JURNAL PARADIGMA HUKUM Pembangunan
ISSN: 2528-7486/ 2654-9298 Vol. 11 No. 1, Februari 2026

ORGANIZED TRANSNATIONAL CRIME IN THE DIGITAL ERA: ANALYSIS OF CYBERCRIME TRENDS AND HUMAN TRAFFICKING IN 2025–2026

Patrcia Swalika Irawan[1], Dwi Putri Lestarika[2]
Universitas Bengkulu, Bengkulu
Corresponding Author: ciapatricia42@gmail.com

ABSTRACT

This study analyzes the latest developments in international crime during the 2025–2026 period, focusing on cybercrime and human trafficking, which have become increasingly complex in the digital era. Using a descriptive qualitative approach, this research collects data from the Global Organized Crime Index 2025 report, Amnesty International reports, and various secondary sources related to transnational crime. The findings indicate that cybercrime has experienced a significant surge, with losses reaching US$10.5 trillion per year, while human trafficking has evolved with more sophisticated modus operandi utilizing artificial intelligence technology. The results reveal that organized crime groups are increasingly adapting to digital transformation by exploiting cybersecurity vulnerabilities and geopolitical uncertainties. The study concludes that the global response to transnational crime requires stronger multilateral cooperation and enhanced institutional capacity to address the growing dominance of non-violent crime threats. This research provides a theoretical contribution to understanding the dynamics of contemporary international crime and offers practical recommendations for policymakers in formulating strategies to combat transnational crime.

Keywords: Transnational Crime, Cybercrime, Human Trafficking, Organized Crime, Qualitative Method

INTRODUCTION

International crime has undergone a fundamental transformation over the past decade, particularly since the COVID-19 pandemic, which accelerated the digitalization of various aspects of human life. The 2025–2026 period marks a critical point at which transnational organized crime (TOC) groups increasingly exploit advanced technologies, especially artificial intelligence, to expand the scope of their illegal operations. According to an Ipsos survey in 2026, crime and violence have become the issues of greatest concern for the global community, with concern levels

reaching 32%.[1]

The Global Organized Crime Index 2025 records a significant shift in the global crime landscape, in which non-violent crimes such as financial crime and cybercrime have increased sharply. Unlike conventional crimes that rely on physical violence, these crimes operate within transnational financial and digital systems that are difficult to detect yet cause massive losses for individuals, businesses, and states. Losses due to cybercrime are estimated to reach US$10.5 trillion per year by 2025, indicating an annual growth rate of 15%.[2]

On the other hand, human trafficking continues to evolve with increasingly complex and organized methods. Reports by Amnesty International reveal large-scale human trafficking operations across more than 50 online scam compounds in Cambodia, involving slavery, torture, and forced labor against thousands of victims from various countries, including Indonesia. The United Nations General Assembly in November 2025 emphasized that human trafficking continues to expand by exploiting AI as a tool to recruit and transport victims, while conviction rates for perpetrators remain very low.[3]

The unstable global geopolitical context, marked by various armed conflicts and international tensions, creates opportunities that are exploited by transnational crime networks to expand their operations. Economic uncertainty, mass displacement, and weak law enforcement in conflict-affected regions act as catalysts for the growth of organized crime. In this situation, victims of international crime become increasingly vulnerable, particularly migrants, refugees, and communities in developing countries.

RESEARCH METHOD

This study employs a qualitative approach with a descriptive-analytical design to

[1] Sukarya, R. R., Anggraini, N., Cambara, H. K., Priyani, I. D., & Al Haddad, A. (2025). Statistik kejahatan siber di Indonesia tahun 2024: Tren, tantangan, dan upaya pencegahan di era digital. *iTech: Journal of Information Systems and Informatics, 1*(2), 1–10.

[2] Ismail, M. N. (2025). Pengaruh teknologi AI terhadap evolusi modus kejahatan siber di Indonesia tahun 2024–2025 dan implikasinya terhadap penegakan hukum. *Jurnal Intelek dan Cendikiawan Nusantara, 2*(1), 45–53.

[3] Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi penyidikan terhadap tindak pidana siber dalam perspektif perbandingan hukum: Indonesia dan Inggris Raya. *Jurnal Ilmiah Penegakan Hukum, 11*(2), 162–172.

ISSN: 2528-7486/ 2654-9298 Vol. 11 No. 1, Februari 2026

gain an in-depth understanding of contemporary transnational crime and to analyze its patterns, trends, and influencing factors. The data used consist of secondary data from credible sources, such as reports from international organizations (Global Organized Crime Index 2025, UNODC, Amnesty International, INTERPOL), academic publications, policy documents, mass media, and statistical data, selected based on credibility, relevance to the 2025–2026 period, and completeness of information, and validated through source triangulation. Data collection was conducted through a documentation study involving stages of identification, selection, extraction, and organization of data, while analysis employed content analysis techniques with a thematic approach through processes of coding, categorization, interpretation, and conclusion drawing. Reliability was maintained through systematic documentation and a clear conceptual framework. The limitations of this study include reliance on secondary data, rapidly changing data dynamics, methodological differences among sources, and the limited study period, which were addressed through triangulation and strict source selection.

RESULTS AND DISCUSSION

International Cybercrime Trends in 2025–2026

The analysis results indicate that cybercrime experienced a significant escalation during the 2025–2026 period, in terms of the volume of attacks, level of sophistication, and economic impact. Global losses due to cybercrime have reached US$10.5 trillion per year, increasing drastically from US$3 trillion in 2015. This annual growth rate of 15% makes cybercrime one of the largest economic threats in modern history, surpassing losses from the global drug trade.[4]

Characteristics of Cybercrime in 2025–2026

Ransomware attacks have evolved into highly organized operations targeting critical infrastructure using double and triple extortion techniques. Primary targets include the healthcare, government, and education sectors, with ransom demands reaching tens of millions of US dollars. The use of AI has created highly personalized and difficult-to-detect phishing threats, including the use of deepfake technology to deceive victims. Autonomous AI agents capable of operating independently have become a serious threat,

[4] Syahrir, M., & Saktiah. (2024). Efektivitas hukuman bagi pelaku kejahatan siber di Indonesia: Analisis kriminologi dengan metode content analysis. *Perkara: Jurnal Ilmu Hukum dan Politik, 3*(1), 1–12.

particularly for Indonesia, which is experiencing rapid digitalization but still has limited cybersecurity capacity.[5]

Supply chain attacks and the exploitation of IoT have increased significantly, taking advantage of vulnerabilities in devices that were not designed with adequate security standards. The cybercrime-as-a-service ecosystem is expanding on the dark web, offering criminal tools and services using cryptocurrency. Perpetrators can operate from countries with weak law enforcement to target victims globally, including the phenomenon of state-sponsored cybercrime for espionage and sabotage.[6]

Modus Operandi of Transnational Human Trafficking

Human trafficking during the 2025–2026 period exhibits increasingly complex characteristics, with the integration of digital technology at every stage of operations, from recruitment to the exploitation of victims. The United Nations General Assembly in November 2025 identified that AI is now being used as a "weapon" by human traffickers to recruit and transport victims in more efficient and harder-to-detect ways.[7]

Digitalization of Victim Recruitment

Social media platforms, dating applications, and job listing websites have become primary channels for recruiting victims through fraudulent advertisements promising high salaries. AI and machine learning are used to identify vulnerable individuals by analyzing social media data, targeting those experiencing economic hardship, social isolation, or a strong desire to migrate. The personalization of approaches based on psychological profiles has made recruitment tactics far more effective.

Cambodia Case: Convergence of Human Trafficking and Cybercrime

Amnesty International reports reveal large-scale human trafficking operations in

[5] Sejati, Y. D. C., & Nugroho, M. A. S. (2023). Upaya peningkatan kompetensi penyidik direktorat tindak pidana siber Bareskrim Polri dalam menangani kasus cyber crime. *Jurnal Riset Manajemen Akuntansi Indonesia, 1*(2), 380–408.

[6] Sugiyono, A. F., & Runturambi, A. J. S. (2023). Memerangi cybercrime dan tindak pidana perdagangan orang pekerja migran Indonesia non-prosedural ke Kamboja. *Jurnal Ilmiah Kajian Keimigrasian, 7*(1), 1–12.

[7] Hasri, H., Mashendra, M., Hayun, H., & Nisa, F. N. (2024). Kejahatan cybercrime dan penanggulangannya dalam kerangka sistem hukum nasional. *Indonesian Journal of Legality of Law, 7*(2), 120–130.

Cambodia involving more than 50 online scam compounds. Thousands of victims from Indonesia, Malaysia, Vietnam, Thailand, the Philippines, and other countries were trapped in conditions described by Amnesty International as "human trafficking, slavery, and torture." Victims were initially recruited with promises of legitimate jobs in sectors such as hospitality, customer service, or information technology, with attractive salaries.[8]

Upon arrival in Cambodia, victims are confined in heavily guarded compounds, their passports confiscated, and they are forced to work in online scam operations targeting victims across various countries. They are compelled to work 12–18 hours per day without pay, carrying out investment scams, romance scams, or phishing schemes to steal money from others. Those who refuse or fail to meet targets face physical torture, beatings, electric shocks, and various other forms of violence.

This case demonstrates a concerning convergence between two forms of transnational crime: human trafficking and cybercrime. Victims of human trafficking are forced to become perpetrators of cybercrime, creating a chain of double victimization. This complexity complicates law enforcement efforts, as it involves multiple jurisdictions and requires close international cooperation.[9]

Transnational Networks and the Involvement of Organized Crime

These large-scale human trafficking operations involve highly structured transnational organized crime networks. These networks include:

- Recruiters in countries of origin who identify and recruit potential victims
- Transportation facilitators who arrange cross-border travel for victims
- Scam compound operators who run operations in destination countries
- Service providers (guards, translators, trainers) who support the operations
- Local protectors who provide political or security protection
- Beneficiaries who manage and distribute the proceeds of the crimes

[8] Lahagu, F., Erma, Z., & Nasution, R. (2024). Law enforcement against cyber crime in the form of phishing according to law number 1 of 2023 concerning criminal code. *Fox Justi: Jurnal Ilmu Hukum, 5*(2), 85–95.

[9] Dinda, A. L. S. (2024). Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik dan Hukum, 2*(2), 69–77.

This complex organizational structure enables operations to run systematically and efficiently, with clear division of roles and layered security mechanisms. The involvement of local government officials, whether through corruption or collusion, further complicates efforts to rescue victims and enforce the law.

Impacts and Challenges in Victim Identification

Victims experience profound physical and psychological trauma, including PTSD, depression, and difficulties with reintegration due to social stigma. Victim identification remains a major challenge, as many are unaware of their status or are afraid to report their situation. INTERPOL's "Libertad IV" operation in July 2025 successfully identified 1,194 potential victims and led to the arrest of 153 suspects across 14 countries in Latin America and the Caribbean. Conviction rates for perpetrators remain extremely low, with fewer than 1 in 100 cases resulting in conviction, due to difficulties in evidence collection, limited law enforcement capacity, corruption, and the complexity of cross-border jurisdictions.

Driving Factors Behind the Transformation of Transnational Crime

Data analysis identifies several key factors driving the transformation of transnational crime during the 2025–2026 period:

Acceleration of Global Digitalization

The COVID-19 pandemic accelerated digitalization, creating greater dependence on digital infrastructure and expanding the attack surface for cybercriminals. Rapid digital transformation without adequate security considerations has created vulnerabilities that are exploited. The development of AI, IoT, blockchain, and 5G has opened new opportunities for crime, with the pace of technological innovation outstripping the adaptation of legal frameworks.[10]

Geopolitical Instability

Armed conflicts create governance vacuums and safe havens for criminal groups. Mass displacement generates vulnerable populations that are easily exploited.

[10] itanggang, A. S., Darmawan, F., & Saputra, D. (2024). Hukum siber dan penegakan hukum di Indonesia: Tantangan dan solusi memerangi kejahatan siber. *Jurnal Pendidikan dan Teknologi Indonesia, 4*(3), 79–83.

Geopolitical tensions hinder international cooperation in information sharing and the extradition of offenders.

Economic Inequality and the Evolution of Criminal Business Models

Economic inequality creates push factors for irregular migration and exploitation. Organized crime groups have adopted professional, diversified business models, operating multiple criminal enterprises. The crime-as-a-service model enables specialization and outsourcing, increasing the efficiency of criminal operations.

Weak Law Enforcement Capacity

Limited resources, technical expertise, and infrastructure make it difficult for developing countries to detect and prosecute offenders. Legal frameworks lag behind the evolution of criminal methods, as legislative processes are unable to keep pace with the speed of criminal innovation. Corruption provides protection for organized criminal operations and creates a culture of impunity.[11]

Responses and Challenges in International Cooperation

The complexity and transnational nature of contemporary crime require a globally coordinated response. Various international cooperation initiatives and mechanisms have been developed; however, their effectiveness still faces numerous structural and operational challenges.[12]

International Legal and Institutional Frameworks

The United Nations Convention against Transnational Organized Crime (UNTOC) and its protocols provide a global legal framework for international cooperation. This convention has been ratified by the majority of countries worldwide and serves as the basis for various forms of cooperation, including extradition, mutual legal assistance, and information sharing.[13]

[11] Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi penyidikan tindak pidana siber dalam perspektif perbandingan hukum. *Jurnal Ilmiah Penegakan Hukum, 11*(2), 162–172.

[12] Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., & Virgio, V. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan siber di Indonesia. *Innovative: Journal of Social Science Research, 3*(6), 1135–1145.

[13] Fathonah, N., & Yusuf, H. (2024). Pencegahan dan tantangan dalam memerangi tindak pidana siber. *Jurnal Intelek dan Cendikiawan Nusantara, 2*(2), 1–10.

For cybercrime, the Convention on Cybercrime (Budapest Convention) serves as the main international instrument, although not all countries are parties to it. This convention establishes minimum standards for national cybercrime legislation, investigative procedures, and mechanisms for international cooperation in cross-border cybercrime cases.

The United Nations Office on Drugs and Crime (UNODC) plays a central role in coordinating the global response to transnational crime, providing technical assistance to member states, and facilitating the exchange of best practices. INTERPOL provides a platform for operational cooperation between countries, including intelligence sharing, coordination of joint operations, and the issuance of red notices for international fugitives.

Multinational Operations and Cooperation Challenges

The INTERPOL "Libertad IV" operation in July 2025 across 14 Latin American countries successfully identified 1,194 victims and arrested 153 suspects. Joint operations against ransomware and botnets demonstrate the effectiveness of cooperation between law enforcement agencies, the private sector, and academia.

Structural challenges include differences in national legal systems, sovereignty issues in extradition, limited resources for complex investigations, differing political priorities, slower response times compared to the mobility of perpetrators, and a trust deficit caused by geopolitical tensions that hinder intelligence sharing. The private sector, particularly technology companies, plays an important role in threat intelligence sharing. Civil society organizations such as Amnesty International expose crimes that escape government oversight. Innovative approaches are being developed through AI and big data analytics, blockchain for transaction transparency, capacity-building programs, and flexible regional cooperation frameworks, as well as victim-centered approaches, although their adoption remains limited..[14]

[14] Lahagu, F., Erma, Z., & Nasution, R. (2024). Law enforcement against cyber crime in the form of phishing according to law number 1 of 2023 concerning criminal code. *Fox Justi: Jurnal Ilmu Hukum, 5*(2), 85–95

CONCLUSION

This study reveals that transnational crime during the 2025–2026 period has undergone a fundamental transformation characterized by the digitalization of operations, the use of advanced technologies such as artificial intelligence, and the convergence of multiple forms of crime. Cybercrime has increased dramatically, with losses reaching US$10.5 trillion per year, driven by increasingly sophisticated ransomware, AI-based phishing, and the exploitation of IoT infrastructure. Human trafficking has also evolved with more complex methods through digital platforms, even forcing victims to participate in cybercrime activities. This transformation is driven by post-pandemic digital acceleration, geopolitical instability, economic inequality, the professionalization of organized crime, and weak law enforcement capacity. Although international responses show progress through multinational cooperation and strengthened legal frameworks, their effectiveness remains limited due to differences in legal systems, resource constraints, and slower response times compared to the rapid evolution of crime, making the involvement of the private sector and civil society increasingly important.

Countering transnational crime requires a comprehensive approach, including strengthening law enforcement capacity, harmonizing regulations, enhancing adaptive multilateral cooperation, investing in cybersecurity, and protecting victims through a victim-centered approach. This study recommends improving real-time information sharing, enhancing the capacity of law enforcement personnel—particularly in digital forensics—developing adaptive regulations, strengthening regional mechanisms, and improving victim protection and reintegration. However, this research is limited by its reliance on secondary data and a restricted time scope. Future studies are recommended to conduct empirical research, evaluate policy effectiveness, perform cross-country comparative analyses, and undertake longitudinal studies to gain a more comprehensive understanding of transnational crime trends.

REFERENCES

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., & Virgio, V. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan

siber di Indonesia. *Innovative: Journal of Social Science Research, 3*(6), 1135–1145.

Dinda, A. L. S. (2024). Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik dan Hukum, 2*(2), 69–77.

Fathonah, N., & Yusuf, H. (2024). Pencegahan dan tantangan dalam memerangi tindak pidana siber. *Jurnal Intelek dan Cendikiawan Nusantara, 2*(2), 1–10.

Hasri, H., Mashendra, M., Hayun, H., & Nisa, F. N. (2024). Kejahatan cybercrime dan penanggulangannya dalam kerangka sistem hukum nasional. *Indonesian Journal of Legality of Law, 7*(2), 120–130.

Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi penyidikan terhadap tindak pidana siber dalam perspektif perbandingan hukum: Indonesia dan Inggris Raya. *Jurnal Ilmiah Penegakan Hukum, 11*(2), 162–172.

Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi penyidikan tindak pidana siber dalam perspektif perbandingan hukum. *Jurnal Ilmiah Penegakan Hukum, 11*(2), 162–172.

Ismail, M. N. (2025). Pengaruh teknologi AI terhadap evolusi modus kejahatan siber di Indonesia tahun 2024–2025 dan implikasinya terhadap penegakan hukum. *Jurnal Intelek dan Cendikiawan Nusantara, 2*(1), 45–53.

Lahagu, F., Erma, Z., & Nasution, R. (2024). Law enforcement against cyber crime in the form of phishing according to law number 1 of 2023 concerning criminal code. *Fox Justi: Jurnal Ilmu Hukum, 5*(2), 85–95.

Sejati, Y. D. C., & Nugroho, M. A. S. (2023). Upaya peningkatan kompetensi penyidik direktorat tindak pidana siber Bareskrim Polri dalam menangani kasus cyber crime. *Jurnal Riset Manajemen Akuntansi Indonesia, 1*(2), 380–408.

Sitanggang, A. S., Darmawan, F., & Saputra, D. (2024). Hukum siber dan penegakan hukum di Indonesia: Tantangan dan solusi memerangi kejahatan siber. *Jurnal Pendidikan dan Teknologi Indonesia, 4*(3), 79–83.

Sukarya, R. R., Anggraini, N., Cambara, H. K., Priyani, I. D., & Al Haddad, A. (2025). Statistik kejahatan siber di Indonesia tahun 2024: Tren, tantangan, dan upaya pencegahan di era digital. *iTech: Journal of Information Systems and Informatics, 1*(2), 1–10.

Sugiyono, A. F., & Runturambi, A. J. S. (2023). Memerangi cybercrime dan tindak

pidana perdagangan orang pekerja migran Indonesia non-prosedural ke Kamboja. *Jurnal Ilmiah Kajian Keimigrasian, 7*(1), 1–12.

Syahrir, M., & Saktiah. (2024). Efektivitas hukuman bagi pelaku kejahatan siber di Indonesia: Analisis kriminologi dengan metode content analysis. *Perkara: Jurnal Ilmu Hukum dan Politik, 3*(1), 1–12.