Defending Cyberspace
India–US Joint Efforts Against Cybercrime

Rohit Kumar Sharma*

This article examines the evolving landscape of cybercrime and emphasises the essential role of international cooperation, particularly between India and the United States (US). Considering the significant economic and national security repercussions of cyber threats such as ransomware attacks, effectively addressing cybercrime requires coordinated, dedicated and concerted efforts from all nations. India and the US are actively engaged in both bilateral and multilateral forums to adequately tackle the diverse and evolving challenges of cybercrime. Despite some limitations in specific areas of cooperation, both countries have remained committed to responding to cybercrime with robust domestic measures and a coordinated global approach to counter criminal syndicates.

Keywords: *Cybercrime, India–US Cybercrime Cooperation, Ransomware, Tech Support Fraud*

Introduction

In early 2024, there were several reports on INTERPOL-supported joint law enforcement operations targeting infrastructure that facilitate cyber threats, ranging from phishing and ransomware to tech support fraud.[1] In India, the

* Mr Rohit Kumar Sharma is a Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi.

ISSN 0976-1004 (print); 2583-7567 (online)

Central Bureau of Investigation (CBI) announced the launch of Operation Chakra-II in October 2023, aimed at dismantling organised cyber-enabled financial crimes through a series of crackdowns at approximately 76 locations across the country.[2] This operation was reportedly supported by a joint referral from major tech companies such as Microsoft and Amazon, specifically targeting tech support fraud directed at their customers.[3] These instances highlight a burgeoning global cybercrime system possessing transnational characteristics. It also exemplifies the fundamental nature of cyber threats, or in this case, cybercrime, which renders sovereign borders obsolete and necessitates cooperation between different states and jurisdictions.

According to estimates, cybercrime will cost the world US$ 10.5 trillion annually by 2025.[4] The implications are not merely economic; they also encompass social, psychological and national security threats. The propensity of threat actors or cybercriminals to target critical infrastructure, such as hospitals and electricity grids, both for financial gain and/or on behalf of other states, makes cybercrime an issue intertwined with national security imperatives.[5] The nationwide Conti ransomware attacks against Costa Rica's public and private sectors, and the country's subsequent declaration of a state of emergency demonstrate the level of threats emanating from the cybercrime ecosystem.[6] The elevation of cybercrime as a national security threat also underscores the technological advancements of threat actors that constitute part of the criminal ecosystem.

Both India and the US have long been targets of cybercriminals. For instance, between January and April 2024, Indian citizens suffered losses exceeding Rs 1,750 crores due to cybercriminal activities, as reported through over 7,40,000 complaints lodged on the National Cybercrime Reporting Portal during the period.[7] On the other hand, in the US, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) registered around 8,80,418 complaints in 2023, with potential losses exceeding US$ 12.5 billion.[8] Interestingly, both countries have also emerged as global hotspots of cybercrime, according to the 'world's first cybercrime index'.[9] The index, which details the geography of cybercrime, features India and the US in the list of top ten hubs of cybercriminal activity. The report underscores a source of concern for law enforcement agencies in India and the US and warrants attention.

India and the US have been cooperating for years in the field of law enforcement through existing avenues such as INTERPOL and Mutual Legal Assistance Treaties (MLATs).[10] Over the years, both countries have also sought to expand cooperation in cybersecurity, culminating in the signing of

the Framework for the US-India Cyber Relationship, which covers aspects such as cooperation on critical infrastructure, cybercrime and malicious actors in cyberspace. However, in response to emerging threats in cyberspace, where cybercriminals increasingly target critical infrastructure such as hospitals and financial institutions, thereby elevating threats to national security, existing collaborative mechanisms appear to be insufficient.

Against this backdrop, this article intends to examine India–US cooperation on cybercrime over the years, both bilaterally and at multilateral forums. In doing so, it will explore India–US collaboration on emerging cybercrime ecosystems, such as ransomware and tech support fraud, and elucidate the domestic responses of both the countries to cybercrimes. Finally, the article will appraise the prospects for future relations between India and the US in addressing the issue of cybercrime. Before that, it is crucial to define what constitutes cybercrime, as there is often no single, universally accepted definition of the term.

Defining Cybercrime

Although scholars have been attempting to define cybercrime for years, to date, there is no single, universally accepted definition of the term. The deliberations on establishing semantic boundaries are an ongoing debate in both academic circles and intergovernmental organisations, which have been contemplating the definition and characterisation of acts that constitute cybercrimes. This section attempts to inform the readers about the existing debates on determining the definition and typologies of cybercrime.

First, it is important to establish the need for a definition and draw clear boundaries of what constitutes cybercrime. In discussing the necessity of defining cybercrime, Brian K. Payne outlines seven overlapping reasons for doing so. Defining cybercrime influence estimates of its prevalence and extent, affect the consequences assigned to specific behaviours, and shape the approaches criminologists use to examine and explain cyber offences.[11] Furthermore, it guides the development of intervention strategies to prevent certain behaviours, informs the methodologies used to study these behaviours, and influences how academics teach about such behaviours.[12] Clearly, establishing the boundaries of cybercrime is significant, as it influences a wide range of responses, from policy-making to the training of law enforcement personnels.

Payne delves further into the intrinsic challenges of defining cybercrime due to its atypical nature, the breadth of cyberspace, and the multidisciplinary

aspects of cybercrime.[13] He also highlights how the term 'cybercrime' is the latest rendition to describe criminal activities in cyberspace, which has replaced terminologies such as digital crime, electronic crime, internet crime and computer crime. The old generations of scholars and organisations preferred the term 'computer crime' over 'cybercrime' to describe certain malicious behaviour in cyberspace.[14] However, acts that qualify as cybercrime are constantly evolving, reflecting the technological advancements of their time. Each epoch of technological advancement introduces new types of cybercrime. For instance, during the 'Third Industrial Revolution', technological advancements such as microprocessors, the Internet and computer transistors led to the emergence of hacking, malware, cyber theft and other related crimes.[15] Similarly, the 'Fourth Industrial Revolution' is characterised by technologically sophisticated forms of cybercrime, such as ransomware attacks demanding Bitcoin, the use of deepfake technologies, and other advanced methods. Amidst the changing nature of malicious threats in the digital realm, scholars have made attempts to offer definitions and, in some cases, conceptual frameworks or categorisations to achieve precise understanding and accounting for the range of cybercrimes.

Gordon and Ford define cybercrime as 'any crime that is facilitated or committed using a computer, network, or hardware device'.[16] By this definition, cybercrime can occur across a broad spectrum, with a computer or any other device serving as the agent, facilitator, or target of the crime. To offer a clear conceptual grasp, Gordon and Ford further introduce a two-factor classification system—Type I and Type II cybercrimes—that represent the opposite ends of the cybercrime spectrum. What distinguishes Type I from Type II cybercrimes is the extent to which the crime relies on technology for its commission. Type I cybercrimes are entirely technological, while Type II is considered to involve more human elements.[17] For instance, Type I cybercrimes cover technical aspects such as developing malicious software (malware), for instance, to gain unauthorised access to the victim's personal information. In contrast, Type II cybercrimes include activities such as online gambling, cyberstalking and harassment. In the first case, specialised software is designed for malicious purposes, whereas in the second, existing legitimate software and applications (any social media platform, email, or browser) are misused to commit a crime.

Another way of comprehending cybercrime is to understand it as 'an umbrella term used to describe two distinct but closely related criminal activities: cyber-dependent and cyber-enabled crimes'.[18]As the name suggests, cyber-dependent crimes are offences that can only be committed through

or that entirely rely on computer, computer networks, or other form of Information and Communication Technology (ICT).[19] Cyber-enabled crimes are traditional crimes that are facilitated by the use of ICT, allowing them to expand their reach and impact. There appears to be a general consensus between the two approaches mentioned above regarding the identification of the two key factors, specifically the extent to which technology is integral to the commission of the crime and what the defining characteristics should be.[20]

Another categorisation that gained traction among scholars was the three-category classification: crimes against the machine, crimes using the machine, and crimes in the machine.[21] Introduced by D. S. Wall in 2007, the three categories broadened the scope to encompass the diverse range of digital offences and deviance in cyberspace. 'Crimes *against* the machine', also known as computer integrity crimes, cover acts such as hacking, network breach and Distributed Denial of Service (DDoS).[22] 'Crimes *using* the machine', also known as computer-assisted crimes, include piracy, robberies and scams, while 'crimes *in* the machine', also known as computer content crimes, encompass acts such as online hate, harassment and pornography.[23] Figure 1 encapsulates the entire cybercrime spectrum by largely following Gordon and Ford's approach, which involves identifying the opposite ends of the spectrum and positioning other classifications either near these extremes or somewhere in between.

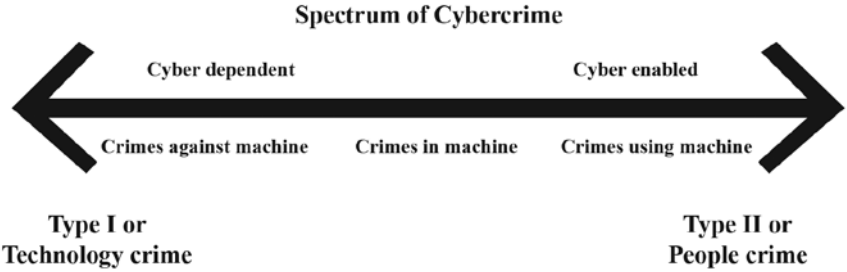

Figure 1 Opposite Ends of the Cybercrime Spectrum

Source: Created by the author using Sarah Gordon and Richard Ford, 'On the Definition and Classification of Cybercrime', *Journal in Computer Virology,* 2006, Vol. 2, pp. 13–20; D. S. Wall (2006); and Mike McGuire and Samantha Dowling, 'Cyber Crime: A Review of the Evidence', Home Office, 2013, pp. 1–29.

While the cyberspace component and the degree of interaction between humans and machines are integral to cybercrime, it is equally important to understand cybercrime from the perspective of its stakeholders or the key actors in the cybercrime ecosystem.[24] The key stakeholders are attackers (e.g., hackers), enablers (e.g., virus writers), defenders (e.g., law enforcement agencies), and the victims.[25] In many cases, stakeholders might simultaneously play the roles of both defenders and victims, particularly if they are in charge of their own systems (e.g., chief information officer or cybersecurity team within an organisation).

The crime is orchestrated in different stages (Figure 2), starting from gathering information about the target and attacking a target, to taking measures to avoid being easily tracked. A range of threat actors are involved in cybercrime activities, including individuals and small criminal groups, organised criminal groups, state and state-affiliated agents, hacktivists, cyberterrorists, script kiddies, and even insiders within an organisation.[26] Given the inherent nature of cyberspace, which provides users with anonymity and the ability to cause disruption with minimum tools and technical knowledge (e.g., through malware-as-a-service), even a novice can pose a significant threat. For instance, script kiddies have been a constant irritant, even with their limited skills and experience, through their reliance on tools developed by those with advanced skills. Furthermore, in cyberspace, attackers do not experience the same level of behavioural inhibitions as they would in a physical context. The reduced sense of proximity to the victim leads to diminished feelings of guilt and a lower fear of retaliation.[27]

Budi Arief et al. emphasise the importance of understanding cybercrime from the perspective of stakeholders by placing them at the centre of their analysis.[28] For a comprehensive understanding of cybercrime, it is pertinent to examine the individual components that make up its ecosystem. This includes examining attackers' motivation, methods employed by them, level of breach, or the extent of the impact caused by an attack.[29] Breaking down these illicit activities in cyberspace into components provides a robust foundation for constructing a comprehensive understanding of the broader picture. Moreover, such a framework will also assist defenders in closing all potential vulnerabilities, thereby minimising the risk of being attacked.

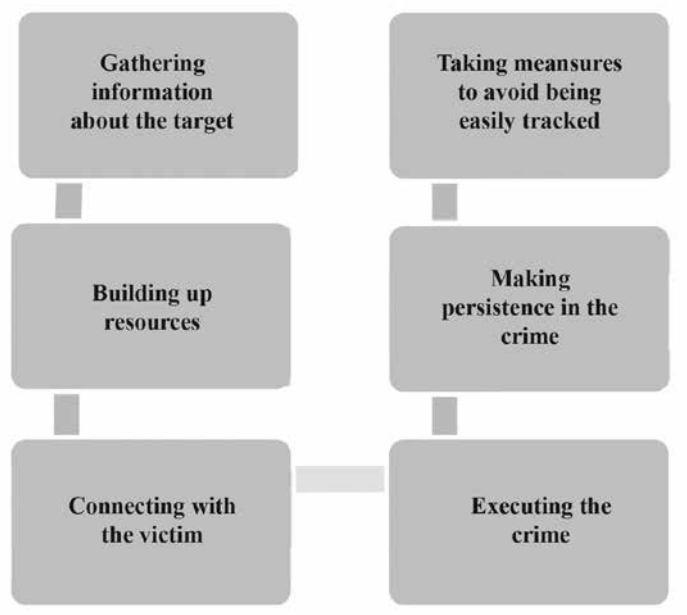

Figure 2 Stages Involved in Cybercrime
Source: Gargi Sarkar and Sandeep K. Shukla, 'Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies', *Journal of Economic Criminology,* Vol. 2, 2023, pp. 1–26.

The characterisations discussed above offer several frameworks for understanding the types of acts that constitute cybercrime. They also provide a foundation for policymakers worldwide to develop a shared language for addressing cybercrimes. This is not to suggest that governments and intergovernmental organisations have made no attempts in the past to reach a common understanding of the definitional aspect of cybercrime. In fact, such efforts have been ongoing for decades.

Intergovernmental Organisations and Cybercrime

The first major international endeavour by an intergovernmental organisation to address criminal activities in cyberspace, as we know them today, occurred in 1994 with the publication of the United Nations Manual on the Prevention and Control of Computer-Related Crime. The absence of clarity

on the definition was clear from the fact that the document used the terms 'computer crime' and 'computer-related crime' interchangeably.[30]

It took more than a decade for the international community to recognise the need for an international instrument or legal framework to address the rise in cybercrime. This realisation came at a time when internet usage was expanding across all areas of the society, making individuals and organisations more vulnerable to online threats and criminal activities. The Convention on Cybercrime of the Council of Europe (ETS No. 185)[31] also known as the Budapest Convention, provided the first binding international instrument on the issue of cybercrime.[32]

The Convention was founded with the global aim to 'pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation'.[33] Given that many states lacked legislation at the time concerning cybercrime and appropriate penalties, the Convention was the first step towards globalising the legislation.[34] While a European cyber instrument, the Convention is open to non-member states, with a unanimous decision of the parties. Despite being specifically charted out to address cybercrime across different jurisdictions, the absence of a cybercrime definition from its definition clause is jarring, especially when the Convention focuses on the definition of what constitutes a *computer system, computer data, service providers,* and *traffic data.*[35] However, on reading the Preamble, one can notice that the Convention makes a subtle attempt to define cybercrime as an

> … action directed against the confidentiality, integrity and availability [CIA] of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct….[36]

The Convention classifies specific offences under distinct categories and provides an important classification model for states to ratify. These categories are as follows:

1. **Category 1**: This category covers offences against the confidentiality, integrity and availability of computer data and systems[37]
2. **Category 2**: Computer-related offences
3. **Category 3**: Content-related offences
4. **Category 4**: Offences related to infringements of copyright and related rights

5. **Category 5**: [38] Acts of a racist and xenophobic nature committed through computer systems

The most recent and ongoing efforts are taking place within the UN, where, since 2021, member states have been negotiating an international treaty on countering cybercrime. If adopted, this would become the first UN binding instrument on cybercrime.[39] Over time, states are increasingly recognising the value of negotiating a binding agreement to address the new and emerging threats that are evolving at an unprecedented scale. According to the reports, the draft convention adopted by the United Nations General Assembly in December 2024, will 'provide tools that will enhance international cooperation, law enforcement efforts, technical assistance, and capacity building relating to cybercrime'.[40]

Table 1 provides an illustrative list of the cybercrime categories and types of offenses, taken from the official website of the Indian Cyber Crime Coordination Centre (I4C). While the list is not exhaustive, the offences and acts it includes are largely consistent across different jurisdictions. In fact, upon closer examination, the list aligns with the classification frameworks discussed above.

Table 1 An Illustrative List to Demonstrate the Scope of Cybercrime Offences

Categories of cybercrime	**Cybercrime offenses**
Cryptocurrency crime	Cryptojacking Crypto mining and Cloud mining Scams Cryptocurrency investment frauds
Cyber Terrorism	-
Hacking/Damage to computer system	Email hacking Tampering with computer source documents Unauthorised access/Data breach Website defacement
Online and social media related crime	Cheating by impersonation Cyber bullying/stalking Email phishing Online job fraud Identity theft

Online financial fraud	Business Email Compromise (BEC) Debit/credit card fraud E-wallet related fraud Fraud calling/Vishing Internet banking related fraud
Publishing/transmitting of explicit material in electronic form	-
Ransomware	-
Child pornography/Child Sexual abuse material (CSAM)	-

Source: Indian Cybercrime Coordination Centre (I4C).
Note: This is not an exhaustive list.

Approaches to Cybercrime: India and the US

Both the US and India have been incessantly facing cyber threats, with profound implications for their economy and national security. On several occasions, the threat actors have targeted critical national infrastructure, such as hospitals and pipeline systems, leading to severe disruptions and, in some cases, forcing businesses into bankruptcy.[41] The perpetrators of these attacks have used methods and tools ranging from malware to gain unauthorised access to financial data, to wipers designed to completely erase data, and ransomware to hold businesses hostage by encrypting their critical data.

Among the various threats, ransomware has emerged as a prominent tool employed by threat actors. These attacks are not merely the work of criminal groups; state-backed actors have also been using ransomware for geopolitical ends. In fact, the nexus between criminal groups and states has been well-documented, detailing the symbiotic relations between these actors as a political–criminal nexus.[42] Scholars have also been attempting to conceptualise the connection between cybercriminals and states, particularly in terms of the degree of control that states exert over these groups. The question of state involvement has always been approached in a national security context, and rightfully so. However, much less consideration has been given to the role of the state in financially motivated crimes, particularly ransomware.[43]

Despite the potential for plausible deniability by states following a cyberattack, there have been numerous cases where states have openly called out adversaries for their belligerent behaviour in cyberspace. One such

instance was the infamous Microsoft Exchange server data breach, which began as an espionage campaign but spiralled into several ransomware attacks. Following this, the US and its allies, including the European Union (EU), North Atlantic Treaty Organization (NATO), and several other countries, openly condemned China's government for 'malicious cyber activity'.[44] This is particularly significant as it marked the first time the US had accused China of abetting ransomware attacks. The act of publicly attributing a ransomware attack to a specific agency of a state actor encapsulates the shift in the US approach towards cybercrime and other form of security threats.

The National Cybersecurity Strategy, which was released in March 2023, summarises the US' approach towards cybersecurity in general and cybercriminal activities in particular.[45] From the introduction onwards, the strategy asserts the need for fundamental changes to the dynamics of the digital ecosystem by implementing appropriate measures against the threat actors. The strategy also publicly attributes major cyber incidents to China, Russia, Iran, North Korea and other 'autocratic states with revisionist intent' as malicious actors.[46] Furthermore, the document also underscores cyber operations of criminal syndicates as a threat to the national security, public safety and economic prosperity of the US and its allies. At the same time, it acknowledges the underlying challenges in addressing threats from criminal syndicates, particularly those operating out of states that do not cooperate with US law enforcement agencies, highlighting the importance of global alliances in tackling the threats.

The US National Cybersecurity Strategy seeks to build and enhance collaborations around five pillars:[47]

1. Defend Critical Infrastructure;
2. Disrupt and Dismantle Threat Actors;
3. Shape Market Forces to Drive Security and Resilience;
4. Invest in a Resilient Future; and
5. Forge International Partnerships to Pursue Shared Goals.

Defending critical infrastructure is vital as states become increasingly reliant on digital technologies for seamless functioning. Given the importance and utility of critical infrastructure, it becomes a valuable target for criminal syndicates and other threat actors. From its previous experiences, the US government has already been proactively preparing for potential black swan events that could impact critical infrastructure. Government-led campaigns such as 'Shields Ready' and 'Shields Up' are some significant steps towards promoting critical infrastructure security and resilience.[48] In addition, the US

government has been encouraging collaboration with private-sector entities to combat malicious activities in the digital realm. Regulators are also being asked to promote the adoption of secure-by-design principles and to prepare for the implementation of voluntary consensus standards.

The US is not solely focused on enhancing its prevention and mitigation capabilities. In fact, one of the stated goals of the National Cybersecurity Strategy is to 'use all instruments of national power to disrupt and dismantle threat actors whose actions threaten…' its interests.[49] To accomplish the stated aim of disruption and dismantling to establish a credible deterrence against threat actors, the US affords itself with a response including diplomatic, military (both kinetic and cyber), financial, intelligence and law enforcement capabilities. All of these responses, with the exception of 'kinetic response', do not represent a significant shift, as the US has already been employing these strategies for some time. There are already existing mechanisms to authorise sanctions on individuals and entities involved in malicious cyber-enabled activities against US interests.[50] To tackle the surge of international cybercrime activities, the FBI has been deploying cyber assistant legal attachés (ALATs) across US embassies, including in New Delhi.[51] The FBI, which is the lead federal agency in the US for investigating cyberattacks and intrusions, also leads the National Cyber Investigative Joint Task Force (NCIJTF). NCIJTF comprises over 30 partner agencies, including law enforcement, the intelligence community, and the US Department of Defense.[52]

As a response to a surge in ransomware activities, the US has convened the Counter-Ransomware Initiative with international partnerships, which has been conducting global exercises to build resilience. Subsequently, the US has also been targeting illicit cryptocurrency exchanges on which threat actors rely and has discouraged ransomware payments to criminals. Given the nature of cybercrime, the US is also focusing on forging international partnerships, both bilaterally and at multilateral forums.

As far as India is concerned, the government is proactively working towards securing India's digital infrastructure. In fact, cybersecurity has been recognised as a key foreign policy and security priority by decision-makers.[53] The Indian government has also intensified its focus on cybersecurity over the last decade by establishing a comprehensive institutional and regulatory framework. The first major step was the National Cybersecurity Policy 2013, which was formulated with an aim to build mechanisms to obtain strategic information regarding threats in real-time, and to 'build a secure and resilient cyberspace for citizens, businesses and Government'.[54] The document charts

out a map for enhancing India's cybersecurity strategy by emphasising on capacity building and encouraging cybersecurity awareness in the private sector. Moreover, it also underlines the importance of public–private partnerships in securing critical information infrastructures.

Initiatives such as Cyber Swachhta Kendra (Botnet Cleaning and Malware Analyses Centre) exemplify the spirit of public–private collaboration, where the centre, operated by the Indian Computer Emergency Response Team (CERT-In), functions in close collaboration with Internet Service Providers (ISPs) and antivirus software companies. Another example is the National Cybercrime Threat Analytics Unit (NCTAU), which enables collaboration between law enforcement agencies, academia, and the private sector to analyse collected information and further disseminate it to the concerned agencies for appropriate response.[55]

Regarding cybercrime, the policy advocates for appropriate legislative intervention to enhance law enforcement capabilities to prevent, investigate, and prosecute criminal activities in cyberspace. The policy has also played an instrumental role in the creation of several institutions pertaining to cybersecurity, particularly the National Critical Information Infrastructure Protection Centre (NCIIPC), the national nodal to protect critical information infrastructure.

The government has also launched initiatives to sensitise law enforcement agencies about the emerging cyber threats by linking promotions with mid-career skill enhancement in specific domains, including cybersecurity.[56] The Ministry of Home Affairs (MHA) periodically issues cybercrime trends and modus operandi to law enforcement agencies in different states.[57] To augment the nation's collective capability to address cybercrime, the MHA launched the Indian Cyber Crime Coordination Centre (I4C) initiative with an aim to serve as a nodal hub for curbing cybercrime across the country. To facilitate real-time collaboration between law enforcement agencies of different states, Joint Cyber Coordination Teams (JCCTs) were established based on cybercrime areas or hotspots.

Anonymous reporting of cybercrimes, including child pornography and child sexual abuse material (CSAM), has also been made easier with National Cyber Crime Reporting Portal. To facilitate the ease in reporting, an Artificial Intelligence (AI) based chatbot (Vani) has been developed to help register citizens' complaints on the portal. Given the large proportion of the cybercrimes reported are financial frauds, a Citizen Financial Fraud Reporting and Management System was launched in 2021 by bringing on board all States and Union Territories for quick reporting and to prevent

flow of funds to fraudsters. As per an official order issued by the Reserve Bank of India (RBI), banks are required to conduct an annual review of fraud incidents and also the amount recovered.[58] The same order has also mandated banks to constitute a Special Committee of the Board for monitoring and following up the cases of fraud (SCBF) involving amounts Rs 1 crore and above. In response to the growing network of predatory loan applications, the government has issued regulations requiring intermediaries hosting these apps to remove them from their platforms.[59]

To sum up, in response to exponential growth in cybercrime incidents, the Indian government has swiftly introduced and launched initiatives to combat cybercrime at every level. These efforts range from spreading awareness, raising alerts and sharing information among stakeholders to ensuring that criminals are brought to justice. The measures undertaken illustrate the importance of every stakeholder in building a resilient cyberspace.

India–US Cooperation at the Bilateral Level

The bilateral relationship between India and the US on securing cyberspace has been steadily strengthening. For years, both countries have worked together in the absence of any official joint framework. The first notable step in securing the then emerging digital realm was taken in 2001 when India and the US decided to establish the India–US Cybersecurity Forum.[60] The aim was to forge cooperation to protect critical infrastructure and enhance cooperation among law enforcement agencies on both sides in dealing with cybercrime. While both countries shared a common understanding of the need for a real-time response to cybercrime, the only available avenues for their law enforcement agencies to collaborate were the INTERPOL and Mutual Legal Assistance Treaties (MLATs).[61] Both countries also forged an arrangement to set up a cyber forensic training course for security personnels in India to efficiently tackle cybercrimes.[62]

It took almost a decade for both countries to sign another landmark agreement in 2011, when the US Department of Homeland Security signed a Memorandum of Understanding (MoU) with India's Department of Information Technology to promote cooperation and timely exchange of information regarding cybersecurity.[63] The agreement was forged to establish best practices and exchange information and expertise between the two governments through their respective agencies dealing with cybersecurity. The agreement also facilitated technical and operational collaboration in the field of cybersecurity.

India is bilaterally engaged with the US on cybersecurity through numerous annual initiatives and dialogues at multiple levels. However, the signing of the Framework for the US–India Cyber Relationship in 2016 marks a significant milestone in the engagement between both countries in cyberspace. The framework recognises cyber issues as a key component of the India–US relationship and underlines shared principles, including:

> A commitment to an open, interoperable, secure, and reliable cyberspace environment … A recognition of the importance of bilateral and international cooperation for combating cyber threats and promoting cybersecurity … A recognition of the importance of and a shared commitment to cooperate in capacity building in cybersecurity and cybersecurity research and development … A commitment to promote closer cooperation among law enforcement agencies to combat cybercrime between the two countries….[64]

The framework emphasises the need to establish appropriate mechanisms to enable real-time information sharing. To adequately respond to the emerging cybercrime ecosystem, the framework underlines the need for skill development, capacity enhancement and digital forensics, as well as the establishment of robust legal frameworks for law enforcement agencies. The need to promote and improve the existing mechanisms, particularly the MLAT, is also part of the bilateral framework.

Following the framework agreement, an MoU was signed between the CERT-In and the United States Computer Emergency Readiness Team (US-CERT) in 2017.[65] The agreement focuses on enabling an ease in exchange of information on cyber incidents and coordination in formulating an appropriate response. Unlike the framework agreement, which has a wider cybersecurity scope, the CERT agreement only concerns the incident alert and response mechanism. Other existing bilateral initiatives that supplement the wider framework agreement include India–US Homeland Security Dialogue (HSD) and India–US Cyber Dialogue, focusing on joint efforts to confront emerging threats in cyberspace.

In 2021, representatives from the US Department of Justice, together with personnel from the FBI, met CBI officials to discuss the outline to combat cybercrimes, particularly cyber-enabled financial frauds.[66] The discussion underlined the need for cooperation in confronting emerging cybercrimes through faster information exchange and evidence-sharing. The parties met again in 2023 to reaffirm existing arrangements that, in some cases, played a crucial role in securing testimony from US victims of call centre fraud for use

in legal proceedings.[67] These efforts contributed to successful enforcement actions against alleged perpetrators in India, including the collection of evidence and the arrest of individuals suspected of involvement in cyber-enabled financial crimes.

The necessity for a bilateral framework on cybercrime is essential as India and the US have emerged as geographical hubs of cybercrime.[68] The World Cybercrime Index, constituted in 2024, only covers profit-driven cybercrime and focuses solely on the countries where offenders are primarily based rather than their nationality. The index classifies cybercrimes into five broader categories, including:

1. Technical products/Services;
2. Attacks and Extortion;
3. Data/Identity theft;
4. Scams; and
5. Cashing out/money laundering.[69]

The study essentially posits a new perspective explaining how cybercrime has a strong local dimension, which is in stark contrast to focusing on it as a fluid and global phenomenon. To the dismay of law enforcement agencies in both India and the US, both countries rank among the global top ten cybercrime hotspots. While the US is a hotspot for both technical and non-technical crimes, India has emerged as a hub for scams.

Tech support fraud or scams have steadily emerged as a new and significant element in the cybercrime ecosystem. This category of crime, associated with the phenomenon of 'cyber slavey' in Southeast Asia, operates on an industrial scale in the region.[70] Tech support scammers acting as a legitimate entity 'use scare tactics' to trick victims into unnecessary technical support devices to fix non-existent issues in their devices and software.[71] Once they gain access to the victims' systems, the scammers exploit the situation to their advantage.

Recently, these criminal syndicates have also begun to emerge in India, primarily through the operation of call centres that facilitate scams and defraud victims. The issue of tech fraud, including the proliferation of fake call centres, was also raised during the FBI chief's visit to India.[72] The tech support fraud perpetrators, according to government reports, overwhelmingly target the elderly based in the US, accounting for loss of over US$ 724 million.[73]

Acting on compounding complaints and intelligence from international partners such as the US, the Indian agencies have conducted search and

seizure operations across different locations in India under 'Operation Chakra'. Table 2 details the different iterations of Operation Chakra and other similar investigations undertaken by Indian agencies in coordination with the US and the private sector. These operations illustrate the growing coordinated response of law enforcement agencies in both countries to the burgeoning cybercrime industry.

As seamless as it may appear, it is challenging for Indian law enforcement agencies to get access to data stored under the control of companies or service providers based in the US. The existing avenues available include the MLAT, which is seen as 'long-drawn and cumbersome'.[74] Reforms in the MLAT process are long overdue. Moreover, scholars have, on occasion, recommended approaches to overcoming the challenges of cross-border data access, particularly between close partners. For instance, Peter Swire and Deven Desai proposed the establishment of a Single Point of Contact (SPOC) designate to handle and process government-to-government requests.[75] In the suggested SPOC approach, the request from the designate would receive different legal treatment than requests coming from another office or agency. Swire and Desai also discuss the inherent challenges faced by law enforcement agencies: first, getting access to data at rest is difficult as any form of communication is stored in the Cloud, often in different countries. Second, accessing data is also challenging due to the widespread use of encryption, making it difficult for agencies to engage in a legally authorised wiretap.

To legally permit US-based technology companies to disclose user data directly to certain foreign governments in response to requests for assistance in serious investigations, the US passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018.[76] This Act establishes a process to streamline such requests for disclosure from foreign law enforcement agencies. The law was enacted as a response to the need for better cooperation between governments in the age of extensive digitalisation.

To avail the benefits of the Act, the Indian government is required to amend the domestic legislation and rules pertaining to protection of personal digital data. However, India can draw key lessons from the countries such as UK and Australia that have concluded agreements with the US. The Act allows the US government to enter into executive agreements with foreign governments to allow foreign law enforcement agencies to access content directly from US service providers.[77] The law also requires the US government to appraise domestic laws and regulations of partner states and also ensure that agencies requesting data have clear and effective oversight mechanisms

in their respective jurisdictions. To the benefit of Indian law agencies, the government has enacted the much-awaited Digital Personal Data Protection Act, 2023, which may ease the case for sealing a deal with the US under the CLOUD Act.

Table 2 India–US Law Enforcement Operations with Partners (2022–2024)

Year	Operational details	Nature of cybercrime
2022	Operation Chakra led by the CBI conducted an extensive search across different locations in India against cyber-enabled financial crimes. The operation was based input from the FBI, INTERPOL, Canadian, and Australian law enforcement agencies.[78]	Cyber-enabled financial crime
2023	The CBI conducted the operation across four different locations in Delhi/NCR and found a fake tech support call centre. The accused were involved in online cheating of US citizens impersonating as tech support executives.[79]	Tech support fraud
2023	As part of Operation Chakra II, the CBI, in collaboration with law enforcement agencies and the private sector, launched a nationwide crackdown across different location in India. The aim of the operation was to disrupt international organised cyber-enabled financial crimes operation in India. Amazon and Microsoft were part of the operation because the illegal call centres raided by the CBI were set up to impersonate Microsoft and Amazon customer support.[80]	Tech support fraud
2023	A transcontinental police operation—HAECHI IV—against online financial crime was concluded, with almost 3,500 arrests and seizures of USD 300 million across 34 countries. India and US were also part of this collaborative law enforcement operation.[81]	Voice Phishing, romance scams, online sextortion, investment fraud, money laundering, illegal online gambling, business email compromise fraud and e-commerce fraud.

2024	The Enforcement Directorate (ED) collaborated with the US authorities to uncover a Rs 3,000-crore scam involving cryptocurrencies.[82]	Cryptocurrency
2024	As part of Operation Chakra III, searches were conducted in different locations across Delhi, Noida, and Gurgaon. CBI is coordinating with FBI and other law enforcement agencies in multiple countries through INTERPOL.[83]	Tech support fraud, malicious software in victim's devices

India–US Cooperation at Multilateral Forums

As discussed in the previous sections, despite existing international frameworks such as the Budapest Convention, countries are also working towards forging a UN treaty on cybercrime. While the US is party to the Budapest Convention, India is yet to come to terms with the framework. This should not be understood as an absence of India–US engagement in multilateral forums.

With the rise in ransomware attacks, including high-profile cases involving institutions such as the All India Institute of Medical Sciences (AIIMS) in India and the Colonial Pipeline in the US, countries are increasingly developing partnerships to curb this growing threat. Particularly concerning are state-backed or supported ransomware attacks, which have elevated the threat of such incidents to a national security level. Against this background, the first International Counter Ransomware Initiative (CRI) was convened in 2021 with participation from more than 30 countries, including India. The joint statement asserted the need for a concerted effort to counter the growing menace of ransomware threat. The statement also acknowledged the need to develop network resilience, counter illicit finance, and actively disrupt criminal syndicates through international cooperation.[84]

The CRI actively discourages ransomware payments, although the declaration remains non-binding. Five working groups were also established as part of the US-led initiative, with India and Lithuania co-leading efforts on resilience[85] in addition to being part of the information-sharing efforts on ransomware.

In pursuit of a significant role in global ransomware response, India has shared its intention to establish a dedicated counter ransomware platform,

Malwarekosh, to analyse, share and cooperate on counter ransomware activities.[86] As part of the CRI, India, along with partnering nations, has undertaken counter ransomware exercises to simulate a widespread cybersecurity incident and allowing participating members to test their capability to respond to a major incident.[87]

India and US are also actively participating in forums such as Quadrilateral Security Dialogue or Quad to galvanise support against ransomware and other forms of cybercrimes. Recognising the importance of a multistakeholder approach to countering the ransomware threat, the group called on states in the Indo-Pacific region not to support or provide safe havens for ransomware actors. Furthermore, initiatives such as Quad Cyber Challenge was undertaken in 2023 to instill cyber hygiene awareness among citizens against malicious activities in cyberspace. In a joint statement, the Quad also expressed its support for a UN treaty on cybercrime.[88]

The issue of emerging cyber threats, particularly those driven by Artificial Intelligence, was also a key focus under India's G20 Presidency. India's Union Home Minister Amit Shah, speaking at the inaugural session of the G20 Conference on Crime and Security in the Age of NFTs, AI and Metaverse, highlighted how ransomware attacks have direct impact on national security.[89] Although the session primarily offered talking points, the deliberations on the theme underscore the gravity of the threat posed by ransomware attacks. Since India is not a signatory of the Budapest Convention, the government relies on INTERPOL and international partners to rely on threat intelligence and investigation.

At the time of the writing, the UN Cybercrime Convention was unanimously approved by UN members. In its proposal at the negotiation stage, Indian government submissions called out countries to make it illegal to share 'offensive messages' on social media.[90] India has also proposed an active 24/7 global communication channel to combat rising cases of phishing, which, according to the Indian proposal stands out as the predominant cybercrime globally.[91] The US, on the other hand, while in broader agreement with the draft, reiterated its opposition to any provisions that may result in human rights abuses, targeting dissidents, journalists, and others.[92]

Conclusion

The article begins with a conceptual overview of cybercrime, examining existing scholarship and the various categorisation and classifications of malicious acts that qualify as cybercrime. This is followed by an analysis of

how cybercrime is understood within current intergovernmental frameworks. The article then evaluates the domestic responses and differing approaches of India and the US to cybercrime, highlighting the agencies involved in both the states. Although India and the US actively collaborate on broader cybersecurity issues, there is no specific bilateral framework addressing cybercrime. However, US-led global initiatives such as the CRI and India's significant involvement underscore India's crucial role in countering cybercrime threats.

With the passage of India's privacy law, the country is now better positioned to negotiate an executive agreement under the CLOUD Act, enhancing information sharing, coordination and joint responses to cybercrimes. Furthermore, the governments can leverage existing strategic dialogue initiatives to prioritise cybercrimes and other forms of malicious activities in cyberspace, addressing the rapidly evolving threat landscape more effectively.

Notes

1. 'INTERPOL-led Operation Targets Growing Cyber Threats', INTERPOL, 1 February 2024, available at https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats, accessed on 5 August 2024; , 'Disrupting a Grandoreiro Malware Operation', INTERPOL, 18 March 2024, available at https://www.interpol.int/en/News-and-Events/News/2024/Disrupting-a-Grandoreiro-malware-operation, accessed on 5 August 2024.
2. 'Press Releases', Central Bureau of Investigation, Government of India, 19 August 2023, available at https://cbi.gov.in/press-detail/NTk0MQ==, accessed on 5 August 2024.
3. Amy Hogan-Burney, 'Microsoft, Amazon, and International Law Enforcement Join Forces to Fight Tech Support Fraud', Microsoft, 19 October 2023, available at https://blogs.microsoft.com/on-the-issues/2023/10/19/microsoft-amazon-tech-support-fraud-india/, accessed on 5 August 2024.
4. Steve Morgan, 'Cybercrime to Cost the World $10.5 Trillion Annually By 2025', *Cybercrime Magazine*, 13 November 2020, available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, accessed on 5 August 2024.
5. Simon Handler and Liv Rowley, 'The 5×5—Cybercrime and National Security', Atlantic Council, 29 June 2023, available at https://www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/, accessed on 5 August 2024.
6. 'Costa Rica Declares National Emergency Amid Ransomware Attacks', *The Guardian*, 12 May 2022, available at https://www.theguardian.com/world/2022/

may/12/costa-rica-national-emergency-ransomware-attacks, accessed on 5 August 2024.

7. Rimjhim Singh, 'Here is How Much Indians Lost to Cyber Frauds between Jan and Apr of 2024', *Business Standard*, 27 May 2024, available at https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html, accessed on 5 August 2024.
8. 'Internet Crime Report 2023', Federal Bureau of Investigation, Department of Justice, United States of America, 2023, available at https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, accessed on 5 August 2024.
9. Martin Bruce, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair and Federico Varese, 'Mapping the Global Geography of Cybercrime with the World Cybercrime Index', *PloS ONE*, Vol. 19, No. 4, 2024, pp. 1–16.
10. Cherian Samuel, 'Prospects for India-US Cyber Security Cooperation', *Strategic Analysis*, Vol. 35, No. 5, September 2011, pp. 770–780.
11. Brian K. Payne, 'Defining Cybercrime', in Thomas J. Holt and Adam M. Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer International Publishing, 2020, pp. 3–25.
12. Ibid.
13. Ibid., p. 7.
14. Kyung-Shick Choi, Claire S. Lee and Eric R. Louderback, 'Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime', in Thomas J. Holt and Adam M. Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer International Publishing, 2020, pp. 27–43.
15. Ibid., p. 30.
16. Sarah Gordon and Richard Ford, 'On the Definition and Classification of Cybercrime', *Journal in Computer Virology*, Vol. 2, 2006, pp. 13–20.
17. Ibid., p. 15.
18. Mike McGuire and Samantha Dowling, 'Cyber Crime: A Review of the Evidence', Home Office, 2013, pp. 1–29.
19. Ibid., p. 5.
20. Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken, 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies', *Forensic Sciences*, No. 2, 2022, pp. 379–398.
21. Ibid.; Gargi Sarkar and Sandeep K. Shukla, 'Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies', *Journal of Economic Criminology*, Vol. 2, 2023, pp. 1–26.
22. Kirsty Phillips et al., 'Conceptualizing Cybercrime', n. 20, p. 384.
23. Ibid.
24. Budi Arief, Mohd Azeem Bin Adzmi and Thomas Gross, 'Understanding Cybercrime From its Stakeholders' Perpectives: Part 1- Attackers', *IEEE Security & Privacy*, Vol. 13, No. 1, 2015, pp. 71–76.

25. Kyung-Shick Choi et al., 'Historical Evolutions of Cybercrime', n. 14, p. 33.
26. Stearns Broadhead, 'The Contemporary Cybercrime Ecosystem: A Multi-disciplinary Overview of the State of Affairs and Developments', *Computer Law & Security Review*, Vol. 34, No. 6, 2018, pp. 1180–1196.
27. Joanna Curtis and Gavin Oxburgh, 'Understanding Cybercrime in "Real World" Policing and Law Enforcement', *The Police Journal: Theory, Practice and Principles*, Vol. 96, No. 4, 2023, pp. 573–592.
28. Budi Arief et al., 'Understanding Cybercrime From its Stakeholders' Perpectives', n. 24.
29. Ibid., p. 75.
30. 'United Nations Manual on the Prevention and Control of Computer-Related Crime', United Nations, 1994, available at https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF, accessed on 5 August 2024.
31. ETS stands for European Treaty Series.
32. Jose de Arimateia da Cruz, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime', in Thomas J. Holt and Adam M. Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer International Publishing, 2020, pp. 223–237.
33. 'Details of Treaty No. 185', Council of Europe (COE), available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, accessed on 5 August 2024.
34. de Arimateia da Cruz, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime', n. 32.
35. 'Details of Treaty No. 185', Council of Europe (COE), n. 33.
36. Ibid.
37. Kirsty Phillips et al., 'Conceptualizing Cybercrime', n. 20, p. 386.
38. Category 5, which addresses the criminalisation of acts of a racist and xenophobic nature, was added in the Convention following the adoption of an additional protocol to the Convention in 2002.
39. Isabella Wilkinson, 'What is the UN Cybercrime Treaty and Why Does it Matter?', Chatham House, 4 August 2023, available at https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter, accessed on 5 August 2024.
40. 'United Nations: Member States Finalize A New Cybercrime Convention', United Nations Office on Drugs and Crime (UNODC), 9 August 2024, available at https://www.unodc.org/unodc/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html, accessed 12 August 2024.
41. Sean Lyngaas and Michelle Watson, 'America's Rural Hospitals Keep Getting Attacked by Cybercriminals. Microsoft and Google are Working to Fix That', *CNN*, 10 June 2024, available at https://edition.cnn.com/2024/06/10/tech/hospital-cyberattack-google-microsoft/index.html#:~:text=A%20February%20ransomware%20attack%20on,try%20to%20recover%20patient%20data, accessed on 12 August 2024.

42. Anita Lavorgna, 'Unpacking the Political-Criminal Nexus in State-Cybercrimes: A Macro-Level Typology', *Trends in Organized Crime*, 2023.
43. James Martin and Chad Whelan, 'Ransomware Through the Lens of State Crime: Conceptualising Ransomware Groups as Cyber Proxies, Pirates, and Privateers', *State Crime Journal*, Vol. 12, No. 1, 2023, pp. 4–28.
44. Kevin Collier, 'U.S. Accuses China of Abetting Ransomware Attack', *NBC News*, 19 July 2021, available at https://www.nbcnews.com/tech/tech-news/us-accuses-china-abetting-ransomware-attack-rcna1448, accessed on 13 August 2024.
45. 'National Cybersecurity Strategy', The White House, March 2023, available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, accessed on 13 August 2024.
46. Ibid., p. 3.
47. Ibid., p. 4.
48. Michael Hill, 'US Launches "Shields Ready" Campaign to Secure Critical Infrastructure', *CSO*, 8 November 2023, available at https://www.csoonline.com/article/1229409/us-launches-shields-ready-campaign-to-secure-critical-infrastructure.html, accessed on 13 August 2024.
49. 'National Cybersecurity Strategy', The White House, n. 45, p. 14.
50. 'Cyber Sanctions', US Department of State, available at https://www.state.gov/cyber-sanctions/#:~:text=E.O.,28%2C%202016%2C%20and%20amends%20E.O, accessed on 13 August 2024.
51. AJ Vicens, 'The FBI is Adding More Cyber-focused Agents to US Embassies', *Cyberscoop*, 3 January 2024, available at https://cyberscoop.com/the-fbi-is-adding-more-cyber-focused-agents-to-u-s-embassies/, accessed on 13 August 2024.
52. 'What We Investigate: National Cyber Investigative Joint Task Force', Federal Bureau of Investigation, Department of Justice, United States of America, available at https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force, accessed on 15 August 2024.
53. Arindrajit Basu, *India's International Cyber Operations: Tracing National Doctrine and Capabilities*, United Nations Institute for Disarmament Research, Geneva, 2022.
54. 'National Cyber Security Policy 2013', Ministry of Electronics and Information Technology, Government of India, 2013, available at https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.
55. 'National Cybercrime Threat Analytics Unit (NCTAU)', Indian Cybercrime Coordination Centre (I4C), available at https://i4c.mha.gov.in/tau.aspx, accessed on 15 August 2024.
56. Bharti Jain, 'IPS Promotions to be Linked to Mid-career Skill Enhancement', *The Times of India*, 1 June 2017, available at https://timesofindia.indiatimes.com/india/ips-promotions-to-be-linked-to-mid-career-skill-enhancement/articleshow/58938893.cms, accessed on 14 August 2024.

57. 'Annual Report 2022-23', Ministry of Home Affairs, Government of India, available at https://www.mha.gov.in/sites/default/files/AnnualReportEngLish_11102023.pdf, accessed 14 August 2024.
58. 'Rajya Sabha Unstarred Question No-2925: Financial Loss Caused Due to Cyber Crimes', Ministry of Finance, Government of India, 29 March 2022.
59. 'Unstarred Question no-1341: Regulation of Predatory Lending Application', Ministry of Finance, Government of India, 1 August 2023.
60. 'India-US Cyber Security Forum - Fact Sheet', Ministry of External Affairs, Government of India, 2 March 2006, available at https://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet/, accessed on 15 August 2024.
61. Cherian Samuel, 'Prospects for India-US Cyber Security Cooperation', n. 10, p. 774.
62. 'FBI to Train CBI Cops Fight e-crime', *The Times of India*, 21 April 2005, available at https://timesofindia.indiatimes.com/fbi-to-train-cbi-cops-fight-e-crime/articleshow/1084535.cms.
63. 'United States and India Sign Cybersecurity Agreement', US Department of Homeland Security, 19 July 2011, available at https://www.dhs.gov/archive/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement, accessed 10 March 2024.
64. 'Framework for the US-India Cyber Relationship', Ministry of External Affairs, Government of India, available at https://www.mea.gov.in/Portal/LegalTreatiesDoc/US16B4110.pdf, accessed on 16 August 2024.
65. 'India CERT Signs a MoU with US CERT', Press Information Bureau, Ministry of Electronics & IT, Government of India, 11 January 2017, available at https://pib.gov.in/newsite/PrintRelease.aspx?relid=156288, accessed on 16 August 2024.
66. 'Readout of Meeting between Department of Justice and the Central Bureau of Investigation of Government of India', US Department of Justice, 21 October 2021, available at https://www.justice.gov/archives/opa/pr/readout-meeting-between-department-justice-and-central-bureau-investigation-government-india.
67. 'Readout of Meeting between the Department of Justice and the Central Bureau of Investigation of India', US Department of Justice, 23 January 2023, available at https://www.justice.gov/archives/opa/pr/readout-meeting-between-department-justice-and-central-bureau-investigation-india.
68. Martin Bruce et al., 'Mapping the Global Geography of Cybercrime', n. 9.
69. Ibid., p. 5.
70. Mark Turner and Anthea McCarthy-Jones, 'Cyber Slavery Starts Up in Southeast Asia', East Asia Forum, 14 June 2023, available at https://eastasiaforum.org/2023/06/14/cyber-slavery-starts-up-in-southeast-asia/, accessed on 16 August 2024.
71. 'Protect Yourself from Tech Support Scams', Microsoft, available at https://support.microsoft.com/en-us/windows/protect-yourself-from-tech-support-

scams-2ebf91bd-f94c-2a8a-e541-f5c800d18435#:~:text=Tech%20support%20scams%20are%20an,problems%20that%20don't%20exist, accessed on 17 August 2024.

72. Ujwal Jalali, 'FBI Chief Meets Delhi Top Cop, Flags Fake Call Centres, Terrorism', *The New Indian Express*, 13 December 2023, available at https://www.newindianexpress.com/cities/delhi/2023/Dec/13/fbi-chief-meets-delhi-top-cop-flags-fake-call-centres-terrorism-2640999.html, accessed on 17 August 2024.
73. 'Internet Crime Report 2023', Federal Bureau of Investigation, n. 8, p. 16.
74. Sreenidhi Srinivasan and Osho Chhel, 'India's Proposed Data Protection Law and an India-US Executive Agreement Under the CLOUD Act', Observer Research Foundation (ORF), 3 June 2022, available at https://www.orfonline.org/research/indias-proposed-data-protection-law, accessed on 17 August 2024.
75. Peter Swire and Deven Desai, 'A "Qualified SPOC" Approach for India and Mutual Legal Assistance', *Lawfare*, 2 March 2017, available at https://www.lawfaremedia.org/article/qualified-spoc-approach-india-and-mutual-legal-assistance, accessed on 17 August 2024.
76. Matt Perault and Richard Salgado, 'Untapping the Full Potential of CLOUD Act Agreements', Center for Strategic & International Studies (CSIS), 6 June 2024, available at https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements#:~:text=Conclusion,sacrificing%20human%20rights%20and%20liberties, accessed on 17 August 2024.
77. Mark Turner and Anthea McCarthy-Jones, 'Cyber Slavery Starts Up in Southeast Asia', n. 70.
78. 'CBI Leads Crackdown on Cyber Enabled Financial Crimes, 105 Places Searched Throughout the Country', *The Hindu,* 5 October 2022, available at https://www.thehindu.com/news/national/cbi-leads-crackdown-on-cyber-enabled-financial-crimes-105-places-searched-throughout-the-country/article65970258.ece, accessed on 5 August 2024.
79. 'Press Releases', Central Bureau of Investigation, Government of India, 16 February 2023, available at https://cbi.gov.in/press-detail/NTUzNA==, accessed on 5 August 2024.
80. 'CBI Launches Operation Chakra-II: What It Is and Why Microsoft and Amazon are Part of This', *The Times of India,* 20 October 2023, available at https://timesofindia.indiatimes.com/gadgets-news/cbi-launches-operation-chakra-ii-what-it-is-and-why-microsoft-and-amazon-are-part-of-this/articleshow/104582380.cms, accessed 5 August 2024.
81. 'USD 300 Million Seized and 3,500 Suspects Arrested in International Financial Crime Operation', INTERPOL, 19 December 2023, available at https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation, accessed on 5 August 2024.

82. 'How India, US Teamed Up to Uncover Rs. 3,000 Crore Scam Involving Cryptocurrencies', *The Times of India,* 1 May 2024, available at https://timesofindia.indiatimes.com/technology/tech-news/how-india-us-teamed-up-to-uncover-rs-3000-crore-scam-involving-crypto-currencies/articleshow/109671833.cms, accessed on 5 August 2024.
83. 'CBI Takes Action to Dismantle A Major Transnational Cyber-enabled Financial Crime Network', Central Bureau of Investigation, Government of India, 26 July 2024, available at https://cbi.gov.in/press-detail/NjQzNQ==, accessed on 5 August 2024.
84. 'Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021', The White House, 14 October 2021, available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/, accessed on 18 August 2024.
85. Cherian Samuel, 'Synergising International Cooperation and National Strategies to Combat Ransomware', Commentary, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), 20 October 2023, available at https://www.idsa.in/idsacomments/National-Strategies-to-Combat-Ransomware-csamuel-201023, accessed on 18 August 2024.
86. Prashant Jha, 'Grouping Steps Up Efforts Against Ransomware, India A Key Partner', *Hindustan Times*, 3 November 2022, available at https://www.hindustantimes.com/cities/delhi-news/grouping-steps-up-efforts-against-ransomware-india-a-key-partner-101667413218970.html, accessed on 18 August 2024.
87. 'India & UK Conducts Counter Ransomware Exercise for 26 Nations', Press Information Bureau, National Security Council Secretariat, Government of India, 6 September 2022, available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1857243; 'CERT-In hosts Cyber Security Exercise "Synergy" for 13 Countries As Part of International Counter Ransomware Initiative - Resilience Working Group', Press Information Bureau, Ministry of Electronics & IT, Government of India, 31 August 2022, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1855771, accessed on 18 August 2024.
88. 'Quad Foreign Ministers' Statement on Ransomware', Ministry of External Affairs, Government of India, 23 September 2022, available at https://www.mea.gov.in/bilateral-documents.htm?dtl/35746/Quad_Foreign_Ministers_Statement_on_Ransomware, accessed on 18 August 2024.
89. 'At G20 Conference, Amit Shah Calls for Cooperation to Tackle Cyber Threats, Flags Ransomware Attacks, Misinformation Campaigns with "Toolkits"', *The Indian Express*, 14 July 2023, available at https://indianexpress.com/article/india/at-g20-conference-amit-shah-calls-for-cooperation-to-tackle-cyber-threats-flags-ransomware-attacks-8833778/, accessed on 18 August 2024.
90. Karan Mahadik, 'UN Cybercrime Treaty Finalised: What Is It and Why Is It Facing Widespread Pushback?', *The Indian Express*, 17 August 2024, available at https://

indianexpress.com/article/technology/tech-news-technology/un-cybercrime-treaty-key-features-and-pressing-concerns-9518068/, accessed on 18 August 2024.

91. Ashish Aryan, 'India Proposes 24x7 Global Communication Link to Curb Cybercrimes', *The Economic Times*, 22 February 2024, available at https://economictimes.indiatimes.com/tech/technology/india-proposes-round-the-clock-global-communication-link-to-curb-cybercrimes/articleshow/107891624.cms?from=mdr, accessed on 18 August 2024.
92. 'On the Adoption of the UN Convention Against Cybercrime', US Department of State, 9 August 2024, available at https://www.state.gov/on-the-adoption-of-the-un-convention-against-cybercrime/#:~:text=The%20United%20States%20welcomes%20the,affecting%20communities%20around%20the%20world, accessed on 18 August 2024.