Jurnal Ilmiah Wahana Pendidikan, Oktober 2025, 11 (10.D), 47-55
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/13048
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Transnational Cybercrime: A Case Study of Indian Phone Scammers and Their Impact on International Security

Fannissa Melya Putri[1] , Flori Mardiani Lubis [2], Prilla Marsingga [3]

[1,2,3]Universitas Singaperbangsa Karawang

Received: 05 September 2025
Revised: 17 September 2025
Accepted: 28 September 2025

Abstract

The rapid advancement of information and communication technology has given rise to increasingly sophisticated cybercrimes, one of which is transnational phone scams. This paper explores the emergence and operation of scam call centers, particularly those based in India, which target individuals in countries such as the United States, United Kingdom, and Canada. These scams not only result in significant financial losses but also undermine public trust in digital communication systems. Through a multidisciplinary analysis incorporating criminological theory and international cybercrime frameworks, this paper examines the structural, technological, and socio-economic factors enabling the persistence of such crimes. Furthermore, it proposes a set of policy implications, including the enhancement of international cooperation, regulatory reforms on data protection, public awareness initiatives, and improvements in law enforcement capacity. By addressing the issue from both global and local perspectives, this study aims to contribute to a more integrated and effective response to cyber-enabled fraud. The findings highlight the urgent need for transnational policy harmonization and collaborative enforcement mechanisms to counter the evolving threat of global phone scam operations.

Keywords: Transnational Cybercrime, Phone Scams, Scam Call Centers, Cybersecurity Policy, International Cooperation, Data Protection

(*) Corresponding Author:

How to Cite: Putri, F., Lubis, F., & Marsingga, P. (2025). Transnational Cybercrime: A Case Study of Indian Phone Scammers and Their Impact on International Security. *Jurnal Ilmiah Wahana Pendidikan*, *11*(10.D), 47-55. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/13048.

INTRODUCTION

The rapid development of information and communication technology in the era of globalization has brought significant changes to how people interact, conduct business, and manage daily activities. Expanding digital connectivity has made the world more interconnected, allowing cross-border interactions to occur in seconds. However, behind this convenience lies the emergence of new threats, particularly transnational cybercrime. These crimes transcend national borders and are often difficult to trace, as perpetrators can operate from locations far from their victims (Castells, 2010).

One of the most prominent forms of transnational cybercrime in recent years is phone scamming, which has been largely conducted by organized networks based in India. The perpetrators often pose as officials from tax agencies, immigration offices, banks, or major technology companies. Using psychological pressure and verbal manipulation, they convince victims—mostly citizens from developed countries such as the United States, Canada, the United Kingdom, and Australia—

to reveal sensitive information or transfer money under false pretenses (FBI IC3 Report, 2022).

These fraudulent operations are typically carried out through illegal call centers based in major Indian cities such as Delhi and Mumbai. These centers operate in a highly structured manner, with organized work shifts, clear task distribution, and even employee training on how to imitate foreign accents and follow pre-written scripts. Many of these call centers present themselves as legitimate businesses, while in reality, their entire operation is devoted to global criminal activity (BBC News, 2021).

This phenomenon highlights that cybercrime is no longer a purely technical issue—it has become a serious matter in the field of international relations. When a country serves as a base for criminal networks that target citizens of other nations, it not only creates diplomatic tensions but also undermines global cybersecurity and the credibility of legal systems. A lack of decisive action against such networks may lead to distrust and strained international relations (Wall, 2010).

Far from being a matter of individual financial fraud, these scams threaten international stability by touching on strategic concerns such as data security, cross-border financial flows, and the effectiveness of international law enforcement cooperation. Organizations such as INTERPOL and the United Nations Office on Drugs and Crime (UNODC) have emphasized the need for joint responses to such threats. However, challenges such as differing legal systems, limited extradition agreements, and technical barriers continue to obstruct progress (UNODC, 2023).

In this context, it becomes essential to understand how these scam networks operate, what long-term impacts they have on inter-state relations, and how the international community can respond effectively to increasingly sophisticated cyber threats. This study seeks to explore these issues by focusing on the dynamics of international security in addressing cybercrime committed by non-state actors on a global scale.

METHODS

This study utilizes a qualitative research approach with a case study design, focusing on phone scam operations originating in India that target individuals in countries such as the United States, the United Kingdom, Canada, and Australia. The qualitative approach allows for an in-depth exploration of the motives, patterns, and consequences of transnational cybercrime, particularly when understanding is needed beyond numerical data (Creswell, 2014).

The case study method is selected due to its strength in examining contemporary phenomena within real-life contexts, especially when the boundaries between the phenomenon and the context are not clearly evident (Yin, 2009). The Indian phone scam networks represent a specific and relevant case to study the wider implications of cybercrime on international security.

Data collection is conducted through documentary research, involving both primary and secondary sources. Primary data includes reports and public advisories from the FBI's Internet Crime Complaint Center (IC3), INTERPOL briefings, and official documents from the United Nations Office on Drugs and Crime (UNODC) related to cybercrime and organized crime (FBI IC3, 2022). Secondary data is

gathered from peer-reviewed academic journals, media investigations, and policy analyses published by cybersecurity research institutions (Europol, 2021).

For data analysis, the research employs descriptive-analytical techniques, enabling the identification of recurring patterns, actor networks, and inter-state responses to cyber threats. This method supports the development of grounded interpretations about how such scams are structured and the international legal and political responses to them (Neuman, 2011).

Additionally, the study is framed within the perspective of international security and transnational crime theory, emphasizing the role of non-state actors in undermining state sovereignty and the traditional framework of international cooperation (Bigo, 2002). By adopting this lens, the research seeks to understand not only the technical dimensions of cyber fraud but also its broader consequences for international relations and collective security efforts.

RESULTS & DISCUSSION

1. Modus Operandi and Organizational Structure of Indian Phone Scammers

The network of phone scammers operating in India has developed into a highly organized structure, akin to a profitable criminal industry. These networks operate in large groups, with a system that resembles professional corporations. Each member of this network has specific roles within a well-programmed process for committing fraud. The perpetrators typically work in **illegal call centers** equipped with advanced communication tools and systems that allow them to make thousands of calls each day.

Their **modus operandi** begins with a highly planned victim selection process. Scammers use personal information obtained from various sources, such as data leaks in the digital space, identity theft, or even information acquired from previous scams. With this data, they tailor their messages to appear more convincing and create a sense of urgency. For example, victims who work in tax or financial sectors are more likely to be influenced when contacted by a "tax officer" claiming there is an issue with their tax payment.

To enhance their credibility, scammers employ various **psychological techniques**. They often threaten victims with severe consequences if they do not immediately comply, such as claiming that the victim will face hefty fines or even jail time if they do not pay a specified amount. Some scammers even use technology to spoof phone numbers, making it appear as though they are calling from legitimate institutions or authorities (FBI IC3, 2022).

The organizational structure within these networks is highly efficient. They have **multiple levels of tasks**, ranging from **callers** who directly interact with victims, to **fund managers** responsible for receiving money from victims and transferring it to designated accounts. There are also individuals responsible for **logistics** and **documenting transactions**, as well as those handling relationships with international networks, for example, moving money through untraceable channels (Europol, 2021).

This flexible system allows the network to adapt to market changes or newer fraudulent methods. In some cases, they even recruit **trained personnel** to deal with various types of victim resistance, offering different scenarios or pressure tactics to

ensure victims remain fearful or pressured into providing sensitive information or money.

2. Impact on International Security

The crimes committed by these phone scammers do not only affect individual victims but also have broader implications for international security and relations between countries. These scams result in significant financial losses for thousands of victims every year. According to the FBI IC3 report, the losses from such scams can reach billions of dollars annually, with most of the victims coming from developed countries, which are the primary targets of these scam networks (FBI IC3, 2022).

However, the worst impact of these crimes is not just financial losses, but also the loss of trust in legal systems and international relations. The country where these scam networks operate—in this case, India—often faces criticism for failing to address illegal activities that threaten global economic stability and international security. This can cause diplomatic tensions between the countries where the victims reside and the country where the perpetrators operate (Wall, 2010).

Additionally, these crimes affect the stability of the global financial system. Since phone scammers often use hard-to-trace payment methods such as international money transfers, cryptocurrency, or informal money transfer systems, they create loopholes in the global financial system that can be exploited by other criminal networks, such as money laundering and terrorism financing. This activity makes the global financial sector increasingly vulnerable to abuse, which ultimately undermines trust in the banking system and international transactions (UNODC, 2023).

3. International Response to Phone Scammer Crimes

To address this issue, international organizations such as INTERPOL and UNODC have taken several important steps. One of the key approaches has been through increasing global awareness of the techniques used by scammers and spreading information to the public to prevent fraud. For example, INTERPOL has issued warnings about phone scams originating from India and has educated the public on how to recognize suspicious calls (INTERPOL, 2021).

Moreover, these organizations have strengthened international cooperation by coordinating between victim countries and the countries where the scam networks operate. On the other hand, many countries have begun introducing new regulations focused on data protection and digital transaction security to prevent such fraud in the future. For example, the European Union has enacted stricter regulations on data privacy in an effort to limit the abuse of personal information in frauds (Europol, 2021).

However, despite these efforts, technical barriers and jurisdictional challenges remain significant obstacles in tackling this crime. One of the major issues is that international law is often not clear or strong enough to provide a solid legal foundation for prosecuting perpetrators operating outside their home countries. Additionally, differences in legal systems between countries also pose a barrier, especially when fraudsters use technology to avoid enforcement and protect their identities (UNODC, 2023).

Some successes have been achieved in combating this crime, including the closure of several illegal call centers operating in India, thanks to cooperation

between Indian authorities and victim countries such as the United States and the United Kingdom. Furthermore, increased technical cooperation and information sharing among countries has helped narrow down the scammers' operational space, although significant challenges still exist.

4. Policy Implications

Phone scams perpetrated by Indian-based scam networks have far-reaching impacts, not only on the individuals who fall victim but also on the economic, social, and diplomatic stability of the countries involved. Therefore, concrete efforts in the form of policies are needed to more effectively address this crime. The following policy implications outline several steps that governments and international organizations should take to mitigate the threat posed by transnational cybercrime like phone scammers.

a. Strengthening International Cooperation

To tackle transnational crimes involving phone scammers, countries need to enhance international cooperation in law enforcement. Countries that are targets of these scams, along with the countries where the perpetrators operate, must strengthen diplomatic and legal relations through extradition agreements and law enforcement collaboration. Countries such as India must commit more strongly to combating cybercrime by involving international authorities like INTERPOL and UNODC. Additionally, increasing information sharing and law enforcement technology among nations can expedite the detection and cessation of these illegal activities (Bigo, 2002).

b. Reforming Cybersecurity Regulations and Personal Data Protection

One critical step is reforming regulations in the fields of cybersecurity and personal data protection. Countries need to introduce and tighten regulations that govern the use of personal data, ensuring that technologies used for online transactions are equipped with stronger security systems to protect citizens from fraud. For example, by adopting regulations similar to the GDPR (General Data Protection Regulation) in the European Union, countries can more strictly regulate how personal data is collected, used, and protected. Such policies can close the loopholes that fraudsters use to obtain personal information, which is then exploited in fraudulent activities (Europol, 2021).

c. Enhancing Public Education and Awareness

It is crucial to enhance public education on the potential threats of phone scams and how to avoid them. Governments and international organizations can collaborate to educate the public on the most common fraud tactics and how to recognize suspicious calls or communications. Additionally, there should be wider cyber-awareness campaigns, especially in countries that are major targets, such as the United States, Canada, and the United Kingdom. By increasing public knowledge on how to protect themselves, it is hoped that the number of victims from this crime will decrease.

d. Upgrading Technology and Strengthening Law Enforcement Capacity

Increasing law enforcement capacity in the countries where the scammers operate is also vital. This includes upgrading technological infrastructure and providing training for law enforcement officers to recognize and handle increasingly complex cybercrimes. For instance, authorities need access to technology that enables them to track and analyze suspicious digital

communications and online transactions. Moreover, countries should strengthen collaboration with the private sector, particularly telecom companies and internet service providers, to block phone numbers or websites used by scammers to carry out their schemes (FBI IC3, 2022).

e. Closing Financial Channels Used by Scammers

The success of phone scammers heavily relies on their ability to transfer the money obtained from victims through hard-to-trace methods. One policy measure that can be taken is to tighten oversight on international payment channels commonly used by scammers, such as bank transfers, cryptocurrency, or informal payment systems. Governments need to introduce stricter policies on digital payment service providers, including the reporting of suspicious transactions, as well as monitoring the use of platforms like cryptocurrency, which are often exploited to conduct illicit transactions.

f. Enhancing Cross-Sector Coordination

A more holistic policy approach should involve various sectors that can contribute to addressing this crime, including the legal, digital security, education, and financial sectors. Countries should develop better coordination mechanisms between government agencies, international organizations, and the private sector to create a safer ecosystem for citizens from cybercrime threats. Additionally, authorities should introduce incentives for the private sector to help monitor and prevent these crimes, such as telecom providers who are involved in restricting access to numbers used by scammers.

CONCLUSION

The proliferation of phone scams originating from India, particularly those involving elaborate transnational networks of scammers, has emerged as one of the most pervasive and complex forms of cybercrime in recent years. These scams, often orchestrated by highly organized criminal groups, have caused immense financial damage to individuals and have shaken the trust between nations and their digital systems. The scale and sophistication of these fraudulent activities highlight the evolving nature of cybercrime and the pressing need for comprehensive, multi-faceted responses at both the national and international levels.

This study underscores that phone scams are not merely criminal incidents affecting isolated individuals; they represent a significant threat to global economic stability, international relations, and the integrity of digital infrastructures worldwide. The targeted approach employed by scammers, which combines psychological manipulation, technological exploitation, and the abuse of international financial systems, has proven to be highly effective in exploiting vulnerabilities within both individual lives and national security systems. These activities contribute to broader concerns regarding the abuse of digital platforms, online security, and the functioning of international financial markets.

Addressing this challenge requires a multi-dimensional approach that tackles both the immediate effects of these scams and the underlying factors that enable their perpetuation. The international community must recognize that combating phone scams is not a task for individual nations to undertake alone. Instead, it requires coordinated global efforts, shared intelligence, and collaborative strategies to disrupt these criminal networks. This is especially critical because the

transnational nature of phone scams means that perpetrators often operate from jurisdictions where enforcement mechanisms are either insufficient or non-existent, making it difficult to hold them accountable.

One of the most pressing issues highlighted by this research is the need for strengthened international cooperation in law enforcement. The existence of cybercrime networks that operate across borders requires enhanced collaboration between national law enforcement agencies, international organizations such as INTERPOL and the UNODC, and private sector actors, especially those in the telecommunications, banking, and cybersecurity industries. Through coordinated actions, countries can ensure that criminals are pursued across jurisdictions and that the financial transactions related to these crimes are more easily traced and blocked.

At the same time, reforms to national and international regulatory frameworks must be prioritized to close the existing gaps that allow these scams to thrive. The regulation of data privacy and security in online transactions needs to be more robust. For instance, adopting policies similar to the EU's General Data Protection Regulation (GDPR) could be one step toward tightening the control over personal data, preventing its exploitation by scammers. Additionally, updating laws surrounding digital payments and financial transactions is crucial in ensuring that criminals cannot easily bypass the regulatory systems that are currently in place. Strengthening anti-money laundering (AML) and combating the financing of terrorism (CFT) frameworks should also be a part of the global response to these types of crimes, as scammers often use difficult-to-trace payment methods like cryptocurrencies and informal money transfer channels to move illicit funds.

Public education is another key component of an effective strategy to combat phone scams. Increasing public awareness about the risks of phone scams and providing guidance on how to recognize fraudulent calls are essential. Governments, alongside international organizations, must invest in education campaigns that inform citizens about the methods commonly used by scammers and provide practical steps for protecting themselves from becoming victims. Such initiatives should target the most vulnerable populations, such as elderly individuals who may be less familiar with digital technologies and more susceptible to manipulation.

The private sector also plays a crucial role in this battle against cybercrime. Telecommunication companies and internet service providers must strengthen their protocols to identify and block fraudulent numbers, monitor suspicious activity, and collaborate with law enforcement agencies to ensure that these actions are effective. Additionally, financial institutions and digital payment providers should work more closely with regulators to implement advanced fraud detection systems and establish more secure channels for international transactions. By doing so, they will not only prevent scammers from exploiting the financial system but also protect their customers from the financial consequences of these scams.

Moreover, technological advancements must be leveraged to enhance the capacity of law enforcement agencies to detect and track the activities of phone scammers. The adoption of AI-driven fraud detection tools, for example, could allow authorities to spot patterns of behavior that indicate fraudulent activity in real-time, allowing for more rapid intervention. In addition, enhanced cyber forensic

capabilities will enable investigators to trace the digital footprints left by scammers, making it easier to gather evidence and bring perpetrators to justice.

Equally important is the role of financial intelligence units (FIUs) and cybersecurity task forces, which should be empowered and equipped to respond swiftly to emerging threats. Governments should ensure that these agencies have access to the necessary resources and technology to effectively track financial transactions, identify suspicious patterns, and take immediate action to prevent the laundering of illicit funds.

One of the critical elements for long-term success in combating these types of cybercrimes lies in creating a legal environment that supports rapid enforcement of actions across borders. Efforts to harmonize cybercrime laws between countries are essential. The existence of clear legal standards that define what constitutes a cybercrime and provide uniform procedures for handling such cases would enable more effective cooperation between law enforcement agencies worldwide.

Ultimately, the fight against phone scams requires a collaborative, all-encompassing approach that integrates the efforts of governments, international organizations, the private sector, and civil society. Only through sustained international cooperation, legislative reform, and technological innovation can the global community hope to limit the operations of these transnational criminal networks. This proactive approach will not only help protect vulnerable populations from the devastating consequences of phone scams but also reinforce the resilience of global digital infrastructures and maintain trust in international financial systems.

As such, governments must recognize that the task of countering phone scams extends beyond national borders and requires a collective effort. Failure to act decisively and swiftly could result in the continued proliferation of these crimes, further destabilizing the financial systems, eroding trust in digital services, and undermining the social contract between citizens and their governments. It is imperative that comprehensive, well-coordinated policies are implemented at all levels to address this growing threat, ensure the safety of citizens, and safeguard the future of international digital economies.

CONFLICT OF INTEREST

Concerning the research, authorship, and publication of this paper, the author(s) reported no potential conflicts of interest.

ACKNOWLEDGEMENT

I would like to express our gratitude to Mrs. Flori Mardiani Lubis, S.IP., M.E, and Prilla Marsingga, S.Sos., M.I.Pol. for their contributions as specialists to this study.

REFERENCES

BBC News. (2022, November 14). *Inside India's fake call centre scams*. https://www.bbc.com/news/world-asia-india-63538809

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives: Global, Local, Political, 27*(1_suppl), 63–92. https://doi.org/10.1177/03043754020270S105

Economic Times. (2023, March 17). *Scam call centres busted in Delhi, Mumbai: Dozens arrested*. https://economictimes.indiatimes.com

Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu

Federal Bureau of Investigation Internet Crime Complaint Center (FBI IC3). (2022). *Internet Crime Report 2022*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Financial Action Task Force (FATF). (2022). *Virtual assets and money laundering risks*. FATF/OECD. https://www.fatf-gafi.org

Ghosh, S., & Tiwari, D. (2021). Cybercrime in India: A growing challenge. *Journal of Cyber Policy, 6*(2), 215–233. https://doi.org/10.1080/23738871.2021.1938470

INTERPOL. (2021). *INTERPOL alerts on global phone scam trends*. https://www.interpol.int/en/News-and-Events/News/2021/Phone-scam-alert

Kapoor, R., & Sinha, M. (2020). The emergence of call center scams in India: A socio-economic perspective. *Indian Journal of Criminology, 48*(1), 57–72.

Ministry of Home Affairs, Government of India. (2022). *Annual report on cybersecurity and law enforcement*. New Delhi: MHA Publications.

Saini, H. S., Rao, Y. V. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications (IJERA), 2*(2), 202–209.

The Guardian. (2021, August 23). *Indian police raid call centres over phone scams targeting foreigners*. https://www.theguardian.com/world/2021/aug/23/india-phone-scams-foreigners-police-raid

United Nations. (2022). *Promoting international cooperation in combatting cybercrime: Report of the Secretary-General*. https://www.un.org

United Nations Office on Drugs and Crime (UNODC). (2023). *Cybercrime and international cooperation: Challenges and responses*. https://www.unodc.org

Wall, D. S. (2010). Criminology and the "new" crimes of the internet. In D. S. Wall (Ed.), *Crime and deviance in cyberspace* (pp. 5–27). London: Routledge.