judiciary. National courts, bound by traditional principles of territorial jurisdiction and mutual legal assistance (MLA) treaties and restrictions, are struggling to adjudicate cases that

*Gary Kelechi Amadi, LL.B (IMSU), B.L (Lagos), LL.M (Liverpool John Moore University LJMU), Research Fellow, Nigerian Institute of Advanced Legal Studies (NIALS)
[1] Susan W. Brenner, 'Cybercrime Jurisdiction' (2006) 1 Crime Law and Social Change, 201.
[2] Steve Morgan, 'Cyber Crime to Cost The World $10.5 Trillion Annually by 2025' (*Cybercrime Magazine*, 13 Novembe2020) https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ accessed 15 October 2023

are, by their nature, stateless and digital.[1] The existing international legal framework, including instruments such as the Budapest Convention on Cybercrime, provides a structure for cooperation but often weak in practice due to procedural delays and jurisdictional conflicts.[2] This has created a significant enforcement gap, where the rate of successful prosecution consistently fails to match the scale of criminal activity thereby eroding public trust and effectively granting impunity to offenders.[3]

This article, therefore, seeks to address this critical gap by interrogating the following central question: what judicial strategies maybe necessary to successfully prosecute CTFC and ensure global compliance with the rule of law? The article argues that overcoming the multilateral challenge of jurisdiction, digital evidence, and international procedure requires a proactive approach. Judges must evolve from adjudicators of domestic law into managers of international justice, equipped with specialized knowledge and empowered by enhanced cooperative mechanisms.

To proceed with this study, the article is divided into sections. The second section will review the existing literature on transnational crime and judicial governance, identifying the specific shortcomings in current approaches. The third section will dissect the core challenges facing the judiciary—the jurisdictional labyrinth, evidentiary hurdles, and procedural bottlenecks. The fourth section will construct a comprehensive framework of judicial strategies designed to overcome these obstacles, focusing on international cooperation, capacity building, and procedural innovation. The fifth section will provide a contextual case study from Nigeria, offering a perspective from the Global South on these universal challenges. Finally, the article will conclude with recommendations for judiciaries, policymakers, and international bodies, contending that a robust and proactive judiciary is the indispensable linchpin for a secure global digital economy.

2. An Overview of the Threat of Cyber – Enabled Transnational Financial Crimes (CTFC):

The digital revolution and advancement of technology in the world has no doubt fostered economic growth but also created opportunities to be exploited by criminals for CTFC. This section looks at the existing knowledge on CTFC, exploring definitions, scope, the pathways available to offenders, the challenges it poses to judicial systems and evolving strategies for combatting it.

Cyber – Enabled Financial Crimes refers to the traditional financially – motivated crimes amplified by information and communication technology.[4] It is important to note that these are not new crimes but already existing crimes such as fraud and theft, however amplified to a new global scale with enhanced speed, anonymity and wider reach.[5] Some common forms of CTFC include Cyber – Enabled fraud which include advance fee fraud, online scams, phishing, Cyber – Enabled theft which may include identity theft, stealing virtual assets, etc and online illicit trade, which basically refers to trading items which may otherwise be prohibited while taking advantage of the invisibility that may be obtainable online.[6]

The financial and social effects of CTFC is unprecedented. Estimates suggest that in the US alone, annual losses total approximately $158 billion, with over 21 million Americans targeted each year.[7] Understanding who commits CTFC and reasons are critical for developing effective prevention and prosecution strategies. Research indicates that the profiles of cyber-enabled offenders are heterogeneous.[8] A review by Loggen, Moneva, and Leukfeldt identifies distinct pathways into financial cybercrime, often involving a combination of technical

[1] See Ilias Bantekas, 'Jurisdiction over Cybercrimes and the Role of International Law' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 362.
[2] Council of Europe, Convention on Cybercrime (ETS No. 185), opened for signature 23 November 2001, entered into force 1 July 2004.
[3] Mark N. Latonero, 'Report on Global Policing and the Rule of Law' (Center on Crime and Security, New York University School of Law 2018) 12.
[4] Loggen J, Moneva A, and Leukfeldt R, 'A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime' (2023) 1 ScienceDirect 1.
[5] Ibid
[6] Ibid N6
[7] K. Westbrook, David P. Mansdoerfer, 'Cyber – Enabled Financial Crime is Surging: How to Fight Back' (13 February, 2025) https://www.thecipherbrief.com/column_article/cyber-enabled-financial-crime-is-surging-how-to-fight-back accessed on the 5th of October, 2025
[8] Ibid N6

curiosity, financial motivation, and social learning within online communities.[1] Nevertheless, there is still an existing gap in research on the processes of initiation into and desistance from CTFC and this makes it challenging to develop targeted interventions.[2]

Going through existing literature in the area of CTFC, a significant theme is the enforcement gap or judicial deficit created by the borderless nature of these crimes and the territorially bound nature of national judicial systems.[3] This is further complicated by the scarce resource constraints within law enforcements; a Secret Service agent once testified that "transnational fraud threats far exceed the current capacity of U.S. law enforcement to sufficiently deter," with only about 0.1% of fraud cases being investigated due to resource restrictions.[4] This in – turn emboldens offenders and strengthens CTFC and calls for a need for intelligent judicial response.

The major challenges faced by the judiciary in adjudicating over CTFC from existing literatures can be summarized into three headings which include: Jurisdictional conflicts which often interrogates the issue of uncertainty over which nation's laws apply, Evidential hurdles which are issues related to digital evidence acquisition, complications in obtaining and preserving evidence from foreign jurisdictions and Procedural bottlenecks which maybe evidenced by delays in Mutual Legal Assistance (MLA) and delays occasioned by slow formal processes of international cooperation.[5]

In response to these challenges there have been a push by governments and international bodies for a stronger global compliance regulation. Standard requirements for Ultimate Beneficial Owner reporting, Know Your Customer (KYC), and Anti – Money Laundering (AML) Protocols are becoming more rigorous worldwide, though it also inadvertently affects business operation across borders.[6] No doubts the current judicial hurdles are pushing for the need for greater transparency, with most jurisdictions expecting compliance regulations to become even more watertight.[7] Studies show that the United Kingdom and Australia are leading the charge to develop a more coordinated national strategy that mostly include provisions aimed at disrupting scam infrastructure through dismantling fraudulent or suspicious websites, requiring tech companies to verify financial advertisers against government – authorized list, mandating telecom providers to block international calls that clone domestic numbers.[8] These measures to a certain extent has led to a decline in fraud losses in the UK and Australia especially in comparison to the US.[9]

Furthermore, while there have been a number of researches in this area, gaps still exist especially in the area of evaluating the effectiveness of judicial strategies both existing and proposed in various studies, as well as specific challenges and adaptation of the legal systems operative in the Global South, who are often on the frontline of these crimes.

3. The Judiciary Challenge in Adjudicating over CTFC:

The prosecution of Cyber-Enabled Transnational Financial Crime (CTFC) confronts national judiciaries with problems which traditional legal doctrines are not fully equipped to tackle. The borderless and transient nature of

[1] ibid
[2] ibid
[3] K. Westbrook, David P. Mansdoerfer, 'Cyber – Enabled Financial Crime is Surging: How to Fight Back' (13 February, 2025) https://www.thecipherbrief.com/column_article/cyber-enabled-financial-crime-is-surging-how-to-fight-back accessed on the 5th of October, 2025
[4] ibid
[5] Loggen J, Moneva A, and Leukfeldt R, 'A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime' (2023) 1 ScienceDirect 1.
[6] 'Global compliance challenges and business complexity' (TMF Group, 6 July 2023). https://www.tmf-group.com/en/news-insights/articles/global-business-complexity/global-compliance-challenges-business-complexity/ accessed on the 5th of October, 2025.
[7] ibid
[8] K. Westbrook, David P. Mansdoerfer, 'Cyber – Enabled Financial Crime is Surging: How to Fight Back' (13 February, 2025) https://www.thecipherbrief.com/column_article/cyber-enabled-financial-crime-is-surging-how-to-fight-back accessed on the 5th of October, 2025
[9] ibid

digital evidence creates a fundamental conflict with the territorially-bound foundations of criminal law.[1] This conflict maybe summarized into these three issues: Jurisdictional conflict, Evidential hurdles, and Procedural bottlenecks.

3.1 Jurisdictional Conflict:

The principle of territorial sovereignty is the bedrock of international law and it stipulates that a state's criminal jurisdiction is primarily limited to offences committed within its territory.[2] A single criminal act of cyber enabled transnational financial crime can involve a perpetrator in one country, a victim in a second, and servers hosting the criminal infrastructure in a third country. This creates a hydra – headed conflict of laws and a foundational question: *which court is competent to adjudicate?* While international law has developed doctrines to address extraterritorial crime, such as the subjective territoriality principle (where the crime was initiated) and the objective territoriality principle (where the crime was completed or its effects felt), their application in cyberspace is still ambiguous.[3] The 'effects doctrine' can be interpreted widely as to accommodate and grant jurisdiction to any state where financial loss is suffered, leading to a risk of concurrent and conflicting prosecutions.[4] Equally, the requirement of 'dual criminality' for cooperation where the act must be a crime in both the requesting and requested state can create a safe landing for offenders if a jurisdiction is yet to update its laws to criminalize specific cyber-enabled activities.[5] This jurisdictional issues often result in legal paralysis, where no state is willing or able to take the lead in prosecution, unintentionally granting impunity to offenders.

3.2 Evidential hurdles:

Where jurisdiction is established, the task of securing admissible evidence presents a challenge. Digital evidence is volatile, easily altered, and can be stored or transferred across multiple jurisdictions in a matter of seconds. For a judge, ensuring the integrity and authenticity of such evidence is paramount.

The first hurdle is acquisition. Law enforcement agencies in the victim's country may lack the legal authority to directly collect evidence from servers located abroad. They must rely on international cooperation, a process that is often stringent and slow – paced to capture data which may be easily altered.[6] Once obtained, the evidence must be verified to prove it's authenticity and that it has not been tampered with. This requires a verifiable chain of custody that documents every person who handled the evidence from its seizure to its presentation in court; a chain that becomes exponentially more difficult to maintain across international borders and multiple agencies.[7] Also, rules of evidence differ from jurisdiction to jurisdiction. Procedures that are standard for obtaining digital evidence in one country may violate the fundamental legal principles of another, potentially rendering the evidence inadmissible under exclusionary rules.[8] Judges are therefore faced with a dilemma: to admit evidence critical to securing a conviction that was obtained through uncertain but maybe legal means abroad, or to exclude it and risk acquitting a guilty party. This undermines the fairness of the trial and the integrity of the judicial process.

3.3 Procedural Bottlenecks:

Usually the mechanism for overcoming these jurisdictional and evidential barriers is through the Mutual Legal Assistance (MLA). However, the MLA process is fraught with bottlenecks. The process is can be slow,

---

[1] Ilias Bantekas, 'Jurisdiction over Cybercrimes and the Role of International Law' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 362.

[2] See; *The Case of the S.S. "Lotus" (France v Turkey)* (1927) PCIJ Series A No 10, 18-19.

[3] Susan W. Brenner, 'Cybercrime Jurisdiction' (2006) 1 Crime Law and Social Change 201, 205-210.

[4] UN Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (United Nations 2013) 78.

[5] Council of Europe, *Transborder Criminal Law and the Budapest Convention: A View from Nigeria* (COE 2020) 12.

[6] E. Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 45.

[7] See' *R v Allpress* [2009] EWCA Crim 8, [54] (considering the integrity of evidence handled by multiple officers).

[8] Mark Zimble, 'The Admissibility of Electronic Evidence in Civil and Commercial Disputes in Nigeria' (2021) 15(1) UNIZIK Law Journal 112, 120.

bureaucratic, and ill-suited to the rapid pace at which digital evidence can be destroyed or moved.[1] Often times requests go through various central authorities, be translated, and comes with specific procedural requirements of the requested state. This can take months in some cases years, by which in some cases may affect the prosecution's case.[2] The 2001 Budapest Convention on Cybercrime intended to simplify this by encouraging direct cooperation between law enforcement agencies, but its adoption and implementation are uneven, and many requests still must follow the traditional MLA procedure.[3]

These procedural delays are further impacted by a lack of trust and reciprocity between judicial systems. Concerns over human rights standards, data protection regimes, and the independence of foreign judiciaries can cause states to refuse or delay assistance.[4] These issues of cooperation leaves judges and prosecutors in a precarious position, holding the jurisdictional mandate to try a case but lacking the procedural tools to access the evidence required to come to a conclusion and deliver a verdict.

4. A Framework for Judicial Strategies: From Adjudication to Active Management:

Following the challenges as discussed in section 3 of this article, it is important that the judiciary do not remain passive and only waiting for well worked cases to arrive. Successfully prosecuting Cyber – Enabled Transnational Financial Crime (CTFC) demands effective strategies and trusted judicial case management. This section proposes a comprehensive framework, encouraging judges to evolve from adjudicators to proactive facilitators of international justice. This framework is built on four pillars which are fostering enhanced international cooperation, mastering digital evidence process, enhancing specialized judicial capacity and deploying interpretative techniques for interpretation.

4.1 Fostering Proactive International Judicial Cooperation:

The nature of the traditional diplomatic channels for cooperation necessitates that judiciaries develop their own networks and procedures. An avenue that may be explored is developing more conversations around establishing direct judicial channels. These channels can facilitate swift execution of commissions, letters of request between designated judicial authorities and thereby effectively but legally side stepping some of the bureaucratic delays inherent in MLA.[5] Also, judicial officers are encouraged to take advantage of and actually champion the use of Joint Investigation Teams (JITs), as provided under articles like the European Union Convention on Mutual Assistance in Criminal Matters.[6] Though JITs are mostlyy seen as law enforcement tools, Judicial oversight is important from their inception. A judge can provide guidance on the admissibility of evidence collected by JIT while maintaining neutrality in the matter, ensuring that multinational investigations follow established standards and protocols and can withstand scrutiny at trial.[7] Judges are also encouraged to leverage informal cooperation and memoranda of understandings with counterpart judiciaries in high – risk jurisdictions, establishing protocols for urgent preservation requests and the exchange of non – controversial evidence.[8]

4.2 Understanding the Digital Evidence Process:

[1] Theodore Christakis, 'Mutual Legal Assistance in the Digital Age: The Challenges and Limitations of the MLA System' (2020) 6 European Law Journal 1, 5.

[2] See the analysis of delays in *A Guide to Mutual Legal Assistance* (U.S. Department of Justice 2019) 3.
[3] Council of Europe, Convention on Cybercrime (ETS No. 185), opened for signature 23 November 2001, entered into force 1 July 2004, arts 23-35.
[4] *Barcelona Traction, Light and Power Company, Limited (Belgium v Spain) (Second Phase)* [1970] ICJ Rep 3, [33]
[5] See United Nations Office on Drugs and Crime (UNODC), *Global Judicial Integrity Network* (UNODC 2018) 5.
[6] See European Union Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C197/1, art 13.
[7] *Director of Public Prosecutions v B* [2018] IEHC 550, [32] (highlighting the role of judicial approval in multinational evidence gathering).
[8] See generally, the model provided by the Commonwealth *Scheme for Mutual Assistance in Criminal Matters*.

The reliability of a CTFC prosecution centers on the digital evidence presented. Judges are therefore expected to master and take an active role in managing this evidence from the earliest stages. This includes issuing preservative and production orders with extraterritorial effect, compelling entities within their jurisdiction to preserve data held abroad, a practice increasingly recognized as necessary.[1]

To address challenges relating to reliability and authenticity of evidence, judiciaries should advocate for and adopt standardized protocols for digital evidence, an example may be seen in the UNODC Handbook on Digital Evidence, The UNODC protocol provides a model for chain of custody documentation.[2] Significantly, judges must be positioned to apply a bit of discretion in admitting evidence obtained through expedited, non-traditional channels, provided its integrity and reliability can be verified. A rigid insistence on formal MLA treaties as the only valid route may affect the delivery of justice.[3] The guiding principle should be the balance between procedural fairness and the substantive need to combat impunity for serious crime.

5. Improving Judicial Capacity and Specialization:

The technical intricacy of CTFC necessitates a specialized judiciary. The most effective response is the creation of specialized cybercrime courts or the designation of specialist judges.[4] This concentration of expertise will allow for the development of deep institutional knowledge, consistent development of jurisprudence around CTFC, and a more effective and competent case management.

This must also be supported by mandatory, continuous legal education. Judicial training programmes must move beyond basic digital literacy to cover more complex and evolving topics such as cryptocurrency tracing, the technical foundations of blockchain, fundamentals of digital forensics, and comparative international cyberlaw.[5] This can be supported by publications in these are and practice directions specifically on CTFC cases for judicial officers. These guidelines and protocols would provide judges with checklists for managing jurisdictional arguments, frameworks for assessing digital evidence, and model case studies, precedents and instructions to explain complex technical concepts.[6]

6. Enhancing Interpretation Strategies for Harmonization:

While working to improve and build judicial capacity to manage CTFC cases, judges can use their interpretative function to bridge gaps. This involves an intentional interpretation of domestic statutes to ensure they remain fit for purpose in the digital age. For instance, definitions of "property" or "document" can be interpreted to include digital assets and data files.[7]

Additionally, judicial officers are encouraged to explore foreign and international jurisprudence as guiding authority where need be. While not binding, reasoned judgments from other jurisdictions handling similar issues can provide valuable insights and foster a gradual harmonization of legal approaches to CTFC.[8] By engaging in this judicial dialogue, courts can help create a more predictable and coherent global legal environment, discouraging forum shopping by offenders.

---

[1] See *Microsoft Corp v United States* 829 F.3d 197 (2d Cir 2016), 222 (discussing the territorial reach of US warrants, though later superseded by the CLOUD Act, the principles inform the debate).
[2] UNODC, *Handbook on Digital Evidence and Information in Criminal Proceedings* (UN 2021) 25-30.
[3] *R v Grant* [2005] EWCA Crim 1089, [53] (addressing the judicial discretion to exclude evidence, but the logic applies to inclusion where fairness is maintained).
[4] The Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 49, implicitly encourages this by providing for the designation of specific judges.
[5] World Bank, *A Comprehensive Study of Cybercrime Legislation and Case Law in Select Countries* (World Bank 2020) 45.
[6] An example is the UK Judicial College, *Crown Court Compendium* (2022) which includes guidance on summing up cybercrime to juries.

[7] For example, the Nigerian Advance Fee Fraud and Other Fraud Related Offences Act defines "property" inclusively, which can be interpreted to encompass virtual assets.
[8] The influence of foreign precedent is evident in cases like *Google LLC v Equustek Solutions Inc* [2017] 1 SCR 824 (Supreme Court of Canada) which cited *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575 (High Court of Australia).

7. The Global South Perspective (A case study of Nigeria):

Nigeria, as a major economic and digital hub in Africa, presents a compelling case study. It is a jurisdiction simultaneously victimized by, and often incorrectly stereotyped as a primary source of, cyber-enabled financial crime. Analyzing Nigeria's experience provides critical insights into the universal challenges of prosecuting CTFC and highlights the urgent need for the strategic shifts proposed in this article.

7.1 Nigeria's Encounter with CTFC:

Nigeria's rapid digital expansion has been paralleled by a surge in sophisticated CTFC. The country is affected by both domestically perpetrated crimes and transnational schemes targeting its growing online population. Prevalent crimes include the infamous "Yahoo Yahoo" schemes, which include advance-fee fraud, romance scams, Business Email Compromise (BEC) as well as cryptocurrency-related fraud.[1] Nigeria has also been the subject of major transnational attacks, such as the 2020 hacking of a Bulgarian pharmaceutical company, which was traced to a Nigerian national, further showing the cross-border nature of the threat.[2] This environment no doubt tests the resilience of the Nigerian judiciary, which operates within a legal system coping to keep pace with fast development in the technological space and especially as it relates to crime.

7.2 Domestic Legal and Judicial Responses:

Nigeria as a country has not been unresponsive to these effects and this led to the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. This legislation criminalizes a range of cyber activities, provides for the procedural powers of law enforcement, and crucially, in Section 49, mandates the designation of a Judge in each Federal High Court to handle cybercrime cases.[3]

On the other hand, the establishment of the Economic and Financial Crimes Commission (EFCC) has been significant to the fight.[4] In 2024 alone, Nigerian courts recorded 4,111 financial crimes convictions primarily facilitated by the Economic and Financial Crimes Commission (EFCC). This achievement can partly be credited to stronger collaborations between enforcement agencies and the judiciary, due to the crucial role of the Corruption and Financial Crime Cases Trial Monitoring Committee (COTRIMCO) in accelerating trials. However, there remains an increasing vulnerability of individuals and organisations to cyberattacks, particularly in the telecommunications, social media platforms and banking sectors. An analysis of some of the cases demonstrates both judicial and procedural wins and failures.

In this popular case; *EFCC v. Obiwanne Okeke***,** The *Economic and Financial Crimes Commission (EFCC) v Obinwanne Okeke,* commonly known as Invictus Obi, offers a critical lens through which to evaluate Nigeria's judicial and procedural capacity in prosecuting economic and cybercrimes. With its blend of domestic and international legal implications, the case stands as a milestone for Nigeria's anti-corruption and transnational financial crime.

Obinwanne Okeke rose to fame as a young entrepreneur and received recognition in international media before his arrest in 2019. He was charged with orchestrating a transnational cyber fraud scheme targeting American businesses and individuals, including a notable USD 11 million fraud against a U.S.-based company[5]. Okeke was arrested by the Federal Bureau of Investigation (FBI) and later extradited to the United States, where he pleaded guilty and received a 10-year prison sentence in 2021. Meanwhile, the Economic and Financial Crimes Commission (EFCC) launched parallel investigations into his activities in Nigeria.[6] This Nigerian case aimed to investigate and prosecute the local aspects of his operations, including asset acquisition and money laundering.

---

[1] Nigeria's Battle Against Cybercrime: An Overview of the "Yahoo Yahoo" Phenomenon' (*The Guardian Nigeria*, 15 March 2023) 21.
[2] 'Bulgaria Firm Hacked by Nigerian, Says Official' (*Punch Newspapers*, 4 February 2020) 12.
[3]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 49.
[4] Economic and Financial Crimes Commission (Establishment) Act 2004.

[5] United States Department of Justice, 'Nigerian National Sentenced for $11 Million Fraud Scheme' (DOJ, 16 February 2021) https://www.justice.gov/opa/pr/nigerian-national-sentenced-11-million-fraud-scheme accessed 7 April 2025
[6] Economic and Financial Crimes Commission, 'EFCC Press Releases on Obinwanne Okeke' (EFCC, 2020) https://www.efcc.gov.ng accessed 7 April 2025.

Nigerian courts have demonstrated a willingness to adapt, with judges increasingly confronting issues of digital evidence. Also, in *FRN v. Osuagwu*, the court admitted electronic evidence in the form of instant messaging transcripts in dealing with issues of authentication in a fraud case.[1]

However, the system faces profound challenges. The Section 49 provision for the designation of specialized judges or courts has not been effectively implemented across board for so many reasons which include capacity and numbers and often overloaded with other complex commercial cases. Furthermore, a significant hurdle remains the proof of *mens rea* (criminal intent). In *EFCC v. Okechukwu***,** the Court of Appeal emphasized that for a conviction under the Cybercrimes Act, the prosecution must prove not just the act, but the specific intent to defraud, which can be difficult with complex digital anonymization techniques.[2] This echoes the evidential hurdles discussed earlier in this article.

7.3 The Cooperation and Jurisdictional Issues:

Nigeria's experience with international cooperation captures the procedural bottlenecks discussed earlier in this work. As a party to the Budapest Convention, Nigeria can request assistance, but the process is often hampered by perceived issues of institutional trust and capacity among partner nations.[3] Requests for evidence from foreign-based technology companies can be delayed for years, and this often times has devastated effects on prosecution and in turn convictions.

An example is the international dimension of the "Ray Hushpuppi" case**,** this is a case of a Nigerian social media influencer, indicted in the United States for massive transnational fraud. While this case led to a successful prosecution in the U.S., it also highlighted the jurisdictional tensions that can arise.[4] It highlighted the reality that where a clear jurisdictional methodology exists to a powerful foreign judiciary, cases may be ceded, potentially impeding the development of robust domestic jurisprudence in countries like Nigeria. This dynamic risk perpetuating a form of judicial dependency, undermining the goal of building a self-reliant, capable judiciary in the Global South.

7.4 Lessons for the Global Community:

Transnational financial crimes thrive in the gaps between national legal systems. These crimes are not constrained by geography, yet the mechanisms to prosecute them often are. Effective judicial cooperation, therefore, is not merely advantageous but imperative. It demands a blend of legal harmonization, trust-building between nations, and innovative use of technology to bridge jurisdictional divides.[5]

At the heart of international judicial cooperation lies the recognition that no single country can unilaterally dismantle cybercrime syndicates. Criminals exploit differences in legal frameworks, slow-moving bureaucratic processes, and the anonymity afforded by digital tools. For instance, a ransomware attack orchestrated from Russia, targeting a German company, and funneling proceeds through a Nigerian crypto exchange, illustrates the complex nature of these crimes. Successfully prosecuting such cases requires seamless collaboration between multiple jurisdictions.

Organizations like INTERPOL and Europol play pivotal roles in streamlining these efforts. Europol's European Cybercrime Centre (EC3)**,**[6] for example, has disrupted transnational fraud rings by coordinating simultaneous

[1] *Federal Republic of Nigeria v Osuagwu* (Unreported, Federal High Court, Lagos Division, Suit No FHC/L/565C/2019, 12 November 2021).
[2] *Economic and Financial Crimes Commission v Okechukwu* [2021] LPELR-56321(CA).
[3] Council of Europe, *Transborder Criminal Law and the Budapest Convention: A View from Nigeria* (COE 2020) 15.
[4] United States Department of Justice, 'Six Indicted in International Scheme to Defraud Qatari School Founder and Then Launder Over $1 Million' (Press Release, 25 November 2020).
[5] Unodc, 'Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape' (*Https://wwwunodcorg/unodc/en/cybercrime/homehtml*, October 2024)<https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf> accessed 22 April 2025
[6] INTERPOL 'National Cybercrime Strategy Guidebook', April 2021.

raids across continents. Similarly, the Financial Action Task Force (FATF) pushes for global standards in tracking illicit financial flows, urging nations to adopt rules like the "Travel Rule" for cryptocurrency transactions.[1]

Nigeria's position as Africa's largest digital economy makes it both a target and a transit point for cyber-enabled financial crimes. The country has taken steps to bolster cooperation, however, systemic hurdles limit its effectiveness.[2] Some of these systemic hurdles include, slow-paced MLAT Processes which has been earlier identified in this article**;** Nigeria's reliance on MLATs to secure evidence from foreign jurisdictions is sometimes hampered by bureaucratic delays. Another hurdle also earlier noted is capacity gaps, while anti – corruption agencies have cybercrime units, many lacks technical training or access to advanced tools like blockchain analytics software. This limits their ability to collaborate meaningfully with counterparts in other jurisdictions as well as Regional Fragmentation**,** West Africa lacks a unified framework for cybercrime cooperation. While ECOWAS has adopted a regional cybersecurity strategy, implementation remains uneven.[3]

The Nigerian case study yields two critical lessons for the global fight against CTFC. First, it demonstrates that the challenge is universal, but its impacts are mostly felt in jurisdictions with fewer resources. The strategies of proactive judicial management, specialized training, and direct judicial cooperation are operational necessities and way forward with the fast-paced development and technological advancements.

Second, it reveals that international cooperation must be focused towards equity and capacity-building**.** The present MLA regime with its complexities, though the idea is understandable; However, a more sustainable model requires developed nations to invest in the digital forensic and judicial capacity of their partners in the Global South, this will have a long – term effect in crime detection and prosecution for both developed and developing nations.[4] This may come in the form of support in the area of capacity building and exchange courses for the Nigerian judges on digital evidence and facilitating direct judicial links. The effectiveness of the global response to CTFC will be determined not by the strength of the strongest judiciary, but by the resilience of the most vulnerable and overburdened ones.

8 A Case for a Comprehensive Global Compliance Regime:

All the discussions and analysis above points to a fact which is that the judiciary is the essential but almost overlooked sector for transforming the international response into a comprehensive global compliance regime for CTFC. While law makers enact laws and law enforcement agencies investigate, it is the judiciary that ultimately operationalizes these norms, giving them practical force and legitimacy. This article argues that the active judicial management framework proposed in Section 4 is not just a tactical improvement but a strategic necessity for closing the enforcement gap and upholding the rule of law in the digital age.

An over-reliance on state-to-state diplomatic and executive channels for cooperation, which are inherently slow and politically contingent[5] creates a procedural void that judiciaries, through their unique function as impartial arbiters of law, are uniquely positioned to fill. The strategies of fostering direct judicial cooperation and employing harmonizing interpretation techniques are not about distorting executive authority and legislative intentions, it is however about creating parallel, specialized methods for justice that can operate with the speed and expertise the digital era demands. This reflects a broader trend in transnational governance where 'judicialization' helps to depoliticize and streamline complex cross-border issues.[6]

[1] Ibid N7

[2] Snail ka Mtuze, S. Dr. Ifeoma Nwafor: *Cybercrime and the law: issues and developments in Nigeria*. (2022) CLDS Publishing. pp. 1–285. *Int. Cybersecur. Law Rev.* **4**, 253–254 (2023). https://doi.org/10.1365/s43439-023-00080-3

[3] Ibid N12

[4] UNODC, *Strengthening International Cooperation in Cybercrime* (UN 2021) 32.

[5] Theodore Christakis, 'Mutual Legal Assistance in the Digital Age: The Challenges and Limitations of the MLA System' (2020) 6 European Law Journal 1, 8-10.

[6] Anne-Marie Slaughter, *A New World Order* (Princeton University Press 2004) 65.

Likewise, A case study of Nigeria as an example in the Global South provides a powerful indication to the judicial challenge and the imbalances of the current system. It demonstrates that without proactive judicial strategies and enhanced capacity, jurisdictions in the Global South risk being perpetually caught in a cycle of being high-volume venues for CTFC but low-capacity venues for its adjudication. This not only undermines their own domestic security but also creates safe havens and weak links that threaten global efforts. The case for international cooperation and commitment in judicial capacity building is therefore not merely one of solidarity but of collective self-interest. An active and effective judiciary in Nigeria directly enhances the ability of courts in Europe, North America, and Asia to secure evidence and convictions, creating a positive feedback loop of compliance and Nigeria aside this applies to most countries in the global south.

This proposed systemic shift also addresses the dilemma of sovereignty against cooperation. Critics may argue that enhanced judicial cooperation and the use of foreign jurisprudence could infringe upon national legal sovereignty.[1] However, this view is do not tell the whole story. In the context of CTFC, sovereignty is not being ceded but is rather being pooled to combat a common threat that individual states may not be able to control alone due to its often hydra – headed nature. By engaging in judicial dialogue and adopting specializes /harmonized procedures, judges are not surrendering their national sovereignty; they are managing it in a way that will ensure effectiveness in this present borderless world.[2] The principle of comity, which is a peculiar feature of private international law, must be guardedly and consciously integrated into the judicial reasoning for criminal matters of a transnational nature.[3]

The quest for global compliance against CTFC cannot be achieved by legislation or technology alone. Laws like the Nigerian Cybercrimes Act 2015 provide the necessary foundation, but they remain passive without a judiciary adequately equipped and empowered to apply them effectively across borders.[4] The framework presented here repositions the judge from a passive gatekeeper of domestic procedure to an active manager of justice. This involves not only administering trials but also ensuring evidence collection is properly positioned, guiding multinational investigations, and building a consistent body of jurisprudence through engagement with global counterparts.

By embracing this role, the judiciary moves beyond simply convicting individual offenders. It becomes the primary institution for validating and enforcing global anti-cybercrime norms, thereby creating the credible deterrence that is currently lacking. Each successfully adjudicated CTFC case, guided by the principles of fairness, cooperation, and specialized knowledge, reinforces the global compliance regime and signals that the digital space is not lawless, but a space where the rule of law, administered by a capable and interconnected judiciary, will prevail.

9 Recommendations:

9.1 Implement Specialization: it is important for the judiciary to operationalize the designation of courts or judges as envisioned by the Cyber Crime Act 2015 of Nigeria. This will help in building expertise in the CTFC as well as build reliable precedence in the area.

9.2 Adopting Proactive Case Management Protocols: Judicial officers especially judges are encouraged to actively use their powers to issue preservative orders for data held abroad and manage pre – trial processes to resolve jurisdictional and evidential disputes.

9.3 Continuous Capacity Building: The digital space evolves and changes every day and to meet with these challenges, judicial training must not only be mandatory but supported adequately by authorities.

[1] See generally, the dissenting opinion in *R v Hape* [2007] 2 SCR 292, which emphasised rigid territorial sovereignty.
[2] Neil Walker, 'The Sovereignty Surplus' (2019) 17 International Journal of Constitutional Law 399, 405.
[3] *Hilton v Guyot* 159 US 113 (1895), 163-164 (defining the doctrine of comity as "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation").
[4] Cybercrimes (Prohibition, Prevention, etc.) Act 2015

9.4 Governments who are yet to do so should prioritize the ratification of relevant treaties, such as the Budapest Convention on Cybercrime and ensure domestic legislation is fully aligned to facilitate cooperation among member states.[1]

9.5 Lawmakers and stakeholders in law enforcement must regularly review and update the criminal codes and evidence acts to address the ever-changing nature of CTFC, digital assets. This will not only accommodate the admissibility of electronic evidence, it will also clarify extraterritorial jurisdiction.

9.6 International organization should promote and develop model protocols for direct judicial cooperation and the handling of CTFC evidence, this is aimed at reducing procedural issues.

9.7 Nations with a more robust and active criminal justice system in the area of CTFCs and International organizations are encouraged to prioritize support for capacity building programs, focusing on technical training and sharing of knowledge and experiences. Also, support should be enhanced for existing platforms like the Global Judicial Integrity Network to include a specific focus on CTFC. This will create a repository of best practices as well as directory for judicial contact.

10 Conclusion:

This article has argued that the spread of Cyber-Enabled Transnational Financial Crime (CTFC) represents a fundamental challenge to equality of states and the doctrine of exclusive territorial jurisdiction, creating an enforcement gap that undermines global economic security and the rule of law. Through an analysis of the challenges, the jurisdictional issues, evidential hurdles, and procedural bottlenecks; it is clear that traditional judicial approaches are inadequate. The case study of Nigeria further illustrates that this is a universal predicament, though one with disproportionate impacts on judiciaries in the Global South.

The article also argued that bridging this enforcement gap requires a concerted shift within the judiciary. Judges must evolve from passive adjudicators bound by territorial limits into active managers of international justice. The proposed framework of strategies, emphasizing proactive international cooperation, advanced knowledge of digital evidence, specialized capacity building, and harmonization of interpretation provides a starting point for this transformation. The judiciary must not be seen as a secondary actor but an important actor for converting international legal norms into concrete global compliance.

The fight against CTFC will be won not by building higher digital walls, but by forging stronger bridges between the world's judiciaries. Empowering judges with the authority, knowledge, and networks to manage the complexities of transnational digital crime is the most critical step towards a future where the rule of law is as borderless as CTFC.

[1] Council of Europe, Convention on Cybercrime (ETS No. 185).