Journal of Management and Economic Sciences Prospects | Volume: 10 / N°: 01 (2026), p 318-335

From Pandemic Shock to Infrastructural Criminality: Global Economic Cybercrime, 2020–2026

KAID MOUNA [*1]

[1] Faculty of Economic Sciences, Commercial Sciences and Management Sciences, University of Ouargla

(e-mail: kaid.mouna@univ-ouargla.dz)

Received: 16/04/2026 *Accepted: 07/07/2026* *Published:30/07/2026*

Abstract:

This article examines the global evolution of economic cybercrime from the COVID-19 crisis to 2026 by combining official cybercrime and fraud reports with an explanatory layer drawn from open institutional indicators on digital exposure, financial inclusion, and institutional response. It argues that the period should not be read merely as one of rising online fraud, but as a structural transition toward infrastructural criminality, in which illicit profit extraction increasingly operates through the ordinary infrastructures of the digital economy itself: remote onboarding, e-commerce, instant payments, fintech services, messaging platforms, virtual assets, and cross-border laundering channels. Methodologically, the study adopts a longitudinal comparative documentary design based on reports issued by the FBI Internet Crime Complaint Center (IC3), INTERPOL, FATF, Europol, ITU, the World Bank, and UNODC. The analysis identifies three major shifts: pandemic-driven digital expansion in 2020–2021, deeper convergence between fraud and illicit financial flows in 2022–2023, and the industrialization of deception in 2024–2026 through scam centres, fraud-as-a-service, AI-enabled impersonation, and crypto-based concealment. The article concludes that economic cybercrime is no longer best interpreted as a peripheral subtype of cybercrime, but as a central transnational criminal economy embedded in digital modernity

Keywords: economic cybercrime; cyber-enabled fraud; illicit financial flows; digital financial infrastructures.

Jel Classification Codes : K42, G28, L86, O33, F65

* ***Corresponding author***

I. INTRODUCTION

The COVID-19 crisis marked a turning point in the global evolution of economic cybercrime. As work, commerce, payments, and communication shifted rapidly into digital environments, cyber-enabled deception expanded into a broader range of everyday routines. Early official assessments already warned that the pandemic was intensifying phishing, online fraud, extortion, and ransomware risks, but the more consequential development came later: the same digital systems that sustained continuity during the crisis increasingly became operating environments for organized illicit extraction .

By 2024–2026, official reports no longer described the problem as a simple rise in "online scams." Instead, they portrayed a globally connected criminal environment in which fraud, money laundering, fintech abuse, virtual assets, organized scam centres, criminal service markets, and AI-enabled impersonation had become increasingly intertwined. INTERPOL's 2026 threat assessment places financial fraud among the world's top five crime threats, reports a 54% increase in fraud-related Notices and Diffusions from 2024 to 2025, and estimates global financial fraud losses in 2025 at USD 442 billion (INTERPOL, 2026, pp. 5, 7). FATF's 2026 paper likewise describes cyber-enabled fraud as one of the most widespread and damaging profit-motivated crimes (FATF, 2026, p. 2).

1. Problem Statement

Although international reporting on cyber-enabled fraud has become richer since the pandemic, the phenomenon is still often treated in fragmented ways: as online fraud, as cybercrime, as financial crime, or as a money-laundering risk. What remains insufficiently theorized is the **longitudinal transformation** that took place across 2020–2026. The key issue is not simply that more fraud occurred online after the pandemic, but that the digital economy itself increasingly became the environment through which illicit value was generated, moved, concealed, and scaled. FATF emphasizes that many contemporary fraud schemes now integrate laundering mechanisms from the outset, while INTERPOL and Europol describe fraud as increasingly organized, transnational, and business-like

2. Main Research Question

How did economic cybercrime evolve globally from the COVID-19 crisis to 2026, and what structural transformations best explain its shift from crisis-driven digital opportunism to a more organized, financialized, and industrialized transnational criminal economy?

3. Sub-Research Questions

First, how did pandemic-era digital acceleration reshape the scale and reach of economic cybercrime between 2020 and 2021?

Second, to what extent did post-pandemic cyber-enabled fraud become increasingly integrated with illicit financial flows, laundering channels, fintech abuse, and virtual assets between 2022 and 2023?

Third, what evidence indicates that 2024–2026 marked a new phase of industrialization through scam centres, fraud-as-a-service, and AI-enabled deception?

Fourth, how do official reports distinguish between growth in complaint volume and deeper structural transformation?

Fifth, what major indicators reveal that economic cybercrime has become more transnational, more collaborative, and more embedded in digital infrastructures than in the early pandemic period?

4. Analytical Hypotheses

This study advances five analytical hypotheses:

H1: The COVID-19 crisis did not merely coincide with a temporary increase in cyber-enabled fraud; it appears to have accelerated the expansion of the exposure base of economic cybercrime by increasing dependence on remote communication, digital payments, and platform-mediated trust.

H2: from 2022 onward, economic cybercrime became increasingly defined by the convergence of fraud with illicit financial circulation, especially through mule accounts, fintech channels, and virtual assets.

H3: between 2024 and 2026, economic cybercrime entered a more industrialized phase characterized by scam centres, service-based criminal markets, modular criminal labor, and AI-assisted deception.

H4: the contemporary distinctiveness of economic cybercrime lies less in technical novelty alone than in its embedding within the ordinary infrastructures of the digital economy.

H5: its transnational expansion has been facilitated by uneven regulatory capacity, fragmented reporting systems, and the inability of conventional enforcement models to match the speed and scale of digitally coordinated criminal markets.

II. Conceptual and Theoretical Framework

The concept of cybercrime remains unsettled in law, policy, and scholarship. The United Nations *Manual on the Prevention and Control of Computer-Related Crime* noted that no internationally recognized definition of computer crime or computer-related crime had been established and that most formulations were functional and context-specific rather than universal (United Nations, 1994, p. 20). More recently, Phillips et al. argued that conceptual ambiguity still affects legal, policy, and academic responses because cybercrime legislation remains inconsistent across jurisdictions and the field lacks a stable shared lexicon (Phillips et al., 2022, pp. 379–380). Lusthaus, by contrast, proposed a deliberately concise definition, describing cybercrime as "crime that uses digital technology in a significant way" (Lusthaus, 2024, p. 369). Taken together, these positions suggest that cybercrime should be treated not as a fixed legal category but as a dynamic field shaped by technological change and institutional perspective.

This article narrows that wider field to **economic cybercrime**. The term is used here to refer to financially motivated offending committed through, against, or within digital systems and infrastructures in order to obtain illicit economic gain. An operational formulation appears in the U.S. Department of Justice's description of economic, cyber, and high-tech crimes as offences committed through networked computers, handheld devices, and Internet technology, including theft, identity abuse, account hijacking, infrastructure intrusions, and hacking (Justice, 2015, p. 4)A complementary law-enforcement perspective appears in INTERPOL's 2024 *Global Financial Fraud Assessment*, which conceptualizes financial fraud as an umbrella category of illegal activities aimed at financial gain through deceptive actions against individuals or entities (INTERPOL, 2024, p. 6) .

At the policy level, the European Commission defined cybercrime as criminal acts committed using electronic communications networks and information systems or against such systems, distinguishing among traditional crimes committed online, illegal online content, and offences unique to digital networks (Communities, 2007, p. 2) .

The theoretical framing is intentionally selective and functional. It relies on three explanatory lenses only. The first is **digital acceleration**, used to explain how the pandemic widened the attack surface by normalizing remote work, digital payments, e-commerce, and platform-mediated trust. The second is **financial convergence**, used to interpret the growing integration of fraud with laundering, fintech abuse, virtual assets, and cross-border payment systems. The third is **organizational industrialization**, used to explain the rise of scam centres, crime-as-a-service, modular criminal labor, and AI-assisted impersonation. These lenses are chosen because they directly serve the article's problem and recur consistently across the official sources used here (FATF, 2026, pp. 2–4; Europol, 2023a, pp. 3–4; INTERPOL, 2026, pp. 5–8).

Infrastructural criminology can be understood here as an analytical orientation that shifts attention from isolated offenders, discrete cyber incidents, or narrow legal categories toward the digital, financial, and institutional infrastructures that enable criminal activity to emerge, circulate, and scale. This perspective is particularly relevant to economic cybercrime because the phenomenon is not limited to technical intrusions or individual acts of deception. Since definitions of cybercrime remain conceptually unsettled and context-dependent, and since cybercrime may broadly be understood as crime that uses digital technology in a significant way, an infrastructural perspective helps explain how financially motivated offending becomes embedded within networked computers, internet technologies, payment systems, fintech platforms, virtual assets, and cross-border laundering channels (United Nations, 1994, p. 20; Phillips et al., 2022, pp. 379–380; Lusthaus, 2024, p. 369; Justice, 2015, p. 4; INTERPOL, 2024, p. 6; FATF, 2026, pp. 2–4). In this sense, infrastructural criminology

provides the broader analytical ground for examining how digital acceleration, financial convergence, and organizational industrialization transform cyber-enabled fraud from a set of online offences into a more structured criminal economy operating through the ordinary infrastructures of digital modernity (FATF, 2026, pp. 2–4; Europol, 2023a, pp. 3–4; INTERPOL, 2026, pp. 5–8).

On that basis, the article proposes the concept of **infrastructural criminality**. The term is not introduced as a grand theory, but as a focused interpretive device. It refers to a stage in which illicit profit extraction increasingly works **through** the ordinary infrastructures of digital modernity rather than simply targeting them from outside. Instant payments, remote onboarding, digital banking, virtual-asset systems, messaging applications, online marketplaces, and platform-based identity relations have become not merely targets of abuse but operating environments for criminal extraction and concealment. This is what distinguishes the current phase from earlier conceptions centered on isolated technical attacks or simple online scams.

III. Data Sources and Methodology

The article adopts a **longitudinal comparative documentary design** built on two layers of evidence. The first layer consists of official cybercrime and fraud reports:

IC3 annual reports for 2020–2025, INTERPOL's 2024 and 2026 financial fraud assessments, FATF's 2023 and 2026 fraud reports, and Europol's 2023–2024 strategic reports.

The second layer adds open institutional indicators that help explain why the criminal environment changed:

- ITU estimates of internet use, the World Bank's Global Findex 2025 on financial and digital inclusion, UNODC's official crime-data portal, and the UNODC Cybercrime Repository on legal and institutional responses.
- This second layer gives the article an explanatory dimension beyond trend description.

These sources are not treated as a perfectly harmonized global dataset:

- IC3 is a U.S.-centered reporting system;
- INTERPOL and Europol provide intelligence-led threat assessments;
- FATF foregrounds illicit-finance vulnerabilities and laundering typologies;
- ITU and Global Findex describe structural exposure and digital-financial inclusion rather than cybercrime directly;
- and UNODC offers official statistical series and legal-institutional repositories rather than a single comprehensive cybercrime incidence database.

The method therefore is comparative and interpretive rather than mechanically aggregative. Its purpose is to identify robust structural transformations across official open evidence, not to create an artificial single metric where none exists.

To improve analytical transparency, the documentary analysis followed three successive steps. **First,** the selected reports were screened according to their relevance to cyber-enabled economic crime, financial fraud, money laundering, virtual assets, digital exposure, and institutional response. **Second,** the evidence was organized chronologically into three analytical phases: 2020–2021, 2022–2023, and 2024–2026. **Third,** recurring patterns were compared across institutional sources in order to distinguish simple increases in reported incidents from deeper structural transformations. Particular attention was given to changes in complaint volume, financial losses, laundering mechanisms, criminal organization, technological enablers, and institutional response capacity. This procedure allowed the study to develop an interpretive synthesis grounded in official documentary evidence rather than relying on a single reporting system or a purely descriptive chronology.

IV. Empirical Analysis and Structural Interpretation of Global Economic Cybercrime Trends

a) Structural Exposure: Why the Post-COVID Environment Changed

Before turning to cybercrime and fraud counts, it is necessary to identify the broader structural conditions that widened the criminal opportunity space. ITU estimates that internet use rose from **60% of the world's population in 2020** to **74% in 2025**, meaning that about **1.3 billion additional people** came online during that period and that approximately **6 billion people** were internet users by 2025. In parallel, the World Bank's Global Findex 2025 reports that **79% of adults globally had an account** in 2024, up from 74% in 2021, and that the database covers nearly **145,000 adults in 141 economies**. These figures do not measure crime themselves, but they do measure the expansion of digital and financial exposure within which economic cybercrime could scale.

Table 1. Structural exposure indicators in the digital economy

Indicator	Earlier point	Later point	Source significance
Global internet users	60% of world population (2020)	74% (2025)	Expansion of digital exposure base
People using the internet	—	6.0 billion (2025)	Greater reach for scalable fraud
Adults globally with a financial account	74% (2021)	79% (2024)	Wider participation in digital-financial systems
Global Findex survey coverage	—	~145,000 adults in 141 economies	Robust official comparative coverage

Source: compiled from ITU official internet-use statistics and the World Bank's Global Findex 2025 materials.

Table 1 establishes the article's first explanatory claim:
the post-COVID surge in economic cybercrime unfolded within a materially expanded environment of connectivity, account ownership, and digitally mediated economic participation. These indicators do not establish direct causality between digital expansion and cybercrime growth. However, they suggest that the widening of digital and financial

participation created conditions under which economic cybercrime could become more scalable. This helps explain why a purely offender-centered or purely technical explanation remains insufficient.

b) Phase I: Pandemic Shock and the Expansion of Digital Exposure, 2020–2021

The first phase is best understood as one of **exposure expansion**. In 2020, the pandemic abruptly relocated work, shopping, payments, communication, and institutional interaction to digital environments. Official reporting shows that this widened the target base for fraud and amplified reliance on remote trust. UNODC warned that COVID-19 was increasing the risks of phishing, online fraud, extortion, and ransomware, while the early pandemic environment enabled fraudsters to exploit fear, urgency, and digital dependency (UNODC, 2020, pp. 1–3).

IC3 data show how sharply the pressure rose. In 2020, IC3 received **791,790 complaints** and reported losses exceeded **USD 4.2 billion**. In 2021, complaints increased to **847,376** and losses to **USD 6.9 billion**.

These figures matter not simply because they rose, but because they indicate how rapidly criminal adaptation followed the migration of work, commerce, payments, and communication into digital environments. The evidence suggests that the pandemic did not merely coincide with a rise in cyber-enabled fraud; it appears to have accelerated the expansion of the exposure base upon which a more organized fraud economy subsequently developed.

c) Phase II: Financial Convergence and the Laundering of Fraud, 2022–2023

The second phase can be interpreted as one of **financial convergence**. In 2022, IC3 registered **800,944 complaints** and losses of **USD 10.3 billion**. In 2023, complaints rose to **880,418** and losses exceeded **USD 12.5 billion**. The analytical significance of this phase lies in the widening gap between complaint counts and financial impact. Losses rose faster than complaint volume, suggesting a shift toward higher-value schemes, more effective targeting, and more advanced monetization structures.

FATF's 2023 joint report with INTERPOL and the Egmont Group provides the key interpretive link for this phase. It shows that cyber-enabled fraud is increasingly connected to money-laundering channels and wider criminal ecosystems and that the proceeds of fraud are moved through mule accounts, payment services, fintech channels, and virtual-asset mechanisms. FATF's 2026 paper deepens this conclusion by stating that growing numbers of fraud schemes integrate laundering from the outset, relying on nominee accounts, money mule networks, traded accounts, and rapid fund movement through fintech platforms (FATF, INTERPOL, & Egmont Group, 2023, pp. 3, 5–6; FATF, 2026, pp. 3–4). Economic cybercrime in this phase is therefore no longer adequately described as deception at the point of victimization; it must be analyzed through its circulation, concealment, and reinvestment logic.

d) Phase III: Industrialization, AI, and Organized Fraud Ecosystems, 2024–2026

The third phase is best understood as a process of **industrialization**. Europol's 2023 *Online Fraud Schemes* report states that online fraud represents a major crime threat in the EU and beyond and that the chain of crime has become increasingly business-like, facilitated by accessible enablers and cybercrime-as-a-service. Europol's broader 2023 financial-crime assessment adds that fraud actors range from opportunistic offenders to highly organized networks using specialized external service providers in banking, finance, law, IT, and money laundering. This points to a major structural shift: the offence is increasingly produced through coordination, outsourcing, and modular labor (Europol, 2023a, pp. 3–4; Europol, 2023b, p. 25).

The complaint-and-loss side of this transformation is equally striking. In 2024, IC3 recorded **859,532 complaints** and **USD 16.6 billion** in losses. In 2025, complaints climbed to **1,008,597** and losses to **USD 20.877 billion**. The 2025 report also identified **452,868 cyber-enabled fraud complaints** linked to **USD 17.697 billion** in losses, **181,565 cryptocurrency-linked complaints** tied to **USD 11.366 billion** in losses, and **22,364 AI-related complaints** involving **USD 893.3 million** in losses. These figures show that the contemporary phase is increasingly structured around digital assets, AI-

enabled manipulation, and scalable fraud architectures rather than only legacy forms of online deception.

INTERPOL's 2026 threat assessment supports the interpretation of global scale of this transformation. It reports that financial fraud is among the **top five global crime threats**, that fraud-related Notices and Diffusions increased by **54%** from 2024 to 2025, and that losses in 2025 were estimated at **USD 442 billion** globally. It also describes scam centres as a global threat affecting victims from nearly 80 countries and highlights the growing role of AI tools capable of cloning voices and faces from seconds of genuine media. This is why the present phase cannot be described merely as "more fraud." It is a phase in which technological automation, organizational specialization, and global collaboration have converged to transform the operating logic of criminal profit extraction.

e) Quantitative Synthesis of Global Economic Cybercrime Trends

Table 2. IC3 longitudinal trend, 2020–2025

Year	Complaints	Reported losses (USD)	Analytical signal
2020	791,790	4.2 bn	Pandemic shock and rapid digital exposure
2021	847,376	6.9 bn	Post-shock escalation
2022	800,944	10.3 bn	Losses accelerate faster than volume
2023	880,418	12.5 bn	Higher-value fraud becomes more central
2024	859,532	16.6 bn	Record losses despite moderate fluctuation in complaints
2025	1,008,597	20.877 bn	Full transition to highly monetized cyber-enabled fraud

Source: compiled from IC3 annual reports.

Across 2020–2025, IC3 recorded **5,188,657 complaints** and approximately **USD 71.377 billion** in reported losses. The critical point is not only the growth of complaints, but the increasingly steep rise in losses. Economic cybercrime became more effective at extracting and monetizing value even

where complaint volume fluctuated. That asymmetry is one of the strongest indicators that the period should be interpreted as structural transformation rather than simple expansion.

Table 3. Indicators of structural intensification

Year	Indicator	Official figure	Analytical meaning
2021	Cryptocurrency-related complaints	34,202	Early crypto expansion in fraud ecosystems
2021	Cryptocurrency-related losses	1.6 bn	Digital assets become a major monetization channel
2022	Investment fraud losses	3.31 bn	Investment fraud becomes the costliest scheme
2022	Crypto-investment fraud losses	2.57 bn	Stronger financialization of deception
2023	BEC losses	2.9 bn	Corporate-targeted fraud remains structurally important
2025	Cyber-enabled fraud complaints / losses	452,868 / 17.697 bn	Fraud becomes the dominant monetary component
2025	Crypto-linked complaints / losses	181,565/11.366 bn	Virtual assets deeply embedded in fraud economy
2025	AI-related complaints / losses	22,364/893.3 m	AI becomes a measurable criminal enabler

Source: compiled from IC3 reports 2021–2025

Table 3 reinforces the argument that the post-COVID period should not be reduced to generalized "online fraud growth." The stronger pattern is **structural intensification**: first through cryptocurrency-linked fraud, then through the centrality of investment fraud, and finally through measurable AI-assisted offending and the dominance of cyber-enabled fraud in overall losses. By 2025, cyber-enabled fraud accounted for **45% of all complaints** but **85% of all losses** reported to IC3, which indicates increasing concentration around highly scalable and high-yield forms of extraction.

Table 4. Institutional indicators beyond IC3

Institution / report	Indicator	Official finding	Analytical value
INTERPOL, 2026	Fraud-related Notices and Diffusions	+54% from 2024 to 2025	Accelerating transnational police visibility
INTERPOL, 2026	Estimated global financial fraud losses in 2025	USD 442 bn	Confirms global scale beyond national reporting systems
INTERPOL, 2026	Threat ranking	Financial fraud among top five global crime threats	Strategic elevation of fraud
FATF, 2026	Jurisdictions identifying fraud as a major ML risk	156 jurisdictions / 90% assessed	Confirms convergence of fraud and money laundering
Europol, 2023	Nature of online fraud	Business-like chain of crime enabled by accessible enablers and crime-as-a-service	Shows organizational industrialization
INTERPOL, 2025	Operation HAECHI VI asset recovery	USD 439 m recovered across 40 countries and territories	Shows scale of enforcement challenge

Source: INTERPOL, FATF, Europol, and INTERPOL operational reporting.

Table 4 prevents the analysis from being overly dependent on IC3. Once the U.S. reporting trend is read alongside INTERPOL, FATF, and Europol, the transformation becomes global in interpretive scope. INTERPOL frames financial fraud as a top-tier international threat; FATF shows that fraud is now widely recognized as a major money-laundering risk; and Europol describes online fraud as increasingly business-like and supported by service-based criminal ecosystems. Together, these indicators provide support for the article's core claim that the post-COVID phase is best interpreted as one of **infrastructural criminality**.

f) Institutional Capacity and the Governance Dimension

A further dimension of the contemporary problem is uneven institutional capacity. UNODC's official data portal confirms that the organization compiles global statistical series on crime and criminal justice from

member states, while the UNODC Cybercrime Repository serves as a central database of legislation, case law, and lessons learned on cybercrime and electronic evidence. These resources matter not because they provide a unified global cybercrime incidence series equivalent to IC3, but because they demonstrate that cybercrime governance is increasingly shaped by disparities in legal architecture, reporting capacity, and operational readiness. The global problem is therefore not only one of expanding offender capability but also one of uneven institutional synchronization.

This institutional perspective is analytically important because it explains why transnational criminal advantage can persist even where awareness of the threat is high. Fraud ecosystems exploit jurisdictional fragmentation by separating victim targeting, infrastructure, fund movement, and laundering functions across territories. FATF emphasizes the need for domestic and international partnerships, beneficial-ownership transparency, and AML tools tailored to fraud proceeds, while INTERPOL's operational reporting shows that large-scale international coordination is increasingly necessary merely to intercept a fraction of criminal assets. In this sense, economic cybercrime is also a governance problem: it grows where digital connectivity and financial speed outpace institutional coordination.

g) Interpreting the Structural Transformation

The evidence suggests four major conclusions:

First, the COVID-19 crisis appears to have widened the **exposure base** of economic cybercrime. Remote work, e-commerce, digital communication, and online payments did not merely create temporary opportunity; they normalized large-scale vulnerability under conditions of digital dependency.

Second, economic cybercrime became increasingly **financialized**. Fraud is now tied more visibly to laundering infrastructures, fintech services, nominee accounts, virtual assets, and rapid cross-border fund movement, which means the offence extends well beyond deception at the point of victimization.

Third, the period 2024–2026 marks a phase of **industrialization**, in which scam centres, AI-enhanced impersonation, and service-based

criminal markets lowered barriers to entry and increased the modularity and scalability of offending.

Fourth, the article's added data layer shows that these criminal changes unfolded in parallel with wider structural shifts in internet use and financial inclusion, while uneven institutional capacity complicated response.

What distinguishes this interpretation from more descriptive overview articles is that it does not treat these developments as parallel trends only. It reads them as parts of a single transformation. Once digital acceleration, financial convergence, criminal industrialization, and institutional unevenness are examined together, economic cybercrime appears less as a growing list of fraud types and more as a transnational criminal economy embedded in the infrastructures of digital life. That is precisely why the concept of **infrastructural criminality** is useful: it captures the shift from external attack to internal exploitation of ordinary digital systems.

V. CONCLUSION

From the COVID-19 crisis to 2026, official evidence suggests that economic cybercrime can be interpreted as having moved from crisis-amplified online victimization toward a more organized and financially embedded global criminal economy. The evidence converges around four main patterns: digital acceleration appears to have widened exposure; financial innovation created additional channels of monetization and concealment; service-based criminal ecosystems contributed to the industrialization of deception; and uneven institutional capacity left significant gaps in detection, coordination, and recovery.

The result is a form of transnational criminality that is not external to digital modernity but increasingly embedded within it. Economic cybercrime has therefore become more scalable, more financialized, more collaborative, and more deeply lodged in digital infrastructures than it was at the start of the pandemic.

The policy implication is clear. Economic cybercrime can no longer be treated as a secondary consumer-protection problem or as a narrow

technical subset of cybercrime. It requires integrated responses connecting cyber security, anti-money-laundering controls, payment-system safeguards, platform governance, international policing cooperation, digital-safety literacy, and stronger reporting and recovery mechanisms for victims. What emerged after COVID-19 is not merely more online fraud. It is a more adaptive and interconnected digital criminal economy.

VI. Bibliography List :

1. Akdemir, Sungur, & Başaranel. (2020). Examining The Challenges Of Policing Economic Cybercrime In The Uk. *Güvenlik Bilimleri Dergisi*, 113–134. Doi:Https://Doi.Org/10.28956/Gbd.695956
2. Albanese. (2022). A Typology Of Cybercrime: An Assessment Of Federal Prosecutions. (J. O. Law, Ed.) Retrieved From Https://Research.Library.Kutztown.Edu.
3. Bank, W. (2025). *The Global Findex Database 2025*. Retrieved From Https://Reproducibility.Worldbank.Org/Catalog/299.
4. Communities, C. O. (2007). *Towards A General Policy On The Fight Against Cyber Crime.* Commission Of The European Communities. Retrieved From Https://Eur-Lex.Europa.Eu/Lexuriserv/Lexuriserv.Do?Uri=Com%3a2007%3a0267%3afin%3aen%3apdf
5. Crime, U. N. (2020). *Cybercrime And Covid-19: Risks And Responses.* Retrieved From Https://Www.Unodc.Org/Documents/Advocacy-Section/Unodc_-_Cybercrime_And_Covid19_-_Risks_And_Responses_V1.2_-_14-04-2020_-_Cmls-Covid19-Cyber1_-_Unclassified_Branded.Pdf
6. Crime, U. N. (N.D.). *Cybercrime Repository*. Retrieved From United Nations Office On Drugs And Crime: Https://Www.Unodc.Org/Unodc/En/Cybercrime/Cybercrime-Repository.Html
7. Europe, C. O. (2001). *Convention On Cybercrime (Ets No. 185).* Budapest: Council Of Europe. Retrieved From Https://Rm.Coe.Int/1680081561
8. Europol. (2023). *European Financial And Economic Crime Threat Assessment 2023 - The Other Side Of The Coin: An Analysis Of Financial And Economic Crime* . Luxembourg.: Publications Office Of The European Union. Doi: 10.2813/105613
9. Europol. (2023). *Online Fraud Schemes: A Web Of Deceit.* Luxembourg: Publications Office Of The European Union. Doi:10.2813/543686

10. Europol. (2024). *Internet Organised Crime Threat Assessment (Iocta) 2024.* Luxembourg: European Union Agency For Law Enforcement Cooperation. Doi:10.2813/442713
11. Europol. (2025). *Eu Serious And Organised Crime Threat Assessment 2025: The Changing Dna Of Serious And Organised Crime.* Luxembourg: Publications Office Of The European Union. Doi:10.2813/0758057
12. Fatf. (2026). *Cyber-Enabled Fraud: Digitalisation And Money Laundering, Terrorist Financing And Proliferation Financing Risks.* Retrieved From Cyber-Enabled Fraud: Digitalisation And Money Laundering, Terrorist Financing And Proliferation Financing Risks: Https://Www.Fatf-Gafi.Org.
13. Fatf, Egmont Group, & Interpol. (2023). Retrieved From Illicit Financial Flows From Cyber-Enabled Fraud: Https://Www.Fatf-Gafi.Org.
14. Federal Bureau Of Investigation, I. C. (2020). *Internet Crime Report 2020.* Federal Bureau Of Investigation, Internet Crime Complaint Center. Retrieved From Https://Www.Ic3.Gov/Annualreport/Reports/2020_Ic3report.Pdf
15. Federal Bureau Of Investigation, I. C. (2021). *2021 Internet Crime Report.* Federal Bureau Of Investigation, Internet Crime Complaint Center. Retrieved From Https://Www.Ic3.Gov.
16. Federal Bureau Of Investigation, I. C. (2022). *2022 Internet Crime Report.* Federal Bureau Of Investigation, Internet Crime Complaint Center. Retrieved From Https://Www.Ic3.Gov.
17. Federal Bureau Of Investigation, I. C. (2023). *2023 Internet Crime Report.* Federal Bureau Of Investigation, Internet Crime Complaint Center. Retrieved From Https://Www.Ic3.Gov/Annualreport/Reports/2023_Ic3report.Pdf
18. Federal Bureau Of Investigation, I. C. (2024). *2024 Ic3 Annual Report.* Federal Bureau Of Investigation, Internet Crime Complaint Center. Retrieved From Https://Www.Ic3.Gov.
19. Federal Bureau Of Investigation, I. C. (2025). *2025 Ic3 Annual Report.* Federal Bureau Of Investigation, Internet Crime Complaint Center. Retrieved From Https://Www.Ic3.Gov.
20. Interpol. (2024). *Interpol Global Financial Fraud Assessment.* Interpol. Retrieved From Global Financial Fraud Assessment: Https://Www.Interpol.Int.
21. Interpol. (2025). *Usd 439 Million Recovered In Global Financial Crime Operation*. Retrieved From Https://Www.Interpol.Int/News-And-

Events/News/2025/Usd-439-Million-Recovered-In-Global-Financial-Crime-Operation

22. Interpol. (2026). *Interpol Report Warns Of Increasingly Sophisticated Global Financial Fraud Threat*. Retrieved From Https://Www.Interpol.Int/News-And-Events/News/2026/Interpol-Report-Warns-Of-Increasingly-Sophisticated-Global-Financial-Fraud-Threat
23. Justice, U. D. (2015). *Economic, Cyber, And High-Tech Crimes National Training And Technical Assistance Program Fy 2015 Competitive Grant Announcement.* U.S. Department Of Justice. Retrieved From Https://Bja.Ojp.Gov/Sites/G/Files/Xyckuh186/Files/Media/Document/Bja-2015-4158.Pdf
24. Levi, D. M., Alan , D., Rajeev , G., David , W., & Matthew, W. (2015). *The Implications Of Economic Cybercrime For Policing: Research Report.* London: City Of London. Retrieved From Https://Orca.Cardiff.Ac.Uk.
25. Lusthaus, J. (2024). *Reconsidering Crime And Technology: What Is This Thing We Call Cybercrime?* Annual Review. Retrieved From Https://Doi.Org/10.1146/Annurev-Lawsocsci-041822-044042
26. Mcguire, & Dowling. (2013). *Cyber Crime: A Review Of The Evidence Research Report 75.* Home Office Science. Retrieved From Https://Assets.Publishing.Service.Gov.Uk.
27. Nations, U. (1994). *Manual On The Prevention And Control Of Computer-Related Crime*. Retrieved From Https://Digitallibrary.Un.Org/Record/162804/Files/Manual_Computerrelatedcrime.Pdf
28. Phillips, K., Julia C. Davidson , Ruby R. Farr, & Christine Burkhardt. (2022). Conceptualizing Cybercrime: Definitions, Typologies And Taxonomies. *Forensic Sciences*. Doi:10.3390/Forensicsci2020028