



**GLOBAL
INITIATIVE**

AGAINST TRANSNATIONAL
ORGANIZED CRIME

A SOCIAL ANTHROPOLOGY OF **CYBERCRIME**

The digitization of India's
economic periphery

PREM MAHADEVAN

APRIL 2020



A SOCIAL ANTHROPOLOGY OF CYBERCRIME

*The digitization of India's
economic periphery*

Prem Mahadevan

April 2020

ACKNOWLEDGEMENTS

The author would like to thank the Government of Norway for funding this project, and Mark Shaw and Tuesday Reitano for their invaluable guidance. Thanks are also due to the three peer reviewers for their helpful comments, and the Global Initiative publications team for editing and design.

ABOUT THE AUTHOR

Before joining the GI, Prem Mahadevan was a Senior Researcher with the Center for Security Studies at the Swiss Federal Institute of Technology. He specialized in research on organized crime, intelligence and irregular warfare. He has co-authored policy studies for the Swiss foreign ministry and written a book on counter-terrorist special operations for the Indian Army. His academic publications include two books on intelligence and terrorism.

© 2020 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative.

Cover illustration: Danie Jansen van Vuuren, Flame Design

Every effort has been made to contact copyright holders of material reproduced in this product.

Please direct inquiries to:

The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalinitiative.net

CONTENTS

Executive summary	1
Why India?	2
Methodology	6
Scope of research	7
Distinguishing between cyber-dependent and cyber-enabled crime	9
The digital underground economy and network types	13
The structure of cybercrime enterprises	17
The dawn of the cybercriminal	21
Technology-driven and knowledge-based superiority	25
Evolution of cybercrime in an ‘emerging superpower’	31
India’s cybercrime hotspots	34
The call-centre boom implodes	36
Early instances of cybercrime in India	37
The response from law enforcement	43
Smartphone scams	42
From Thane to Jamtara: Different methods, similar motives	47
Policy implications – remedy the economics, but do not forget the politics	53
Notes	59





EXECUTIVE SUMMARY

It was November 2018 and the staff of the Indian subsidiary of the Italian multinational firm Maire Tecnimont SpA may have started to wind down mentally. Perhaps no one expected a sudden rush of activity. But then an email arrived from the company's chief executive officer (CEO) in Milan, addressed to the head of the India office; it asked him to create a special Gmail account for future correspondence on a 'highly confidential' acquisition project. The email matched the CEO's communication style. It was followed by telephone conferences between India and Italy, and accompanied by further email exchanges. A prominent Swiss-based lawyer joined in from the Italian side. The situation was clarified to everyone's satisfaction: European regulations prevented the Italian headquarters from making direct payments to a Chinese firm that was being bought, and so the Indian subsidiary would have to act as an intermediary.¹

Upon instructions from Milan, payments were made in three tranches to bank accounts in Hong Kong, totalling US\$18.45 million. As instructions arrived for making yet another payment, the Italian CEO turned up in person at the India office for a surprise inspection. He got a surprise all right: so much so that the head of the Indian subsidiary and its accounts chief were both fired.

They had fallen prey to an elaborate hoax that is thought to have been devised by Chinese hackers. Although investigators have revealed little about how exactly the hoax was carried out, it appears that a combination of naivety and sophisticated deception from the hackers' side had convinced the Indian staff that they had been communicating with the European business managers.

◀ Client-support call centres for foreign businesses, such as this one in Bangalore, is where India made a mark on the global information industry. © Indranil Mukherjee/Getty Images

The deception was not a science-fiction-like operation. Beyond accessing email accounts and emulating their writing style, the scam's success hinged on human gullibility. This lies at the core of most cybercrime, not just in India but in many parts of the world. If a society embraces advances of information technology (IT) much faster than it contributes to creating them, its members will have little understanding of cybersecurity and the risks posed by online fraud. India has long had a reputation for being an IT powerhouse; but the ease with which its own citizens get scammed, as well as their apparent willingness to scam others halfway across the world, suggests that serious deficiencies may lie beneath its technical prowess. Unlike countries with a strong tradition of computer-science research, India has an IT industry optimized for the low-level backroom support of Western companies. Rather than cutting-edge hardware development, what the

country specializes in is IT-enabled services (ITes), chief among which is the business process offshoring (BPO) sector.

Operating client-support call centres (in effect, 'digital sweatshops') for foreign businesses is where India has made a mark on the global information industry. And it is a mark that has been at risk of fading for over a decade as a result of intercultural fissures and the after-effects of the 2008 economic crisis. As India's youthful population rush to buy smartphones but struggle to find stable employment, the logical outcome of having had a glimpse of Western consumerism is being felt: increased frustration at poor local job prospects and a surge in cybercrime. Should such an interpretation seem alarmist, readers are encouraged to keep in mind that while the world average for unemployment is falling, India is currently showing a rise to levels unseen since the early 1970s.²

Why India?

The giant South Asian country is a useful case study for tracking the growth of cybercrime in the developing world. Most analyses of such crime focus on advanced, industrialized countries because that is where the largest and most sophisticated offences originate from. But threat factors can also spring from contexts where having a technical degree is only a passport to frustration in low-wage, overpopulated and nepotistic job markets. While considerable attention has been given to Nigerian-based online scams, the case of India suggests a different growth trajectory to cybercrime. In Nigeria, such crime 'evolved upwards' from poorly educated and impoverished sections of the population towards the working class, who were subsequently enticed to join because of lack of legitimate opportunities for generating household income.³ In India, cybercrime 'devolved downwards' from the relatively well-off English-literate working class towards poorer (non-English-speaking) sections of society. The country's initial wave of cybercrime was motivated by greed, not need.

Unlike Nigeria, which has a history of ongoing political instability exacerbated by military rule, India is a democracy with nearly three decades of decent

economic growth. But this growth has belied the expectations harboured by some sections of its population that they would achieve rapid social mobility in the globalizing first decade of the 2000s. Those who turned to cybercrime did so because they were lucky enough to find short-term employment in the call-centre industry, but unlucky in having few marketable skills beyond spoken English (basic conversational ability). When they looked to move on to higher positions, they found that they lacked the requisite experience and knowledge sets.⁴ Furthermore, in order to stem anger from Western callers who resented having their customer-service complaints 'fobbed off' to low-wage workers in the developing world, call-centre employees were instructed to adopt fake American identities during work hours. Accent training, immersion in cultural reference points, such as popular US television shows, and the adoption of Anglo-Saxon names became essential to fulfilling what was otherwise a low-prestige clerical job. Some employees struggled to cope with the abuse thrown at them by foreign callers; others refused to leave behind their Americanized personas in the workplace, and became conflicted about their own identity and socio-economic status.⁵



FIGURE 1 Business-process offshoring units set up call centres in cities like Bangalore and Hyderabad in the south, Pune and Mumbai in the west, and Gurugram and Noida in the north.

The result was anger and frustration. In India, a country with a deeply classist mentality, those who could converse fluently in the 'elite' English language perceived themselves as being at the front of the queue for better-paying jobs. When these jobs failed to appear in sufficient numbers – as might be expected, considering that one million Indians become age-eligible to join the labour force *each month* – confusion and resentment prevailed.⁶ Coupled with unpleasant telephonic interactions with Western clients, who took it upon themselves to unload racist vitriol upon 'job-stealing Indians', the result was a sharp sense of political and economic grievance. It is not difficult to envisage how this disaffection cynically mutated into criminal schemes

intended to defraud Westerners who were perceived as enjoying a higher quality of life thanks to the underpaid drudgery endured by Indian youth. As one call-centre scammer said: 'Americans complain of being scammed, but have they thought of people ... on the other side of the call who sit around talking to them for hours for 30 000 rupees [about US\$415] a month?'⁷

Clearly, notwithstanding close security and diplomatic ties with industrialized powers, at the level of sub-state or 'people-to-people' contact, India's relations with the West have been less than rosy. This has had implications for globalization as a social concept – what India has experienced, in the form



The Indian subsidiary of the Italian multinational firm Maire Tecnimont, shown here, fell victim to an elaborate hoax in November 2018. © Wiki Commons

of a working-class backlash triggered by envy of the much higher living standards of Western societies, could appear elsewhere. There are already signs that Kenya, owing to its high internet speed (unusual in the African context) and sophisticated banking sector, is becoming a hub for business email compromise (BEC).⁸ According to this *modus operandi*, hackers penetrate email accounts of companies that routinely make wire payments overseas. After studying the writing habits of key executives, they generate fake requests or instructions for payment. This was the kind of scheme that the Indian office of Tecnimont SpA fell prey to, although the perpetrators in that case were suspected to be Asian. India itself is moving up the list of countries that are sources of cybercrime: in 2019, the country stood at eighth place worldwide, behind the United States, Canada, United Kingdom, Germany, Ireland, Brazil and Mexico, but ahead of France and China, which rounded off the top 10.⁹

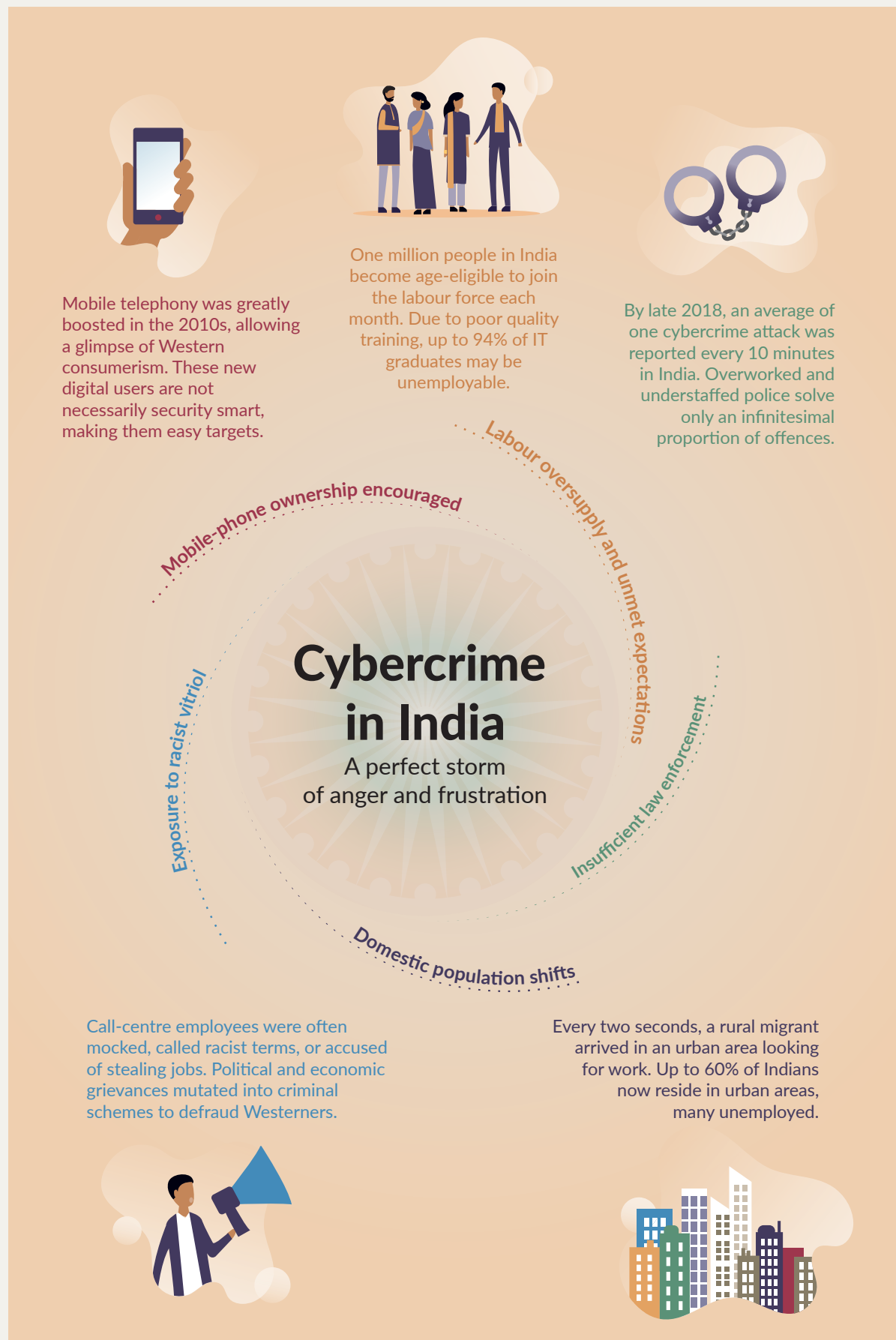
Indian online fraudsters are still at low to intermediate levels of operating skill. They thus present a case study in how a political economy may develop around cybercrime, in places with a low

technological base. For a long time, Indian cyber-criminals have existed on the periphery of the global digital ecosystem. Their role has been that of end-users in data chains that originated either with proficient computer experts in the developed world or with disgruntled local insiders of commercial enterprises. Data used to be (and predominantly still is) obtained for the sole purpose of devising scams.

What distinguishes such activities from traditional organized crime is an apparent lack of patronage from corrupt officialdom. From published accounts, it does not seem that cybercrime in India has political or bureaucratic links. Rather, it thrives in a macro environment of unemployment, urban anonymity and weak police surveillance. A 2019 survey across 22 Indian provinces found that a third of Indian police stations did not have a functioning computer; meanwhile, cybercrime rates had increased by 457% in the preceding five years.¹⁰

At the same time, the country was experiencing massive domestic population shifts. Every two seconds a rural migrant arrived in an urban area looking for work, leaving the government and civil

The perfect storm of factors that led to a rise in India's cybercrime



society with no time or capacity to assimilate such workers into the urban economy or keep them under community-based surveillance. Indeed, there has even been little clarity over just how much of the total Indian population lives in urban areas – although conventional wisdom holds that two-thirds of the population is rural, some guesstimates suggest that 60% of Indians now reside in urban areas.¹¹ Whatever be the true statistics of India's urban population size, the fact remains that there are enough possibilities for disaffected youth to hide out in large cities even as they scam victims.

There are signs that Indian cybercrime might be gradually upskilling. In early 2020, a Singaporean security firm revealed that in a cache of 461 976 payment card details being offered up for sale on the darknet, 98% of the potential victims were Indians. The stashed information was estimated to be worth US\$4.2 million on the illicit data market.¹² From published reports, it is unclear whether the data was acquired by Indian or non-Indian hackers, but the former possibility cannot be dismissed outright. This is because, even as the Indian call-centre industry has faced challenges from Western protectionism, increasing numbers of IT graduates are entering the country's start-up sector.¹³ Unfortunately for them, aspirations of becoming the next Bill Gates or Steve Jobs have remained

fantastical, as fledgling IT businesses are ground down by excessive governmental red tape.

For a large number of these graduates, start-ups are anyway viewed as a mere finishing school to hone their trade. The gold standard of professional (and social) achievement is to land a full-time, stable job at a multinational company, preferably overseas. Most IT workers leave start-up jobs within two years, during which time they deliver sub-par performance because they are constantly scouting for new opportunities anyway.¹⁴ Should the desired roles fail to materialize – either owing to difficulties with obtaining foreign work permits or competition in an overcrowded Indian job market – some computer programmers turn to criminal hacking or online scams.

One recent trend is to use search engine optimization to ensure that Google searches for customer care numbers in the banking sector show false results. The numbers that are most prominently displayed are not those belonging to genuine help-lines but to fake call centres operated by scammers. Since people calling such numbers usually are under some psychological pressure or distress about prior banking transactions that have failed to occur, it is easy for the scammers to elicit confidential information out of them. This information is then used to withdraw money from the caller's bank account.¹⁵

Methodology

Sources consulted for this paper range from academic articles on methods of cybercrime, to media reports from India and elsewhere. As the paper was being prepared, a 10-part Netflix series about online scamming in India was aired. The series thrust awareness of low-tech cybercrime into the public domain, more than any textual publication could hope to achieve. It showed how scams target not only foreigners, but also Indians (a point that readers of this paper may wish to bear in mind).

To study the ecosystem in which cybercrime has evolved, the researcher examined a total of six years of media reports, between 2012 and 2018, from two Indian current-affairs publications, *India Today* and *Frontline*. Between them, they provided glimpses not only of how the IT and ITes industries

were running into difficulties in an increasingly protectionist global economy, but also how India's own failure to invest in quality education for its youth was creating a massive unemployment problem. The work of journalist Snigdha Poonam, as encapsulated in her book *Dreamers: How Young Indians Are Changing Their World*, brought home how some of these youth were concocting fantasies of rapid wealth generation, which were disassociated from their everyday reality.

The report aims to synthesize these disparate narratives, with an analysis about types of cybercrime and the state of the Indian digital economy, into a single story. In doing so, it attempts to provide a better understanding of some of the mechanisms behind the rise of cybercrime in India. It is divided

into two parts. The first provides a general overview of cybercrime literature, including ethnographic studies about the methodologies and motives of different kinds of cybercriminals.¹⁶ The second part examines the evolution of cybercrime in India and the factors that have fuelled its development as a dark side of globalization. The paper concludes with a brief set of policy

Social engineering (or scamming) by telephone is the favoured technique of Indian cybercriminals.

recommendations for developing-world countries, which are likely to face growing risks from cyber-enabled crime.

Scope of research

There are two questions about cybercrime that are often hinted at and sometimes openly discussed but whose answers prove elusive:

- Is cybercrime 'organized', in that it is controlled top-down by larger criminal syndicates, much like large-scale human trafficking or drug smuggling? Or is it a bottom-up, illicit entrepreneurial activity engaged in by technically qualified people who operate autonomously?
- Are there unique characteristics of cybercrime that distinguish it from traditional forms of (offline) criminality, as well as cyber warfare and cyber espionage?

Using India as a case study, this paper attempts to provide some value-added insights that help answer the questions above, being careful not to promise categorical answers. What emerges is that cybercrime has a degree of organization, but – with the notable exception of Eastern Europe – this does not seem to originate from recognized mafia-like entities.¹⁷ Instead, the structure of cybercrime mirrors that of legitimate businesses, with the main difference being that it features a combination of deception, theft and/or extortion, albeit without an accompanying threat of physical violence. 'Social engineering' (or scamming) by telephone is the favoured technique of Indian cybercriminals. Their activities are individually rationalized as necessary adaptations to the pressure of living in an unpredictable job market where dishonesty is not just the fastest but perhaps the only route to financial stability and improved social status.¹⁸ They see themselves as either innovative entrepreneurs or victimized wage-earners, but not as lowly criminals preying on the vulnerable.

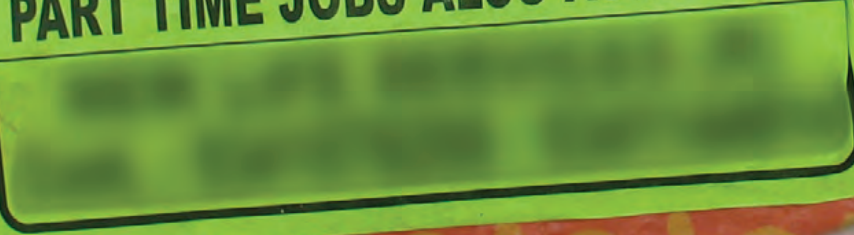
Although cybercrime is entrepreneurial, it also needs to be part of an underground ecosystem if it is to endure – an ecosystem that trades in data, as opposed to violence and protection. Cybercrime 'organization' is limited to two components. First, the sale and resale of computerized information obtained by hackers or by rogue employees of a business or financial institution and then marketed through online forums or in person; and, second, the laundering of criminal proceeds through front companies and bank accounts set up under false identities.

These two components remain challenging areas to research, with journalists and academics struggling to understand just how illicit data markets operate and how online frauds are cashed in. Their task has been complicated by the fact that in certain highly sophisticated cases of cybercrime that did not involve social engineering, such as when the Bank of Bangladesh lost US\$81 million through a hack in 2016, state actors from a foreign power may have been involved.¹⁹ In an international system where the Chinese model of state-led capitalism is gaining credibility through infrastructure projects, the boundary between government and private commercial interests is being blurred.²⁰ This also has the effect of eroding any distinctions between economic espionage (conducted by state actors) and industrial espionage (conducted by private companies). When an ostensibly private entity uses cyber technologies to steal trade secrets across international borders, it is now becoming harder to say whether it is a cybercrime that has been committed or an act of peacetime spying on behalf of a foreign government.

WANTED

Fresh or Exp. Receptionist, Clerks, Office Assistant,
Accountants, Administration, Computers,
Office, Delivery Boys, Technical, Counter Sales, Field
Investigators, Stewards, House Keeping, Engineers,
Security Guards / Supervisor, Collection, Helpers, etc.

CALL CENTRE / BPO EXECUTIVES M / F
PART TIME JOBS ALSO AVAILABLE





DISTINGUISHING BETWEEN CYBER-DEPENDENT AND CYBER-ENABLED CRIME

There seems to be a trade-off between two kinds of cybercrime, the one cyber-dependent and the other cyber-enabled. *Cyber-dependent* crime occurs when technical penetration of an individual computer or a network of computers is integral to the commission of the crime; in other words, the crime would not be able to happen without this penetration. *Cyber-enabled* crime occurs when the scale of criminal activity is greatly increased by computer technology, but the actual crime is a variant of existing criminal behaviour; scamming would fall into this category.²¹ Also, cyber-enabled crime is rampant in the physical world (one need only think of street con-artists), but has been enlarged in geographic scope and in the size of potential profits thanks to online markets.

The trade-off is due to the fact that contexts that see higher levels of cyber-dependent crime (such as advanced economies and countries with high levels of computer literacy) are also those where a greater awareness of cybersecurity exists among ordinary computer users. There is therefore less scope in these contexts for unsophisticated online scams to be successful. In contrast, when a country offers low yields from cyber-dependent crime (owing perhaps to a weak currency and/or limited household earning potential), there is greater room for deceiving unaware internet users through cyber-enabled scams. India is particularly vulnerable in this regard, with new digital payment systems being introduced to reduce the amount of untaxed or 'black' money

- ◀ During the early 2000s, India's IT industries derived 60–70% of their contracts from North America and Europe. This led to a wave of recruitment for work in call centres.

© Flickr/Paul Keller

Unless cybersecurity awareness drastically improves, India could become the world's biggest target for online scams.

in circulation. While beneficial for the country and economy as a whole, e-payment technologies pose a serious hacking risk. It has been estimated that mobile transactions in the country will be worth one trillion dollars by 2023.²² Unless there is a marked improvement from 2020 levels of cybersecurity awareness on the part of Indian smartphone users, the South Asian nation will become perhaps the world's biggest target for online scams. This is because the widespread penetration of English-language devices will render India vulnerable to international cybercriminals. In contrast, China, despite its comparably huge population, would most likely be shielded by strong internet controls built on pre-existing surveillance systems, as well as having a more inaccessible language.²³

Cybercrimes have varying levels of sophistication, which help differentiate between those that are cyber-dependent and cyber-enabled. A small percentage feature absolutely no human interaction. These are executed remotely by malware and their most frequent targets seem to be the research-and-development facilities of corporate giants. Such incidents technically fall into the category of cyber espionage, but in the absence of a clear (and prosecutable) link to a foreign government, they might be classed as 'crimes'. Another kind of cybercrime is network disruption by digital hitmen. A British hacker once took the whole of Liberia off the internet while he attempted to vandalize the IT systems of a local company. His motive was financial: he was allegedly commissioned by a rival firm to do the job, but the scale of the attack exceeded his intentions.²⁴ More famously, hackers in Eastern Europe are thought to have played a crucial role in disrupting public services (especially electricity grids, banks and media outlets) during periods of inter-state tensions. Their actions could be ascribed to cyber warfare, but in the absence of clear proof of state backing, can also simply be called 'crimes'. For the purposes of this paper, it is only relevant to note that since the actions described above are predicated on gaining access to an adversary's computer networks, they are *cyber-dependent* crimes.

During the 1990s, some reports suggested that there existed seven types of cybercriminals, differentiated according to who/what was being targeted and for what reason.²⁵ Although an argument can be made that cybercrime has since mutated to become more networked, less reliant on the individual skills of a lone hacker and more integrated with above-ground structures of commerce, the 1990s typology is still helpful. It disaggregates the constituent parts of the modern cyber-threat landscape, and helps unpack the sheer range of offences that are loosely defined as 'cybercrimes'.

Such typologies help to capture the broad range of motives and competence levels that make up the online criminal community. Almost all the actors described above would qualify as 'hackers' since they need a measure of skill in breaking into computer networks. But what sets the traditional 'hacker' apart from the others is that he/she is an anachronism – hacking skills are becoming so common nowadays that the sense of personal achievement attainable through purely 'recreational' hacking is somewhat diminished. The other six actor types also have claims to being 'intelligent' and they have secondary motives (like making money) to reinforce their superior self-images.

Most cybercrimes feature at least some degree of victim participation, making it difficult to draw a clear distinction between cyber-enabled and cyber-dependent criminality. Perhaps a useful definition might be that if a crime is committed with one-off victim participation against a well-protected target, and is reliant thereafter solely on technical means, it is a cyber-dependent crime. If a measure of ongoing human interaction is present, and levels of security are poor, it is cyber-enabled.

The Indian context features a few examples of cyber-crimes with low human interaction, but the majority of offences registered in the country, or originating from it, involve extensive use of deception against a human target. The technical sophistication of these crimes is low, while the level of human interaction is high (low-tech/high-interaction). This brings one to the trade-off mentioned earlier: cyber-dependent crimes are characteristic of societies with a high level of digitization and a technologically aware population. Those who commit such crimes expect that they will have to overcome


Actor	Motive	Objective
 Hacker	Egotistical and technical	Demonstrates individual prowess by penetrating well-protected public- and private-sector networks
 Spy	Professional	Steals secrets from friendly and hostile countries for the purpose of helping own side gain a diplomatic, economic or military advantage
 Terrorist	Ideological	Undermines government's credibility by disseminating hate messages and disrupting public life through interference with critical infrastructure
 Corporate raider	Monetary	Steals information from a business entity that can be used by a rival firm for either product improvement or to inflict reputational damage
 Professional criminal	Monetary	Steals information or takes control of a computer system for personal profit, either with the aim of conducting blackmail or perpetrating a fraud
 Vandal	Egotistical and vengeful	Defaces or disrupts internet traffic to a website for the sole purpose of individual gratification
 Voyeur	Egotistical and sexual	Breaches the privacy of another individual or several individuals to satisfy a personal obsession

FIGURE 2 Seven categories of cybercriminals

strong suspicions and make many attempts before they can smooth talk or phish their way into a victim's bank account. So, they rely on a technology-heavy approach with minimal human interaction. They conduct research into the psychological and technical profiles of their anticipated victims, as in the case of Tecnimont SpA, to score an instant success.

Cyber-enabled crimes, on the other hand, (with the exception of online child sexual exploitation, for example) usually depend on the susceptibility of their

victims to being deceived.²⁶ The less advanced the level of digitization in a society, the easier it is to defraud people who have only recently purchased a smartphone or computer but have little understanding of how it could compromise their private information. Such crimes are less discriminating and adopt a mass-based approach in which the perpetrators make multiple synchronized efforts to defraud victims, aware that only a small percentage of these efforts need to actually pay off in order to turn a profit.



पवन हैयर ड्रेसर्स
मास्टर किशन लाल

THE DIGITAL UNDERGROUND ECONOMY AND NETWORK TYPES

An estimate from 2018 held that cybercrime generates US\$1.5 trillion a year worldwide, of which more than half (US\$860 billion) comes from illicit sales online, while another US\$500 billion comes from theft of intellectual property and a further US\$160 billion from data theft. Interestingly, ransomware was thought to account for the comparatively small amount of US\$1 billion in the digital underground economy.²⁷ If accurate, these figures would suggest that espionage against industrial and scientific assets is an enormous cybercrime threat. This raises the question of whether such activity is tacitly encouraged by some state actors as a way of boosting their own research and development efforts.

Concerns are particularly focused on China, with one observer stating in 2020 that Chinese intelligence agencies had over a five-year period built a more comprehensive database about the US and its capabilities than any country in history had possessed about a possible adversary. This vast pool of information had been partly obtained by hacking into personnel files of American citizens. (Although too large to be sorted by human methods, with the development of artificial intelligence and facial recognition technologies, it would also be possible for Beijing's spy-hunters to use such data to identify American covert operatives through analysis of travel patterns.)²⁸

Studies suggest that there are two kinds of cybercriminal networks, distinguished by size. Small networks usually have a fluid membership, relying on hired technical expertise as and when needed.²⁹ Those that are large and bureaucratized have a clear leadership structure and are more gang-like. But even these do not match the conventional idea of mafias, as they do not trade in physical violence. As a general pattern, it seems that large and multifaceted cybercrime operations have three

- ◀ **Telephone scamming is prevalent in India: a form of low-tech, high-interaction cyber-enabled crime that draws on the use of stolen customer data.**

© Andrew Caballero-Reynolds/AFP/Getty Images

A factor that contributes to bridging the differences between cyber-dependent and cyber-enabled crime is the emergence of so-called botnets.

components, each of which is responsible for a single step in the process of victim exploitation: an upper management or core leadership with experience of financial crime and money laundering; a middle rung, consisting of professional and recruited 'enablers', who respectively provide technical and informational support; and a lower rung of 'foot soldiers', who handle the operation's external interface. Members of this last rung could be 'money mules', who physically help launder the proceeds of cyber-crime for a fee, or they could be call-centre employees who mollify angry customers by reading off prepared client-support scripts.

Aside from professional enablers – computer specialists who steal data remotely – other members of the operation do not need particularly advanced computer skills.³⁰ The core leadership has to manage administration and the movement of large funds; the recruited enablers need to steal information that cannot be obtained through digital means and the foot soldiers only have to do whatever little they have been told to do.³¹

These three layers serve to blur the boundary between cyber-dependent and cyber-enabled crime, by allowing the latter to assume a degree of penetration that was previously an exclusive characteristic of hackers. Another factor that contributes to bridging the differences between cyber-dependent and cyber-enabled crime is the emergence of so-called botnets. These are networks of computers that have been hacked into and taken over without their users' knowledge, and can be used to send out phishing messages, post advertisements, steal data or engage in disruptive attacks against digital infrastructure. Botnets can be created through malware, which in the more advanced cases can simply enter a computer under the guise of a routine software update without any action taken by the user. Less sophisticated botnets rely on social engineering to trick users into installing the malware. In either case, the compromised devices are controlled by a human 'botmaster' who can then rent them out for specific tasks. The cost of hiring a botnet is as low as US\$0.10 per computer.³²

With this new intermediary technology to facilitate contacts between high-skilled hackers and low-skilled scammers, the entry barriers to sophisticated cyber-enabled crime have come down. An August 2019 press report stated that India had been under attack from botnets originating in Central Europe (primarily the Czech Republic, Poland and Slovenia) but controlled from South Asia, most likely Pakistan. The fact that these botnets targeted military installations suggests that a hostile intelligence service might have subcontracted European botmasters to create a false digital trail that masked a classic cyber espionage effort.³³

The overall size and diversity of the digital underground economy was well articulated by one British law-enforcement official:

[I]f I wanted to get involved in phishing a bank or something that everybody knows, but I don't know how to write the actual page, someone will write it for me online and reasonably cheaply I can ask them to do it. And if I'm not too sure how to host it, they'll host it for me on one of the bots for a part payment. And if I don't want to get involved in cashing out and receiving the money because that's a little bit too risky, there's guys doing cash out services all over the world who you can talk to and meet online. There's a whole community out there of thousands of people that can solve any one of the problems online or make up any link of the chain if you don't want to get involved.³⁴

The 'community' referred to here consists of professional enablers – computer experts who handle the technical side of a cybercrime operation. As for the non-technical foot soldiers, one can see how cybercrime, like many categories of offline organized crime, offers a source of additional income for people who may be primarily avaricious but also (as a secondary motive) have limited opportunities to legitimately earn sufficient cash for their needs. Professional enablers tend to gain their technical skills well before turning to criminal activity, suggesting that greed for wealth and the need for income are not always linked. Like many cybercriminals, their recourse to the illicit economy is often a result of struggling to land a stable long-term job that pays as much as they think their skills are legitimately worth.³⁵

Anecdotal evidence suggests that Eastern Europe is where cyber-dependent crime is currently at its most sophisticated. This is thanks to the Soviet legacy of a strong scientific and technological base, combined with the societal shock caused by the economic transition from communism to capitalism. The region is also where linkages between cybercriminals and organized crime are reported to be at their strongest. One source from the early 2000s asserted that:

Organised crime gangs are starting to actively recruit skilled young people into cybercrime. They are adopting KGB-style tactics to recruit high flying IT students and graduates and targeting computer society members, students of specialist computer skills schools and graduates of IT technology courses.³⁶

Although striking, these conclusions about close ties between cybercriminals and organized crime do not appear to be uniformly represented in different parts of the world. It may be that some instances of collaboration are focused on specific incidents launched on an opportunistic basis. One well-known example, from 2000, occurred when the Sicilian mafia attempted to spoof a banking website in order to siphon off European Union funds amounting to US\$400 million. (The scheme, which was thwarted by an informant, featured the participation not just of hackers but also about 20 insiders who had supplied information.)³⁷

Certainly, many organized-crime actors are likely to use IT graduates to develop secure communications and enhance operational security. But there is little evidence that they are deploying these experts to generate new revenue streams from enterprises built solely on computer skills. In other words, cybercriminals may collaborate with traditional gangsters as part of a business relationship, without themselves being subsumed into a gang affiliation.³⁸ Support for this view comes from surveys finding that cybercriminals tend to have a different mindset from the kind of career hoodlum most likely to join a gang. A cybercriminal thinks of him/herself as more brainy than brawny. Those who go to jail, according to this mindset, are dumb for having been caught;³⁹ this differs from the ranking process in gangland hierarchies, where prison time is seen as a sign of machismo and street credibility.

Cybercriminals may collaborate with traditional gangsters as part of a business relationship, without being subsumed into a gang affiliation.



Together We Can Fight False Information

Here are some easy tips to help you decide if something sent to you on WhatsApp

Understand when a message is forwarded

Starting this week, we're rolling out a new feature that lets you see which messages have been forwarded. Double check the facts when you're not sure who wrote the original message.

Check information that seems unbelievable

Stories that seem hard to believe are often untrue — so check elsewhere to see if they are really true.

Check photos in messages carefully

It is easier to believe photos and videos, but even these can be edited to mislead you. Sometimes

2

Question information that upsets you

If you read something that makes you angry, ask whether it was shared to make you feel that way. And if the answer is yes, think twice before sharing it again.

4

Look out for messages that look odd

Many messages containing hoaxes or fake news have spelling mistakes. Look for these signs so you can tell if the information is accurate.



And check links too

It may look like the link to a well-known website

THE STRUCTURE OF CYBERCRIME ENTERPRISES

A large-scale cybercrime enterprise provides a good illustration of how legitimate and illegitimate components of a business model can mix, with the former covering up for the latter. During the first decade of this century, one such enterprise, Innovative Marketing Inc (IMI), which originated from the United States, became a prototype of the kind of online scams that are now growing increasingly widespread in India.

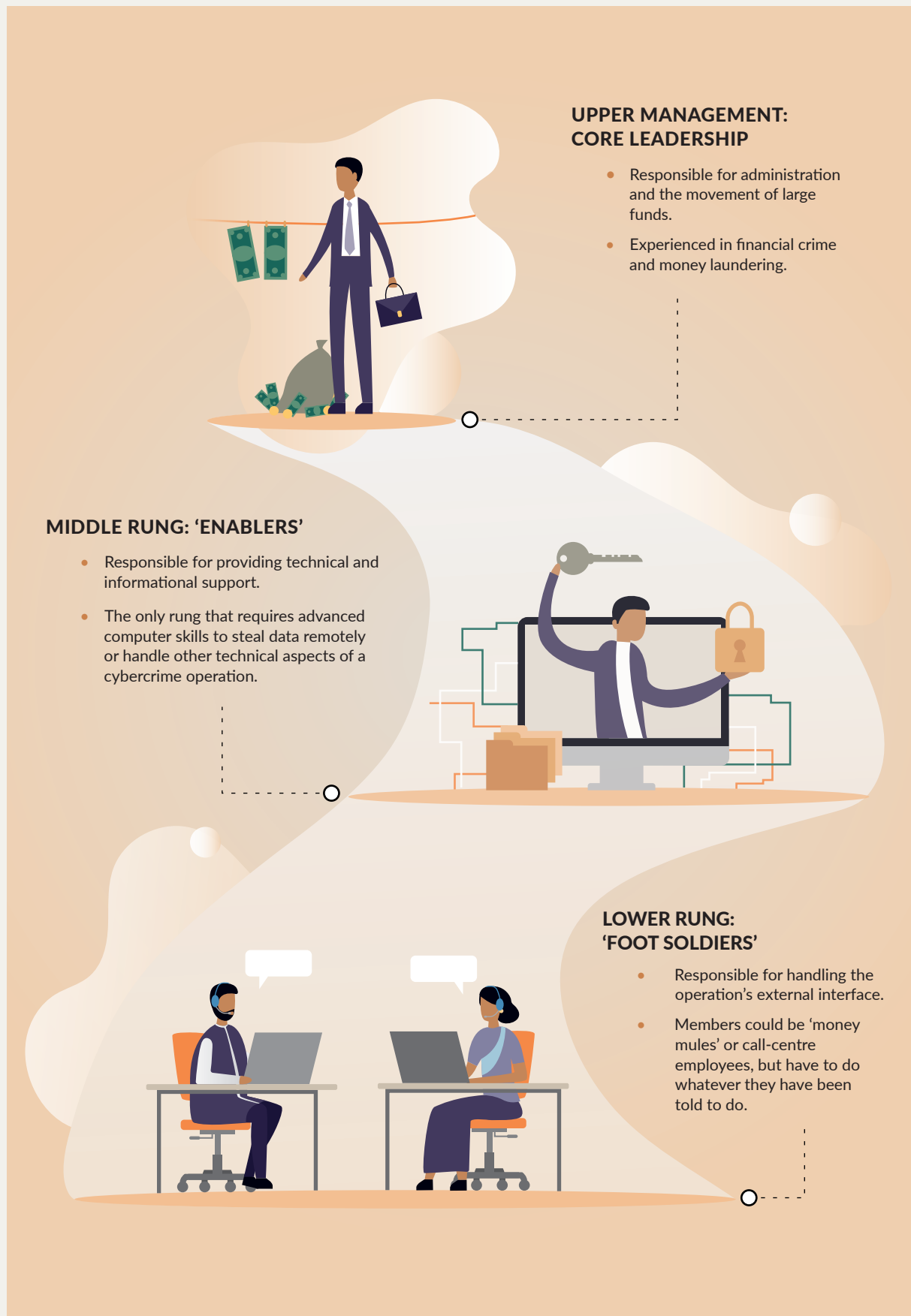
The case of IMI is similar to what later transpired in one of India's biggest call-centre scams, the Mira Road scam (discussed later). Like Ukrainian programmers who worked for IMI, some of the Indians working in junior capacities for call centres that scam Westerners may not know that they are part of a criminal enterprise. Even if they have their suspicions, they keep silent about these and prefer not to seek clarifications that could potentially threaten their source of livelihood. A cybercrime operation that is multi-layered, with different levels of awareness and culpability, fits with what researchers have discovered about the global trade in data: an entire 'parallel economy' exists to service scamming. The division of labour between different functional specialists occurs here just as it does in legitimate businesses. In 2019, law-enforcement agencies across Eastern Europe broke up a network called GozNym, named for its use of a combination of Nymaim malware and the Gozi ISFB banking trojan.⁴²

Although police spokespersons described GozNym as a consolidated entity, some of its members appear to have been freelancers recruited through online chat forums. The main trait they shared was their use of the Russian language. But that in itself did not imply centralized control. It seems that those arrested had worked according to a loosely structured model, behaving more like external consultants than gang members. That being said, many network members still remain at large, so the complete picture on GozNym is not yet clear.

- ◀ New digital users are particularly prone to cyber-enabled scams. In India, this vulnerability is heightened by the widespread penetration of English-language devices.

© Prakash Singh/AFP via Getty Images

The hierarchical structure of a large cybercriminal network



A binary mindset: The case of scammer Sam Jain and IMI

Since his youth, Shaileshkumar 'Sam' Jain had had a propensity to play fast and loose with ethics. As a US immigrant of Indian origin, he looked different and perhaps experienced discrimination. His associates would later describe him as having a binary worldview on life: 'Screw or be screwed.'⁴⁰ At the age of 21, he was caught trying to open a bank account using false identification papers.

After this less-than-promising criminal debut, in the early 2000s he began running a number of petty scams, some of which played out online. One of these got swept up on a rising wave of post-9/11 paranoia and propelled Jain to the heights of the Federal Bureau of Investigation's wanted list.

It was 2003 and computer users were increasingly worried about virus attacks. Jain partnered with another internet hustler, Daniel Sundin, to set up a company that marketed fake antivirus software. It was a networked operation based out of the United States, Argentina and India. The administrative hub was Ukraine, a country that had a strong educational base in mathematics and science, and a skilled labour force. But the economic difficulties the country had been experiencing since the end of communism meant that its working-age population were starved for work. Jain and Sundin coordinated the activities of their company, known as Innovative Marketing Inc (IMI), almost among the company's leadership. The line employees, meanwhile, ranged from Ukrainian computer specialists looking for interim employment to Indian call-centre staff looking for any employment.

IMI used pop-up advertisements to falsely inform users that their computers had been infected, and to peddle 'antivirus software' (actually malware) that then did infect the computers, causing them to slow down significantly. To deal with the inevitable customer complaints, since victims had paid good money for the dud software, the company used 'tech-support' call centres to talk exasperated customers into uninstalling all other (genuine) antivirus software that might be on their systems. It was a self-perpetuating scheme:



Sam Jain masterminded a software scam that would generate an eventual revenue of US\$180 million. © fbi.gov

with the bona-fide virus protection removed and a fake version installed, computer users no longer received alerts that viruses had entered their systems. They mistakenly thought that the IMI product had finally begun working as it was meant to, when alerts stopped coming. The elaborateness of this scheme meant that IMI sold over a million fake software packages across 60 countries, and in its final year of operation had revenue totalling US\$180 million. Hackers were paid US\$0.10 for each computer they compromised, while IMI generated sales worth between US\$2 and US\$5 for every one of those machines. If these amounts seem small, it must be remembered that the key to the operation's success was its size – potentially, the entire globe was its market.

Jain and Sundin became fugitives in 2009 and 2010, respectively, and most of their former employees – at one point numbering in the hundreds in Ukraine alone – drifted into new jobs. Later, reflecting on this period in his life, one of the employees said: 'When you are just 20, you don't think a lot about ethics. I had a good salary and I know that most employees also had pretty good salaries.'⁴¹ It seems that IMI compartmentalized its activities to such a degree that many of its computer programmers did not know for sure if they were part of a criminal enterprise, and if they suspected it, they may have avoided asking questions.



THE DAWN OF THE CYBERCRIMINAL

To understand why individuals with advanced computer qualifications might turn to crime, it is helpful to examine research from a different field. In 2016, a landmark study sought to explain why large numbers of engineering graduates participate in Islamist movements. The study points out that until the 1970s, many Middle Eastern and North African economies had been experiencing strong consumer-led growth. This began to stagnate at the same time as mass education devalued the employment potential of a university degree.

Particularly hard hit were engineering and medical graduates, who had enrolled for such programmes partly because of the prestige they expected to find in lengthy and stable careers. Although public discourse still held engineers to be the technocratic vanguard of national development, in practice social mobility was massively diminished by labour oversupply. A disconnect appeared between what engineering students aspired to become after graduating and what they actually became: underemployed labourers. They watched as their much-anticipated place at the helm of society was usurped by businessmen in increasingly privatized and unequal economies. This combination of high aspirations and deep disappointment proved toxic.⁴³

During the 1990s, a similar trend unfolded in Eastern Europe. The shock of privatization, coupled with a financial crisis in Russia in 1998, meant that many state-educated IT programmers were unable to find decent-paying work in societies that suddenly respected wallets rather than brains (or, more accurately, believed that the two should go together). Working for an organized-crime group could yield a salary 10 times greater

- ◀ In India, the legitimate job market for IT skills has not been large enough to absorb new talent. This led to a toxic combination of high aspirations and deep disappointment, and prompted some workers to seek employment with illicit enterprises. © Adobe Stock/Dirk70

*The complicated status
of IT workers showed
how many working-
class Indians resented
Western prosperity
even as they yearned
for a slice of it.*

than what the legitimate cyber industry could remunerate.⁴⁴ Rising costs of urban life made it almost irrational to resist the temptation. Eastern Europe at the time had no equivalent of America's Silicon Valley to absorb its talent, nor would the limited English-language skills of computer experts from this region permit them to seek work in the US.

The 1998 financial crisis drove East European hackers to monetize their skills. The strong industrial and manufacturing base of the former Soviet bloc had already given them a technical education. (Indian computer programmers would later struggle to attain the same level of competence due to the more rudimentary agriculture-dominated economy of South Asia.) During first decade of the 2000s, a view emerged in the global cybersecurity community that Russian-language speakers were the most sophisticated and talented hackers.⁴⁵ And they were better at generating revenue from their activities than cyber offenders elsewhere in the world.⁴⁶ Perhaps this was due to the simultaneous rise of violent and white-collar organized crime in the Russosphere and the creation of new money-laundering opportunities. Some reports speak of specialized training institutes where youngsters were taught how to penetrate cyber defences.

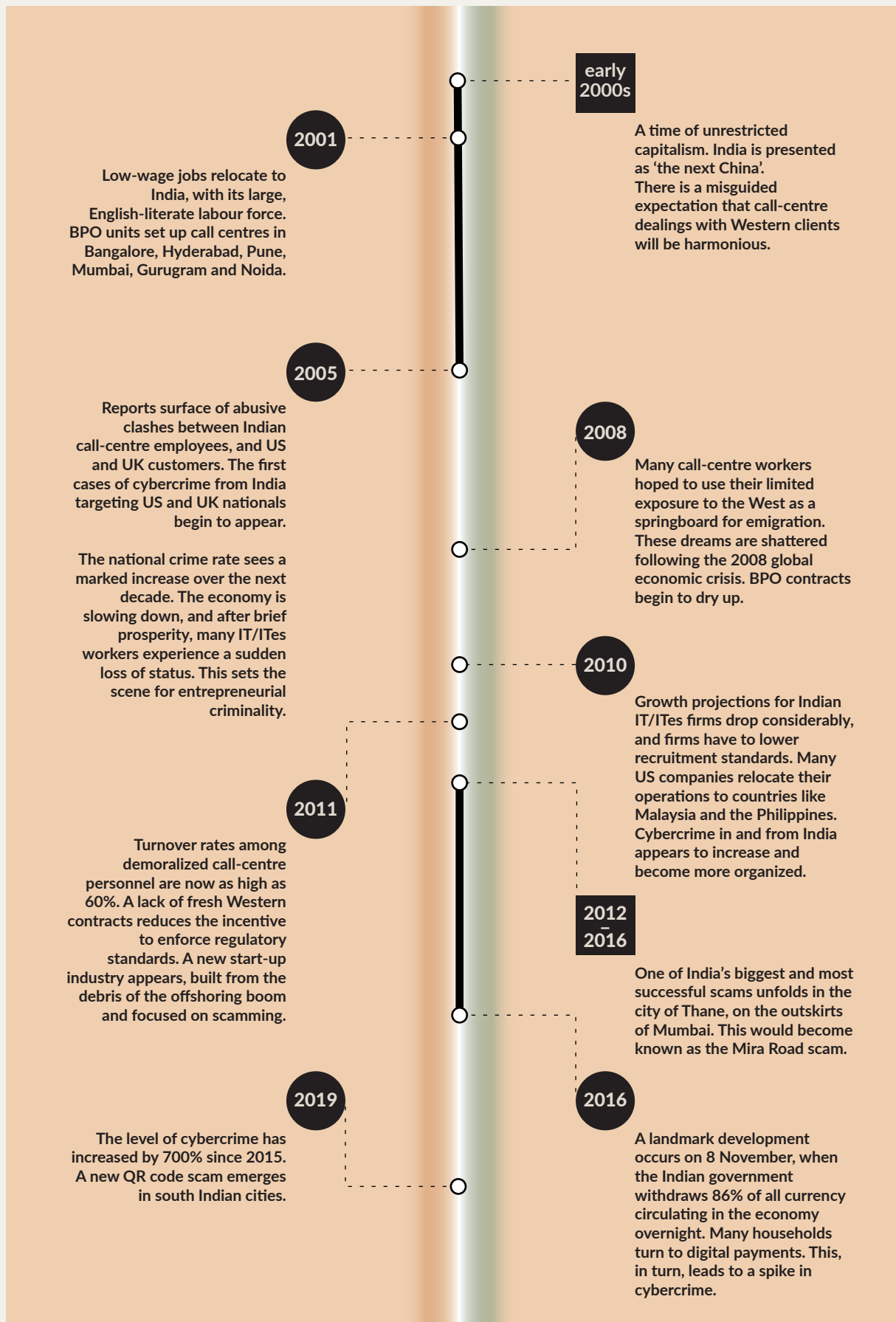
A culture of competitiveness grew, encouraging those with advanced knowledge of computer science to take apart Western IT systems, understand how they worked and adapt the operating principles to work with Soviet-era technology. One can perhaps see how, as East European countries rushed to catch up with Western living standards, IT skills were considered a shortcut to administrative and economic progress.

A similar but more rudimentary process unfolded in India, where the government encouraged private ownership of mobile phones as a way of skipping over the creation of landline telecommunications infrastructure.⁴⁷ When this mobile telephony was technologically upgraded in the 2010s with the introduction of smartphones and internet data services, lower living standards collided with online imagery of opulent (foreign) lifestyles.⁴⁸ A ferocious appetite for the consumerist 'good life' enjoyed by Western societies was triggered in a country still underdeveloped in terms of scientific achievements and corporate governance.

Even the technology that enabled virtual glimpses of the West – technology that included social media – had not been developed within India but was itself a Western import. Such realities did not matter, however: once the hunger for wealth had seeped into various strata of Indian society, just as it had in Eastern Europe with the decline of communism, any method of satiating it seemed justified. As one British commentator observed, 'A generation [was] coming of age that combine[d] the cultural values of the traditional Indian family with the life goals of the American teenager, "money and fame"'.⁴⁹

Perhaps one of the best examples of how many working-class Indians resented Western prosperity even as they yearned for a slice of it, was the complicated status of IT workers within Indian society. The 'techie', as both IT and ITes workers were loosely called (regardless of their individual skill sets), represented an aspirational standard in terms of income level, but not moral values. 'Techies' were associated with 'Westernization', a corruption of an otherwise 'pure' local culture.

From call-centre boom to India's season of scams



Up to 75% of India's engineering graduates might be unemployable due to the poor quality of their training.

A 2017 Bloomberg article described how the mainstream English-language press in Bangalore, India's main IT hub, focused on running voyeuristic stories about the domestic misfortunes of IT workers:

Techies arriving from across India are assumed to be more interested in the Western lifestyles of the modern workplace than the local culture of their new city. They tend to live away from their parents, drink alcohol, spend money freely, travel abroad, keep strange hours (because they work on the schedules of U.S. and European clients), and choose 'love marriages' over traditional arranged ones.

Someone who suspects tech workers of immorality would find plenty of grist in the newspapers, where techies are frequently killing their spouses and having affairs. Such stories sometimes implicate the victim in his fate. An article might note, for example, that the parents of a woman whose techie husband killed her had disapproved of the marriage, or that a techie killed himself after a 'trivial' argument with his wife.

Taken together, the stories can read like morality plays. They assuage a reader's envy by suggesting that a tech worker's material wealth conceals a deeper poverty. 'If a techie can commit suicide or kill his own wife,' said Sahana Udupa, a social anthropologist who previously worked as a journalist in Bangalore, 'it says something about the stress, something about the depression, something about their loose morals.'⁵⁰

Being caught between admiring the West's material achievements and detesting its supposed immorality is not a uniquely Indian malady. It can be found in societies from Africa through to East Asia. But what is unique about India is the country's size and importance to the global economy. Whether India succeeds or fails in meeting the expectations of its working-age population will be crucial to international affairs. A workforce of 500 million frustrated by job insecurity and overseas protectionism would retreat into conservatism, making the world, in the words of one commentator, 'a darker, more angry place'.⁵¹ Should the same country empower its youth to build the 'world's first bottom-up digital economy', by incubating a start-up culture and upskilling labour, it could provide a template for other developing countries to follow.

Wherever the legitimate job market for IT skills has been large enough to absorb new talent, countries have been able to reap the positive effects of globalization. When that market has been too small, the same globalizing process has prompted some workers to seek employment with illicit enterprises. One of India's worst developmental failures has been its inability to create a strong manufacturing base to absorb surplus manpower from the agrarian sector. Less than 3% of the Indian workforce is trained in any kind of vocation, compared to averages of 60–70% in the developed world.⁵²

A stop-gap measure has been to encourage higher education, undertaken at a student's own cost (actually, the family's cost), in the hope that this would lead to an increase in human capital. But all it has done is compound the potential threat to law and order by creating a pool of 'educated unemployed'. Despite the large number of Indians investing in university degrees, especially in engineering and IT, estimates suggest that 75% of engineering graduates in the country might be unemployable,



There is a view in India that IT companies are built on recognition of individual merit rather than political connections and family ties. A professional affiliation with the IT sector is still perceived as a sign of success for many working-class Indians.

© Shutterstock/Catalin Lazar

due to the poor quality of their training. With IT graduates specifically, that number rises to an alarming 94%.⁵³ Fewer than 5% can write intelligible computer code, which is a prerequisite for a programming job.⁵⁴

All of this means that India is struggling to get out of the lower end of both the legitimate and illegitimate digital economy, where it has been trapped by poor-quality education.

Technology-driven and knowledge-based superiority

Across cultures, hackers seem to feel intellectually superior, both to other criminals and to society in general. They usually earn 10–15% more than traditional criminals.⁵⁵ Many feel a thrill from engaging in online activities that are not just illegal but also require innovativeness. Protected by distance and anonymity, they view law enforcement with contempt.

Since cyber-dependent crime in particular can be committed with little or no direct communication with a victim, perpetrators are often confident that investigators

will have a hard time locating them. Such confidence is based on more than just the inherent complexity of long-distance police work that crosses national jurisdictions. In Eastern Europe, some law-enforcement communities are not particularly cooperative with their Western counterparts in investigating cybercrimes, partly due to a lack of resources and partly due to political tensions. The impact of these crimes is in any case not felt on local economies (except in a positive way, in that money comes into the country from abroad).

Damage done is limited to foreign persons and businesses, whose protection is another jurisdiction's responsibility. There is also a sneaking sense of admiration among members of the public for high-tech but locally born cybercriminals who target 'rich Westerners'.⁵⁶

This seems to be the case in China, where being a hacker in the early 2000s commanded social respect. Perhaps because 'hacking' in itself is not an illegal activity if done with the target's explicit approval (for example, in 'penetration-testing', a process aimed at strengthening cyber defences), it is not perceived as synonymous with criminality in non-Western cultures. Furthermore, in both Russia and China, local communities of hackers are quick to align with hyper-nationalistic politics and acquire a 'patriotic' halo. The fact that they become quite vocal whenever there is a standoff between a Western government and their own endears them to their compatriots.

Some reports by cybersecurity firms and investigative journalists assert that certain intelligence services (both in the West and elsewhere) use local criminal hackers for international cyber espionage.⁵⁷ Although evidence of this is sketchy in the public domain, observed patterns of hacker behaviour point towards many advanced persistent threats (APTs) having a tacit arrangement with local law enforcement, wherein they steal foreign secrets on behalf of the government by day and run online scams for their own profit by night.

Although intelligent (surveys have found that cybercriminals are more talented than those who commit property offences, for example), cybercriminals also have a tendency towards misogynistic expression.⁵⁸ One reason for this might be the anonymity afforded by the internet. Base behaviour tends to come out on online forums, which is off-putting to females and leads to hacker communities becoming male-dominated bastions. A self-reinforcing cycle begins, with women who try to enter such forums on their own terms ridiculed as 'scene whores' and excluded from discussions.⁵⁹ The fact that the global cybersecurity industry as a whole has a low rate of female participation – estimated to be just 11% as of 2017 – suggests that women in general have not been eager to enter the field of computer science.⁶⁰ Those who have are reported to be highly competent, a factor that probably triggers insecurity in their male counterparts and feeds existing misogyny. What is true for the aboveground cyber economy is likely to be true for the underground one, with the added element of abusive language.

How a ticket to a good job became a tool for social engineering

Call centres attracted recruits who were fluent in English, seen as an elite skill in India. Yet their accent would frequently be mocked by Western clients, leading to anger and frustration. BPOs began to conduct cultural immersion and accent training, instructing employees to adopt fake identities during work hours.

Workers' dreams of emigrating to the US were crushed after the 2008 crisis and slowdown of the BPO sector. For some, the linguistic skills honed in call-centre work found new utility in 'social engineering' (or scamming) by telephone – a favoured technique of Indian cybercriminals.

Perhaps there is a tendency to release pent-up frustrations in cyberspace. In order to commit a scam a less-skilled criminal must usually masquerade as someone they are not, such as a bank manager, a company CEO or an obscure royal. Social engineering requires faking an image or a voice of authority, especially now that hardly anyone falls for a phishing email that makes a plea for humanitarian assistance. This need for keeping up a pretence may cause tensions with the physical reality in which a computer-enabled scammer lives. When linguistic barriers are added, the probability of deceiving a victim is lowered, compounding the personal stress of devising and delivering a credible pitch. Some of the wealthier cybercrime networks can overcome this problem by 'offshoring' language-dependent parts of their operation to native speakers. Thus, cybercriminals in Eastern Europe have generated immaculately written phishing emails in the languages of Western Europe. In poorer countries, such as India, however, a cybercriminal generally has to restrict himself to targeting either local victims or English-speaking foreigners, which is why most scams in the country have focused on the Anglosphere. On the rare occasions that an Indian-based cybercriminal has been documented communicating with a victim who has become suspicious, the scammer may over time show signs of frustration at his own limited vocabulary, and this frustration often comes out as invectives or threats. Facing up to the fact that his English might not have been fluent enough to fool a native speaker can shake the self-confidence integral to committing an online scam.

Yet, even as they nurse latent feelings of socio-economic inferiority and the resentment that comes with it, cybercriminals also have a sense of superiority over their potential victims. This stems from their access to confidential data.⁶¹ Whether working legally as penetration-testers for cybersecurity companies or illegally for themselves or criminal enterprises, hackers and scam-artist telemarketers can obtain information that is thought by its owners to be secure.

Not only can this information be monetized but the personal gratification that comes from having a one-sided advantage over someone else can be addictive. A study found that 14% of IT workers admitted to accessing company data for private gain. Translated into raw numbers, this would mean that approximately one million employees out of a total of seven million in the US IT sector are potential insider threats (and it must be remembered that the study only counted those who *voluntarily admitted* to misusing data).⁶² In poorer countries, such as those of Eastern Europe or South Asia, the percentage can be expected to be much higher.

Besides data theft committed by those still serving in a company, there is an even bigger risk of staff merely appropriating information when they leave for a new employer or enter self-employment. Client lists are the most obvious target. The same study cited above found that a third of those working in the IT sector admitted to having helped themselves to company data shortly before switching to a new job. This was lower than the 60% estimate reported in surveys of other industries, but it makes clear that data security is a human endeavour with scope for abuse.

The most lucrative data is government-issued personally identifiable information, such as social-security numbers in the US.⁶³ Unlike credit cards, such numbers cannot be easily cancelled and are sold online by hackers for anywhere between 25 and 100 times the value of credit-card information. Less prized but still valuable is patient

Social engineering requires faking an image or a voice of authority, especially now that hardly anyone falls for a phishing email that makes a plea for humanitarian assistance.



India is home to around 111 million people for whom poverty is a chronic, cross-generational condition. However, the real origin of cybercrime lies in the middle and lower echelons of the working class, who have few job prospects and no useful family connections.

© Shutterstock/Yavuz Sariyildiz

medical data obtained from hospital records: this costs about 10 times the price of a stolen credit-card number.⁶⁴ Much like personally identifiable information, medical records have a low perishability, while banks can quickly block suspicious card transactions (and even legitimate ones that raise automated red flags).

With an overview of the types, structure and motives of cybercrime, we can now turn to examining the specifics of cybercrime in a single country. This report has chosen India because of the large size of its ITes sector, its extreme poverty and income inequality, and the potential that these factors, combined, offer for online criminality.

Estimates portend a grim future: India is home to 28% of the world's poor and has around 111 million people for whom poverty is a chronic, cross-generational condition. Those who are chronically poor will see their children inherit the same level of deprivation, with no hope for improvement through their lives. Government schemes to alleviate such extremes of poverty have not had long-term impact, although this is not for want of effort.⁶⁵

The poorest classes in India already face such harsh conditions that they are not sources of cybercrime, since they cannot even obtain a livelihood by living off the land. The real origin of cybercrime in India lies in the middle and lower echelons of the working class, who have few job prospects and no useful family connections but are not threatened in the short term with death from malnutrition-induced illnesses. For them, fear of sliding into chronic poverty is a motivator, but the concomitant desire for



a better life (rather than merely preserving the status quo) also creates a proclivity for get-rich-quick schemes.

Studies have found that unlike job-seekers of the 1980s and 1990s, who were prepared to accept any kind of work and had few qualms about some jobs being beneath them, today's Indian youth carry a sense of entitlement. They are prepared to remain unemployed rather than accept a job that they feel does not match their educational qualifications.⁶⁶ This attitude has driven many into temporary work in the call-centre business, where they get to practise salesmanship skills as a prelude to entrepreneurship, which is increasingly regarded as a respectable way of earning a living.

Even so, it must be emphasized that the role of Indian nationals in digital crime is weighted towards that of foot soldiers and recruited enablers (data thieves who do not have the technical skills to remotely penetrate a network, but must have physical access to its systems). The country has struggled to produce quality software from its own research-and-development base.⁶⁷ Consequently, it lacks the local talent needed to move very high up the value chain of cybercrime, from cyber-enabled to cyber-dependent.

Much of what follows in this paper is a description of telephone scamming through the use of stolen customer data, a form of low-tech, high-interaction cyber-enabled crime prevalent in India.





EVOLUTION OF CYBERCRIME IN AN 'EMERGING SUPERPOWER'

One of the paradoxes about India is how little its fundamentals are understood, despite it being a very open society. But perhaps this openness is actually a hindrance to clear analysis. Superficial and impressionistic news reporting focused on the country's large metropolises shapes policy commentary, and this commentary frequently becomes unchallengeable orthodoxy. In the process, underlying trends are often ignored. During the first decade of the 2000s, India was breathlessly projected as 'the next China' and an 'emerging superpower'. A decade and a half later, such predictions have vanished, even though ground realities have remained unchanged for the most part.

What seems clear in hindsight is that much of India's 'prosperity' in the early 2000s was illusory to begin with. Rather than exports, the country was dependent on high levels of foreign investment and domestic consumption to boost its economy.⁶⁸ Meanwhile, it was unable to generate jobs for low- and medium-skilled workers, who made up the vast bulk of its labour force. In fact, between 1996 and 2001, India lost 900 000 jobs from the organized sector as a result of the weakening of labour unions. Even so, parties from both ends of the political spectrum rushed to claim credit for high rates of economic growth, which kept the focus of public debate away from a slowly mounting domestic unemployment crisis.

There was one unambiguously positive trend that propelled the narrative of 'Shining India' (a term used as an electoral slogan in 2004 before being discarded as disingenuous) – the growth of the country's IT and ITes sectors. Between 1998 and 2015, their combined share for India's gross domestic product increased from 1.2% to 9.5%. The technology sector became the country's main source of new jobs in the formal

- ◀ The 'Shining India' narrative of the early 2000s was in large part propelled by the growth of the country's IT and ITes sector. Shown here is the Bandra-Worli Sea Link in Mumbai.
© Wiki Commons



Bangalore was projected as a world-class technology hub, but also became a magnet for cyber scams. Pictured here is a World Information City campaign banner from 2005. © Flickr/Paul Keller

Bangalore: India's top cybercrime target

The first few years of the 21st century have been described as the 'go-go years' of Indian corporate governance.⁷¹ Media reportage at the time suggested that economic growth of 8–9% would be something of a new normal.

Places such as Bangalore were projected as world-standard technology hubs, with over 3 500 companies (including 750 multinational firms) based there.⁷² Interestingly, Bangalore seems hardly to feature in media reports as a source of cyber-enabled scams, but it registers the country's highest rate as a target of cybercrimes, at roughly 30 per day.⁷³ The concentration of foreign companies, as well as less 'conservative' lifestyles adopted by young workers, makes it a magnet for scams targeted at businesses and sextortion targeted at individuals. Furthermore, the city has a greater penetration of internet and mobile banking among its residents than other large cities in India, and is thus a logical focus of online fraudsters. To handle roughly 4 000 cases, the Bangalore police had as of 2018

allocated a team of just 20 constables, who between them had to conduct investigations using a single police vehicle.⁷⁴ Subsequently, manpower dedicated to cybercrime cases was substantially increased but the fact that India's most prominent IT hub had approached online criminality with such paltry resources for many years is still telling.

One reason for the dissonance between high levels of reported cybercrime in Bangalore and the (apparent) absence of a cyber-scamming industry on par with other large cities might be as follows.⁷⁵ Notwithstanding job losses in the IT and ITes sectors in 2001/2002, 2008/2009 and since 2017, Bangalore benefits from being the capital of the southern province of Karnataka, which has the lowest unemployment rate in India. Even if IT workers resident there are sacked, they can theoretically relocate to seek jobs in their home towns (if they have relocated from other parts of the country) or rely on financial support from employed family members (if they are locally based).



economy and, being urban-centric, helped to mask the financial difficulties faced by India's rural population. In 2000/2001, the American IT sector was badly affected by the collapse of the dotcom bubble. What should logically have led to a contraction of IT and ITes within India instead led to an expansion, thanks to fortuitous circumstances.⁶⁹

A displacement effect unexpectedly kicked in, with low-wage jobs being relocated from the US to India as a result of the country's even lower local wages. India had a large English-literate labour force that was starting to get some exposure to Western culture through satellite television, and this lured American companies into cutting costs by outsourcing technical and administrative support work. BPO units set up call centres in cities like Bangalore and Hyderabad in the south, Pune and Mumbai in the west, and Gurugram and Noida in the north. (The eastern part of the country was the least digitized of all regions and had a smaller role in the offshoring industry, with the exception of the massive city of Kolkata.)

Staff who worked in these call centres were not from the middle classes; rather, they were members of the English-literate urban working class who imagined that they had obtained a boost in social status because they were working for businesses that dealt with Western clients. The fact that they could converse in English (considered a sign of superior education in India) created the false impression that they were skilled workers. In reality, the only skill they had was the gift of the gab. Nonetheless, there was optimistic talk of a 'demographic dividend' – an expectation that with rising incomes and a young population, India would enter into a cycle of consumption-led growth.

As James Crabtree notes in *The Billionaire Raj*, senior echelons of the Indian IT sector have long had something of a halo constructed around them (even though rank-and-file IT workers are sometimes viewed as moral degenerates, public judgmentalism seems

Greater online exposure and the IT/ITes boom in India triggered an appetite for the consumerist 'good life' enjoyed by Western societies, including mega malls and gated communities.

© Wiki Commons

to diminish as one moves into a higher income bracket).⁷⁰ The sector has been perceived as one of the few islands of excellence in a largely agrarian economy, providing first-class services and products. The orthodox view is that IT companies are built on recognition of individual merit rather than political connections and family ties. India's dynastic billionaires, suggests Crabtree, yearn for the societal respect that their counterparts in the IT sector receive. Those who come from traditionally wealthy business families are seen as hereditary robber-barons, while those who built IT empires are seen to have risen up the ranks through personal grit. In short, to have a professional affiliation with the IT sector, or its less-prestigious cousin the ITes sector, is still seen as a sign of success for many working-class Indians. IT workers are now viewed as the developmental vanguard that engineers were in the 1970s.

India's cybercrime hotspots

Cities that have the highest association with online scamming are concentrated in the northern and western provinces of India, which have much higher unemployment rates. Prominent among these are the provinces of Delhi, Punjab, Uttar Pradesh and

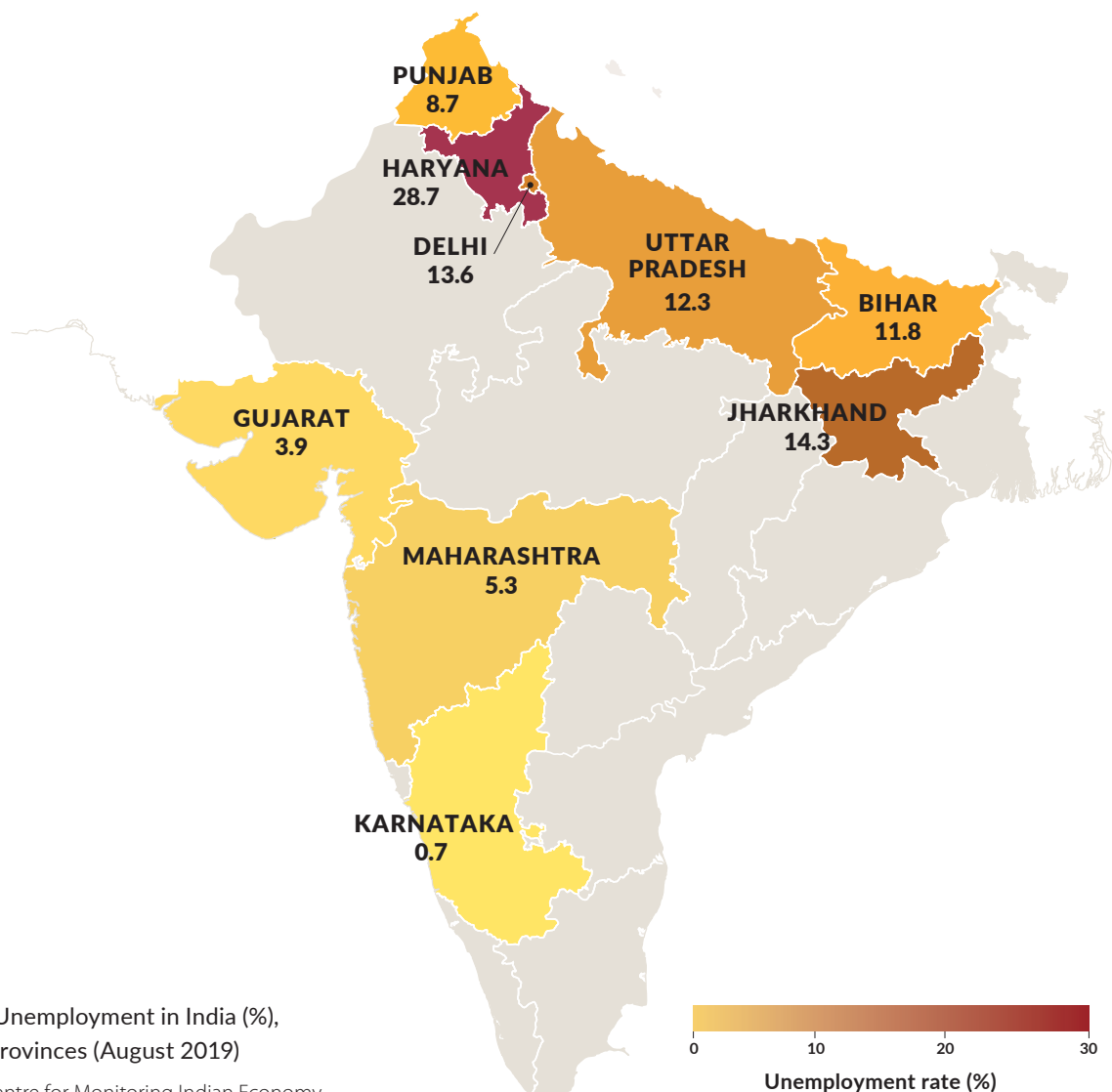


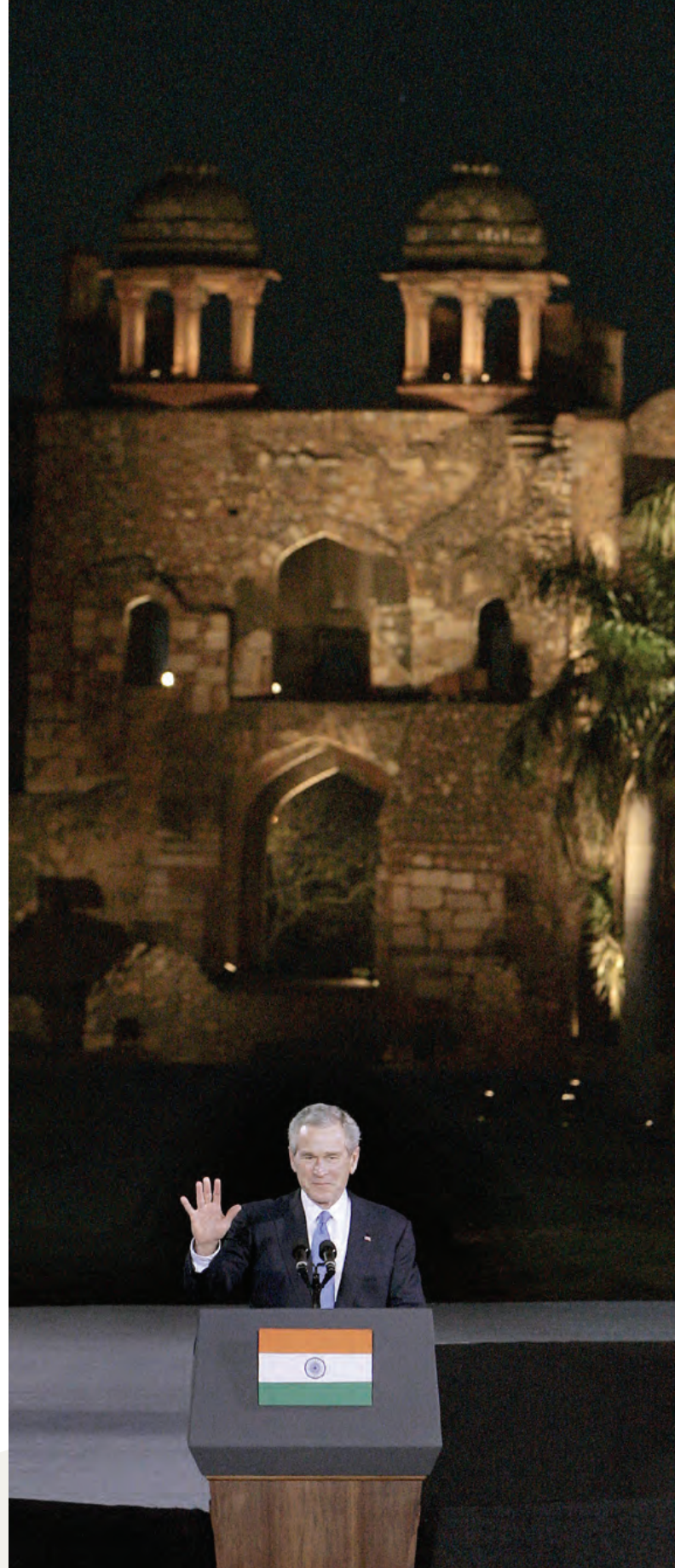
FIGURE 3 Unemployment in India (%), selected provinces (August 2019)

SOURCE: Centre for Monitoring Indian Economy, <https://unemploymentinindia.cmie.com>

Haryana. Figure 3 shows the Indian provinces from which high volumes of cyber-enabled scams reportedly originate. Karnataka is included for purposes of contrast. With the exception of Karnataka, Bihar and Jharkhand, all provinces are located in northern or western India. The latter two are located in the central-eastern region and are hubs of domestic cybercrime, targeting primarily Indian nationals.

Why are cybercrimes clustered around Delhi in particular? One reason could be the high rate of internet penetration (the region has the highest in the country at 69%);⁷⁶ another could be local culture. As one recruiter for fake call centres – those responsible for carrying out scams – told a journalist: ‘In Delhi, you can’t become an important man without pulling some kind of fraud.’⁷⁷ A third reason could be language – both Delhi and Maharashtra (a western province with a high incidence of cybercrime) are regions where much of the population speak Hindi. The latter is India’s main link language (India has 22 official languages) and thus serves as a platform for job seekers from other provinces. In contrast, southern India has more distinct provincial languages, which are harder for non-natives to learn. An out-of-town migrant who is unemployed in Delhi or Mumbai could survive on the basis of communication in Hindi, whereas a similar migrant in Bangalore would find few job opportunities as a result of the inaccessibility of the local language, and would probably be forced to return home. This means there is less of a ‘talent pool’ for scam operators to connect with.

During the early 2000s, the Indian IT and ITes industries derived 60–70% of their contracts from North America and Europe, with the US being by far the biggest source of work. In effect, the prosperity of Indian IT engineers was linked to the state of bilateral relations between New Delhi and Washington. As these relations grew more cordial (after decades of official hostility that stemmed from Cold War-era geostrategic disagreements), there were hopes and even expectations that some parts of the American Dream could become a reality for working-class Indians. For the most ambitious, it was thought that a job in IT or ITes might provide an opening for legal emigration to the US.



Former US president George W Bush delivers an address in New Delhi, 2006. An increasingly friendly US-India relationship spurred hopes of emigration to the US.

© Emmanuel Dunand/AFP via Getty Images

The call-centre boom implodes

Today, with a right-wing trend in Western democracies, such thoughts seem delusional. But the fact is that less than a decade ago the ultimate dream of Indian call-centre workers was to use their limited exposure to the West as a springboard for emigration. After interacting with trainees at an English-language course, who were hoping to then get a job in a call centre, two foreign journalists wrote:

The nature of the job [working in an Indian call centre] – the quasi-immersion in Western culture, the huge boost in disposable income, and the off-putting hours – pushes employees away from the conservative elements of their own culture. Because so many employees are young, the jobs can cultivate tastes for Western media and goods, packaged in the mega malls springing up everywhere in Indian cities ... It also makes many employees want to go to the countries they are speaking to – some just to see and finish building the image they have in their head, others to work and make new lives for themselves. Most importantly, the call centers can serve as a stepping stone. The culture shock, job stress, and cash burn out some, but a few can hurdle further up the white-collar ladder, helped by the language and soft skills that 10 hours a day of problem-solving will give you.⁷⁸

Such hopes were irreversibly deflated by the 2008 global economic crisis. When the financial disaster hit, most Indian IT and ITes companies initially expected another business windfall of the kind they had enjoyed in 2000/2001. But this time, instead of more work being outsourced to them, the flow of projects began drying up. American and British companies simply had less money to risk than before, and protectionist impulses had gripped political classes in their home countries.

The consequence for India was severe: Indian ITes firms, which had become accustomed to annual growth projections of 40% in the years 2004–2006, found themselves confronted with 6% growth in 2010.⁷⁹ Naturally, this had an adverse effect on staffing, with many newly hired personnel made redundant. In Hyderabad, where banks previously would not bother

checking the credit history of IT engineers who sought personal loans, 10% of the sector's workforce was sacked in just six months.⁸⁰ Job-hopping in search of higher salaries, once a standard practice, was no longer an option, nor were expensive nights out and parties.

Besides the economic crisis, there was another reason why the ITes sector found itself in a bad situation. During the first decade of the 2000s, there had been a misguided belief that Indian call-centre workers, being English literate, could deal harmoniously with Western clients. But in 2005, reports began surfacing of fierce clashes playing out in telephonic exchanges between Indian call-centre employees and American and British customers. Both sides had difficulty understanding each other's accents. The Indians were also accused of stealing jobs. Some reports alleged that US-based protectionist groups set up websites containing pronunciation guides to Hindi-language insults, which callers could use while speaking with Indian operators. For employees of call centres, most of whom were fresh out of college and had never before spoken with Americans, being hit with explicitly racial abuse was a shock.⁸¹ Perhaps the most infamous case occurred in 2005, when a radio presenter in Philadelphia made an on-air telephone call to an Indian call-centre and, to the apparent merriment of his studio colleagues, addressed the woman who answered as a 'bitch' and a 'dirty rat-eater'.⁸²

The fact that government ties between New Delhi and Washington (as well as with London) were fast showing signs of improvement at the time made person-to-person invectives all the more incomprehensible to those on the receiving end.irate Americans were particularly hard to deal with because they tended to be more forthright in dishing out racial insults than their British counterparts.⁸³ For citizens of a country like India, where memories of a once-grand civilization having been humiliated and robbed of its wealth by Western conquerors still persist, such a barrage of abuse was bound to hit a nerve. (According to one estimate, less than two centuries of colonialism had led to the transfer of approximately US\$45 trillion from India to the UK, a country whose gross domestic product as late as 2018 was a seventeenth of this amount.)⁸⁴

At first, the managerial staff of Indian call centres tried to instruct employees to merely absorb the insults; answering back was forbidden, as was hanging up on a rude customer (for a while, the latter was deemed a sackable offence). But high turnover rates among demoralized personnel (up to 60% in 2011), plus negative media coverage, eventually led to a stricter regime wherein some of the worst offenders could be disconnected from calls after being warned repeatedly to watch their language.⁸⁵ Even so, junior-level workers were still on the receiving end of clients' passive aggression and had to be offered on-site counselling to cope with the resulting stress.

One analysis describes the Indian call-centre industry as having re-created a colonial-style social hierarchy: abusive white foreigners were at the top, their transgressions excused or trivialized by an intermediate layer of co-opted 'brown sahibs' who were little more than slave drivers, while ordinary Indians did the donkey work without adequate pay or job security.⁸⁶ The fact that call-centre salaries, while decent, were not particularly high (slightly above US\$200 per month) in cities with relatively inflated living costs, that working hours were long, and that the job would not lead to a clear career path for employees all meant that the money earned did little to compensate for psychological trauma and long-term financial concerns. To top it off, being mocked for having an 'Indian accent' – a frequent source of irritation to Western clients –

Besides the economic crisis, there was another reason why the ITes sector found itself in a bad situation.

would have infuriated some workers who believed that merely being able to speak in English entitled them to a degree of respect from Westerners, just as it earned them respect from fellow Indians.⁸⁷

By the end of the first decade of the 2000s, much of the optimism that had initially surrounded the call-centre industry had disappeared, and the quality of personnel applying to such jobs fell. BPO firms had to lower recruitment standards, waiving the requirement that applicants have a tertiary degree.⁸⁸ Unlike the first wave of call-centre employees, this new cohort were barely proficient in English, which they had mastered just enough to land a call-centre job. With the drop in personnel standards came a further increase in customer complaints about the service quality of Indian call centres. Under pressure from their clients, many American companies began relocating their offshoring operations to other countries, such as Malaysia and the Philippines, whose populations were on average more globalized than India's, and more exposed to Western culture and speaking styles.⁸⁹ The loss of business was a further blow to India's ITes sector and reduced its viability as a pathway towards social mobility.⁹⁰

Early instances of cybercrime in India

Interestingly, it was almost exactly around the time when the racial abuse faced by Indian call-centre employees first began to be reported in the press that the first cybercrime targeting US nationals originated from India. In April 2005, five employees of a call centre in Pune siphoned off nearly US\$500 000 from four Citibank accounts held in New York.

A month later, a British tabloid revealed that its undercover reporters had been able to purchase information on 1 000 bank accounts held by UK citizens, for the equivalent of US\$5.50 per account. The seller had been an employee of an Indian offshoring company based in Gurugram.

Shortly afterwards, another company in Mumbai found that two of its staff members had been manipulating the credit information of up to 400 American customers.

These worrying developments led the National Association of Software and Services, an umbrella body of the ITes sector, to establish the Data Security Council of India (DSCI) in response. The DSCI was meant to create standards of data protection and ensure that offshoring companies adhered to this. Even so, there remained one weakness that was outside its jurisdiction: if Indian cybercriminals purchased data that was stolen from overseas by foreign-based hackers, there was nothing that could be done.

The free market had begun to enter the psyche of a young, impressionable and aspirational population.

This was what happened from the end of the first decade of the 2000s, as the effect of the global slowdown began to be felt. A new start-up industry appeared, built from the debris of the offshoring boom and focused on scamming. Using contacts that had been forged with Indian expatriates (during the early 2000s an unprecedented number of Indian students had enrolled in British and American universities and then sought jobs in the West, with mixed success), connections are believed to have been made with data thieves. Furthermore, although there is little hard evidence, it has been speculated that even Indian companies dealing with the data of foreign customers became somewhat less concerned about guarding against theft and leakage after 2009. A lack of fresh contracts from Western businesses perhaps meant that there was less of an incentive to enforce tough regulatory standards.

Most indications are that cybercrime in India originated not with out-of-work computer programmers, as it did in Eastern Europe, but with frustrated employees of the offshoring sector. It was only later, in the mid-2010s, that IT graduates started to get into cybercrime once finding jobs became difficult.

Initially clustered around large IT hubs, such as Pune and Gurugram, cyber-enabled scams spread to the countryside. The reason was sociological: as the lure of working in ITes companies diminished (especially for client-facing roles), vacant positions were increasingly filled by domestic migrants from the rural hinterland. These new employees had even fewer skills than their predecessors, but they discovered the techniques and profitability of social engineering. At a time when scams targeting Western countries were beginning to pop up in large Indian cities, migrants from rural areas were able to observe the success of telephone-based fraud. They subsequently brought these techniques back to their home towns and villages. This time, however, instead of defrauding foreign nationals, they targeted Indian citizens. The most notorious examples of copycat cyber-criminality were clustered in the district of Jamtara, in Jharkhand, a province of central-eastern India (discussed below).

The free market had begun to enter the psyche of a young, impressionable and aspirational population, but with such vaulting ambitions had not come the skills needed to stay competitive in a globalized knowledge economy. Hence, a lack of social mobility emerged similar to that currently found in the Middle East, North Africa and Eastern Europe, and a similar resentment about unmet expectations.

After interviewing several low-level employees of call centres who were likely to be engaged in illegal activity (i.e. phone scams), Indian journalist Snigdha Poonam summarized their dystopian and self-exculpatory logic in the following terms: 'As young men with no prospects, they are the biggest victims – and the whole world is a big scam.'⁹⁵

Through her investigative reports, Poonam found that the unemployment crisis in India was acute and many youths were so desperate for work that they did not bother to ask questions of a potential recruiter. They had no loyalty to their employers, and did not expect any in return. It was easy in this situation for a low-tech cybercrime industry to take root in the country, despite the best efforts of the government to preserve the integrity of data and the reputation of the ITes sector.

Cyber-enabled crime in India became a two-level business. One tier focused on targeting foreign nationals, including Indian immigrants living in Western countries;



India's streaming market is a key target for Netflix and Amazon, as shown on this billboard in Mumbai.

© Indranil Mukherjee/AFP

A season of scams: The decade after 2008

For a while, data-security efforts concentrated on disrupting the nexus between disgruntled ITes employees and 'brokers' who bought confidential files from them. The files would be sold on to any criminal groups who had a use for them. But in the early 2010s, evidence emerged that some data leakage was occurring directly to Indian business partners from US-based companies. Rather than being merely the activity of rogue insiders of Indian offshoring firms, the problem was structural. In one case, a Californian debt-collection company was sued by the US Federal Trade Commission because one of its Indian partners had misused information about American citizens to run a scam.⁹¹ The Indian company would telephone people with a history of applying for high-interest, short-term loans and falsely inform them that they were in debt and could face legal action as a consequence. Over the two years that the scam operated, its victims lost a total of US\$5 million paying off fictitious debts.

Simultaneously there occurred a steady increase in Indian media reports about cybercrime within the country, with sharp increases in the number of registered offences noticed in 2012/13. Why exactly this spurt occurred is difficult to say. One hypothesis is that it was at about this time that domestic media coverage started to focus on the issue of political corruption and crony capitalism.

A number of multi-billion-dollar scams run by government ministers in collusion with big business were exposed. One of these concerned coal mining and another, the allocation of broadband spectrum in the telecommunications sector. Between them, these two scams were estimated to have cost the Indian taxpayer nearly US\$64 billion (the figure remains speculative).⁹²

Combined with the country's economic slowdown and the loss of status that many IT and ITes workers had felt after just a brief period of enjoying good times, it is probable that the mood among disillusioned employees was ripe for entrepreneurial-type criminality. There was already an increase under way in the national crime rate, rising from 456 reported cases per 100 000 persons in 2005 to 582 in 2015.⁹³ Now epochal thefts were being committed by politicians. Taken together, these contextual factors may have cleansed the consciences of some working-class people regarding prospective involvement in non-violent, low-level scams. In any case, the unrestricted capitalism of the early 2000s had suggested, to a society that was still making a psychological transition from socialism, that there was nothing inherently wrong about using one's persuasive abilities to falsely advertise a product or close a fraudulent sale. One commentator summed up the prevailing mood as: 'If you can't beat 'em, cheat 'em.'⁹⁴



The futuristic DLF CyberHub in Gurugram houses several top IT and Fortune 500 companies.
© Wiki Commons

the other was directed at victimizing residents of India. Both involved telephonic phishing, with calls or messages sent to personal phone numbers obtained from stolen datasets. Victims were partly deceived, partly coerced into handing over money. Only the level of sophistication differed in the two tiers. Scams directed at foreigners needed to be more convincing than those targeting Indians, many of whom were (or are still) in the process of understanding the use of smartphones for online payments. The domestic target market therefore had a limited awareness of the risk of being scammed once their private information was compromised.

The fact that the Indian police would record cyber-crimes based on the location of the victim, rather than that of the perpetrator, also prevented a clear picture from emerging in crime statistics. In essence, provinces such as Maharashtra, where Mumbai is located, were shown to be cybercrime hubs, whereas the province of Jharkhand, thought to be the source of 50% of domestic cybercrime, ranked much lower. This was because

scammers based in Jharkhand were careful to avoid targeting residents of their own province so as to keep local police off their backs.⁹⁶

As a result of India's rife poverty, training for cyber-crime investigations was – until recently – a luxury that few police units in the country could afford in any substantial measure. There are horror stories of policemen bungling investigations out of sheer ignorance. According to an anecdote from 2004, a junior investigator stored diskettes that had been seized as evidence by punching a hole in each and running a string through them, as if hanging his laundry to dry.⁹⁷ Delays in the examination of digital evidence meant that valuable information was erased in the interim. Then there was the additional problem of personnel rotation: Indian government bureaucracies frequently post officers to roles for which they have no prior training or experience. A cybercrime investigator trained at considerable expense might thus have had little time to develop competence in the field before being reassigned to a completely different task.⁹⁸

The response from law enforcement

Things have begun to change slightly in the last few years, mainly in response to the spiralling rate of cybercrime offences. In 2019, India experienced a 90% increase in reported cyber offences from the previous year. Moreover, this represented a 700% increase from the level of cybercrime reported in 2015. Of course, allowance must be made for the probability that more people were coming forward to report crimes that may have otherwise gone unrecorded. Even so, such a dramatic increase suggests an overall surge in the scale of online criminal activity in India.

Bangalore was by far the most affected city, having been so in previous years as well.⁹⁹ During the period 1 January 2019 to 12 December 2019, the city recorded 10 204 cybercrimes, as opposed to 7 883 street crimes, a trend that shows how severe a threat online crime has the potential to become in India.¹⁰⁰

Owing to a backlog of cases, and a heavy caseload per officer, the Bangalore police increased the number of dedicated cybercrime stations from one to eight. (The sole police station had anyway been compelled to shut down for a few weeks in late 2019 because its computer system had not been set up to register complaints whose serial number exceeded four digits. Having never anticipated that the number of cybercrimes in a single year could cross the 9 999 mark, Bangalore's cyber-crime station had to install new software before any further complaints could be filed.)¹⁰¹

Between them, the new stations were able to dispose of 400 pending cases within 15 days. In some instances, they were unable to trace the perpetrators, partly because they were based in other provinces whose police had little incentive to cooperate in investigating offences that occurred elsewhere. (Here one can see parallels with the reluctance of some East European law-enforcement agencies to investigate scams targeting Westerners.) In such cases, the Bangalore police focused on proving that the complainants had indeed been defrauded by cybercriminals. This would be sufficient to enable the complainants to recover their monetary losses from banks and declare the matter closed, even if the actual scammers went unpunished.¹⁰²

Thus, just because a case had been 'disposed of' did not mean that justice had been served. A factor that

disincentivized investigators from pursuing cross-jurisdictional offenders was that the total cost of identifying, tracking and arresting cybercriminals far exceeded the losses borne by the victim. Especially when dealing with cybercrimes that originated from overseas, one senior police officer noted that '[t]he economics do not add up and the physical international boundaries are major hurdles'.¹⁰³

For all these reasons, the public and business corporations have had little faith in the Indian police's ability to solve acts of cybercrime. By late 2018, an average of one cybercrime was being reported every 10 minutes in India, but this statistic may well be a severe underestimate because only 10% of all cybercrimes are thought to be reported in the first place.¹⁰⁴ Being overworked and understaffed, the police, in most cases, could solve only an infinitesimal proportion of all recorded offences. For instance, there were an estimated 30 000 cybercrime complaints received by the Mumbai police between 2013 and 2019, of which just 627 were formally registered. Out of these, only 169 were solved.

Cybercrime victims, whether private individuals or corporate entities, were also frequently reluctant to report an offence.¹⁰⁵ Reasons varied from hesitation over discussing personal information with police officials (it could be embarrassing to reveal, for instance, that one had been blackmailed over intimate photographs stolen from a mobile phone) to worries about prompting investor panic.

A survey found that while most ITes firms in Gurugram had been subjected to cybercrimes, 70% of incidents went unreported.¹⁰⁶ Other studies identified a possible chink in India's cybersecurity defences: although many companies were aware of the business risks posed by cybercrime, they seemed to believe that it was the government's responsibility to mitigate these risks. They did not comprehend that their IT security was nobody's problem but their own, and that they would have to bear the costs of upgrading it to match developing threats. A paucity of low-price indigenous antivirus software, as well as an inclination to not to purchase expensive foreign-produced software, meant that an estimated 22% of computers in India have been assessed as infiltrated by some form of malware.¹⁰⁷

Smartphone scams

Even more vulnerable are thought to be smartphones, because of the fact that young Indians, in an effort to be trendy, have downloaded apps that are likely to contain malware. These types of malware help cybercriminals to access banking information when the phones are used for digital payments. Importantly, it is not clear how many of these more sophisticated attacks originated from within India and how many from abroad.

A landmark development occurred on 8 November 2016, when the Indian government withdrew 86% of all currency circulating in the economy, literally overnight. In doing so, it was seeking to expose petty and medium-level tax evaders who typically cache hard currency at home, rather than depositing it in a bank. At the time, this 'demonetization' was announced, an estimated 20% of India's US\$2.3 trillion economy was thought to consist of so-called black money generated through informal transactions.¹⁰⁸ The slow and apparently clumsy manner in which the government bureaucracy thereafter issued fresh bank notes pushed many households into making digital payments. This, in turn, led to a spike in cybercrime, both cyber-dependent and cyber-enabled.

One study published in 2019 found that 96% of those defrauded in online scams over a 12-month period had only recently started to use digital-payment apps on their smartphones.¹⁰⁹ Echoing such analysis, police in the city of Vijaywada noted that it was not demonetization per se that had increased the risk of cybercrimes. Rather, the haste with which households had turned to digital payment systems after 2016 had allowed cybercriminals to use scare-mongering as an elicitation tool.

Scammers would typically begin by trawling social-media sites for active users who put a great deal of personal information online, such as birthdays and mobile numbers. This information would then be used to build trust with potential victims, by citing it as 'proof'

The 2019 QR code scam

When it comes to mobile banking especially, a little knowledge can be a dangerous thing. During 2019, a new scam was discovered in south Indian cities, including Hyderabad and Bangalore. People who had advertised products for sale on popular e-commerce sites would receive a call from a prospective buyer. The caller would offer to pay via mobile banking, and share a quick response (QR) code over WhatsApp. What the intended victim would not know is that after scanning the code, as asked by the caller, the automatically-generated link that victim subsequently received and was instructed to click on, was not configured to receive payments but to *authorize payments*.

To ensure that the victim would not have time to get suspicious, a scammer would sometimes pretend to receive another call, which would fluster the victim and throw him or her off balance. The apparent 'disruption' would ensure that the victim would open the link hurriedly. The caller would then ask the victim to enter their personal identification number to complete the transaction. In all this, the one point that the victims would not realize is that they would not need to scan a QR code to receive payments in the first place, but only to make them.¹¹¹ This unfamiliarity with the nature of e-banking meant their loss.



that an unknown caller was telephoning on behalf of a bank and was investigating suspicious account activity. The victim would be asked to share confidential information in order to stop their account from being imminently frozen, as a part of a 'verification' process. Usually, only impoverished and poorly educated persons, as well as stay-at-home housewives with no understanding of bank procedures, would fall for this tactic. Even so, it was quite successful in a remote backwater (even by Indian standards) like Vijaywada.¹¹⁰

Over the past few years, there have been signs that India is increasingly recognized as a high-yield country for cybercriminals based overseas. In 2016, a phishing attack on a local bank led to the transfer of US\$171 million to accounts in Cambodia, Thailand, Taiwan and Australia. The choice of destination countries pointed to the attackers being from East or Southeast Asia. On that occasion, the bank's vigilance department was quick to react and the payment was reversed before it could be laundered.¹¹² However, in 2018, another bank was hit with a malware attack that allowed US\$13.5 million to be withdrawn over 48 hours in 15 000 cash-machine pay-outs spread across 28 countries.¹¹³ The pay-outs were conducted with cloned debit cards. In this case, the perpetrators are thought to have been based in Canada.

People queue to withdraw cash in Allahabad after Prime Minister Narendra Modi announced demonetization of India's 500- and 1 000-rupee notes in November 2016. Many households turned to digital payments.

© Ritesh Shukla/NurPhoto via Getty Images

More recently, in 2019, a joint operation by Nigerian and Indian cybercriminals was uncovered in which 2 500 Indian bank accounts were hacked. The modus operandi involved sending mobile text messages to potential victims, purportedly originating from tax officials offering a refund on excess taxes paid. Clicking on an embedded link would lead to a spoofed webpage that resembled the genuine webpage of the Indian tax authority. Over a multi-step process, victims were lured into revealing increasingly confidential information and then had their mobile phones hacked by a fake e-banking app, which they would unthinkingly download. The relatively sophisticated nature of this scheme meant that it enjoyed a high conversion rate of 50%: roughly half of all those who received the original text message about a refund, ended up following the deception process through to the end and lost money from their bank accounts.¹¹⁴

Less technologically advanced social-engineering schemes have relied on sheer mass to succeed. Here, one sees the real effect that the legitimate Indian ITes sector, coupled with high unemployment levels, has had on facilitating cybercrime. The main advantage for online scammers is that there are so many call centres operating in the country that creating one focused on defrauding people and hiding it in plain sight among others is relatively easy. One commentator noted that '[o]n their surface, little sets the illicit call centres apart from legitimate ones. They operate almost in the open, using the same corporate-style office spaces and recruiting from the same vast pool of English-speaking college graduates – allowing the crimes to persist for years.'¹¹⁵

Gurugram and Noida, two satellite towns on the outskirts of Delhi, illustrate this point. They are among the most prominent hubs of both genuine and fake call centres in India. Such duality shows how cyber-enabled crime cloaks its presence by hiding in the shadow of the legitimate digital economy (see Figure 4).

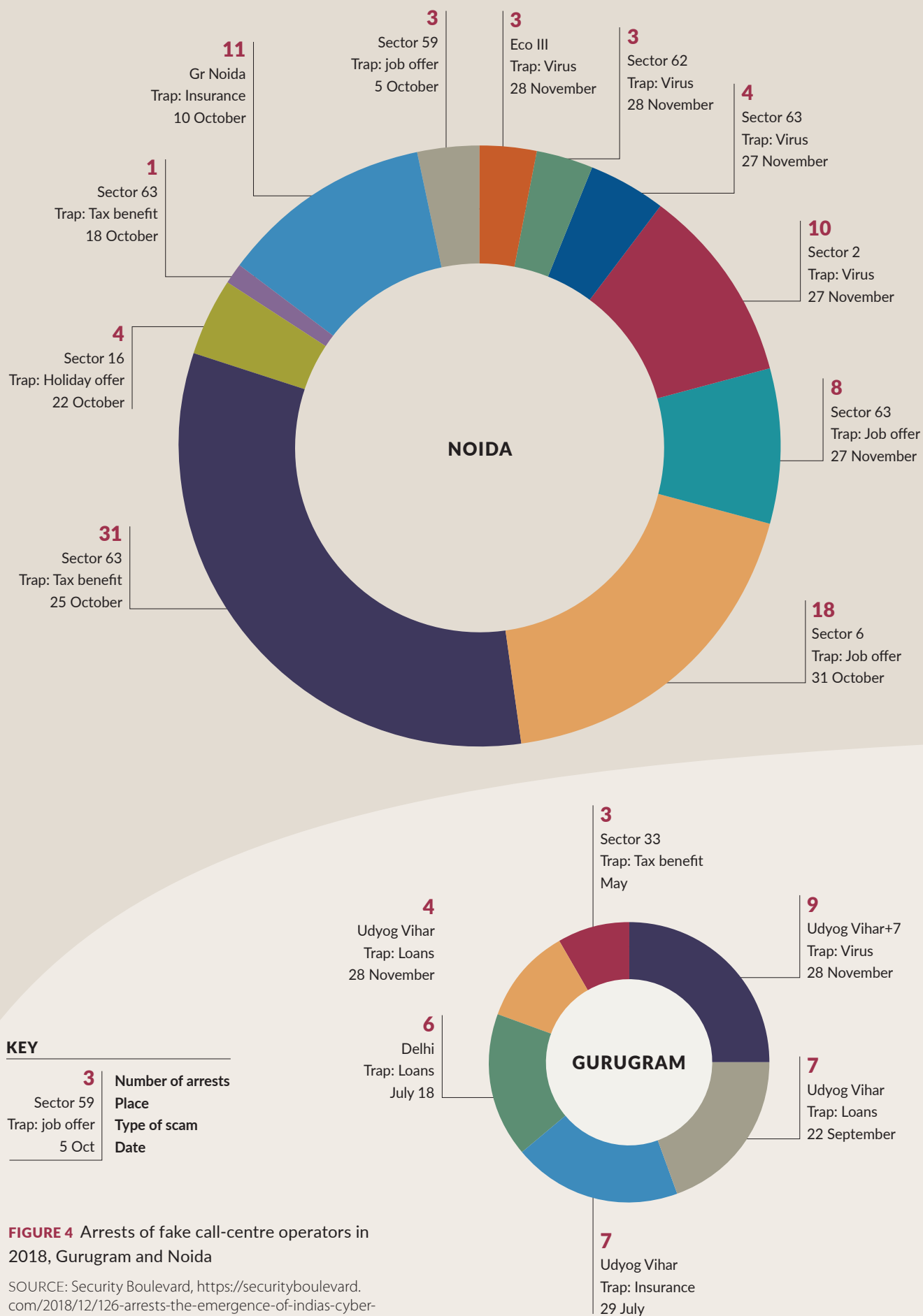


FIGURE 4 Arrests of fake call-centre operators in 2018, Gurugram and Noida

SOURCE: Security Boulevard, <https://securityboulevard.com/2018/12/126-arrests-the-emergence-of-indias-cyber-crime-detectives-fighting-call-center-scams>

जामतारा
JAMTARA





FROM THANE TO JAMTARA: DIFFERENT METHODS, SIMILAR MOTIVES

One of India's biggest and most successful scams unfolded in the city of Thane, on the outskirts of Mumbai. Known as the Mira Road scam, after the neighbourhood in Thane where most of its activities took place, it was operational between 2012 and 2016.

In the weeks after the Mira Road scam was shut down, US officials noticed a 95% drop in the number of fraudulent debt- and tax-collection calls made from India to the US.¹²³ Indian police followed up the raid in Thane with raids in the city of Ahmedabad, located in the province of Gujarat. Ahmedabad has a strong diaspora link to the US; in fact, American investigators later said that the Mira Road scam had originated from Ahmedabad, which could point to its origins lying with Indian American expatriates. In any case, the trail within India allegedly ran cold because by the time the call centres in Ahmedabad had been located and raided, all their staff and paperwork had disappeared. US law enforcement meanwhile arrested an Indian-origin immigrant for laundering money for the operation, but as far as is known, he was more of a mid-level organizer, who made a surprisingly modest amount from the scam, rather than a high-level mastermind.¹²⁴

Personnel working in Mira Road were mostly new to the call-centre business and looking to make quick money. They were paid the equivalent of US\$300 a month, plus bonuses, which is moderately higher than what might be earned in a legitimate call centre. They appear not to have thought it unusual that they were required to masquerade as American officials.

- ◀ Scammers in Jharkhand province typically target citizens living in other provinces of India. Youths from Jamtara who are engaged in cyber-enabled crime are mostly school drop-outs.
© factordaily/Pankaj Mishra



Hari Om IT Park was among the premises used for some of the fake call centres behind the infamous Mira Road scam. © *dnaindia.com*

The Mira Road scam

On 5 October 2016, 200 Indian policemen raided a building in which a large call centre was located, detaining 700 employees. Over the course of the day, 630 were released but 70 of the most senior staff were taken into custody. It soon emerged that the raid had been prompted by intelligence from the US, as well as undercover work carried out by local policemen, who discovered that the call centre was engaged in fraud that targeted Americans. Notably, the building's caretaker (who was not charged) professed his bewilderment to the media, saying: 'It looked like a normal call centre.'¹¹⁶

The Mira Road scammers had a well-rehearsed procedure, one that hinged on them posing as officials of the US Internal Revenue Service (IRS). It began with the purchase of American tax records. A press report suggests that a database containing 100 000 records was obtained for just US\$1 400.¹¹⁷ Using software known as Magic Jack, the call-centre staff would send out thousands of automated text messages to US citizens, spoofed to look as though they had originated from within the US.¹¹⁸ Recipients were warned that they were under investigation for tax evasion and that

if they wanted to avoid a visit from the authorities, they needed to call back on a certain number. Approximately 10–15% of those contacted called back, and 3–4% actually ended up making payments to the scammers. The low conversion rate can be explained by the fact that the scammers were targeting citizens of a developed country who were aware of the dangers of cybercrime, even if they were ignorant about the specific techniques and technologies employed.

For the 3–4% who were successfully victimized, the following occurred: upon calling the number provided in the text message, they were connected to a call-centre employee in Mira Road. This employee was known in the business as the 'opener' and could be either male or female. (Unlike with cyber-dependent crime more generally and cyber-enabled crime in rural India, both of which are heavily dominated by men, it appears as though urban-based call-centre scams feature a sizeable participation of young Indian women.) The opener's job was to build credibility with a potential victim, by demonstrating that she or he had access to personally identifiable information that only a government agency could possess.

The Mira Road scam would have callers posing as US Internal Revenue Service (IRS) officers. Other IRS cyber scams have used fake forms (pictured left), which look remarkably similar to authentic forms (pictured right).

Persons of immigrant origin were especially susceptible because of the threat of arrest and deportation. From the case of Mira Road, as well as other call-centre scams, it seems that the opener would speak in a fake American accent. (As a result of the racist backlash that Indian call-centre employees had faced in the first decade of the 2000s, many had been provided with accent training and told to Anglicize their names when speaking with Westerners. They would have sounded reasonably convincing to victims who had an immigration background, especially if those victims had previously had limited interactions with US government officials.)

To such prospective 'marks', a call from the tax authorities would almost certainly have been a nightmare come true.¹¹⁹ Skilled workers moving to the US from India, including IT engineers, are typically employed under an H1B visa. This visa is a time-limited work permit that binds a foreign employee to the local company sponsoring his or her visa application. It is seen as a possible step towards Green Card status (permanent residency), but its tenuous nature, together with the extremely long processing times for Green Card applications, creates high levels of insecurity among Indian expatriates.¹²⁰ A relatively minor legal problem can become grounds for removal from the United States, which causes much anxiety as H1B visa holders try to clock up the minimum number of years needed to apply for residency.¹²¹

It is possible that the organizers of the Mira Road scam recognized the fear of job termination and deportation that haunts many recently immigrated families in the US.

Some IT workers had gone through severe emotional distress after 2008 when their positions were made redundant and they were forced to return to India. The scam seems to have effectively played upon fears that the same could happen to others, if even the flimsiest legal infraction marred their immigration record.

Once the potential victim showed signs of falling for the scam, the opener would demand immediate payment of arrears. Officially, payment was supposed to be made with a so-called 'federal card'.¹²² No such type of card actually exists, but the victim would not know that. When the bewildered victim would profess ignorance about how to make a payment, the opener would seemingly display compassion and offer an alternative method: payment via gift cards worth several hundred or even thousands of dollars that could be easily purchased at supermarkets.

At about this time, the opener might have handed over the call to another call-centre employee, whom he or she would introduce as their supervisor. This second employee would play the role of the 'closer' within the scam. The closer's job was to keep the victim on the telephone without interruption and talk them through the process of driving to the nearest supermarket, buying a gift card, scratching the code number and reading it over the phone. With such information, the scammers could make purchases that would then be resold and the revenue laundered back to India through a variety of routes, including, allegedly, the hawala system. At its height, the scam generated a weekly revenue of US\$155 000.

It is considered a matter of pride to call oneself a 'cyber', even though the crimes have little to do with computers.

Some later told the media that when they had asked their supervisors about this, they had been told that a US government agency had outsourced the task of pursuing tax evaders to the Mira Road call centre. Their claims strain credulity even if there might be a grain of truth, in that illegality was perhaps not openly admitted or discussed by the call-centre management. (One can detect echoes of the Ukraine-based and American-led IMI scareware operation that also made use of Indian call-centres.) Even so, there were still people involved on the ground in Mira Road who were aware of the deception and yet genuinely nonplussed about its illegality. They felt that since the targets of fake messages and telephone calls were not Indian nationals, local police had no business interfering with a lucrative business enterprise.

Ironically, a similar mindset can be found among the inhabitants of Jamtara district in Jharkhand province. Scammers here target citizens living in other provinces of India. When reporters have visited villages that are either known to have profited or are suspected of profiting from cyber-enabled crime, they receive a frosty reception. Scams have helped families build new houses and purchase consumer items that are considered luxuries in this deeply impoverished part of India – including expensive cars and more basic goods, such as household appliances.

As far as villagers are concerned, those suspected of committing acts of cybercrime have done nothing wrong, as they were merely aspiring to provide better lives for themselves and their relatives. Jamtara had a tradition of criminality before cybercrime – in the past, local youth would board long-distance trains passing through the district, befriend passengers and drug their food, and then steal their possessions.¹²⁵ Now, the criminal mind has gone online. It is considered a matter of pride to call oneself a 'cyber', even though the actual crimes committed have little to do with computers and are primarily conducted through the use of smartphones and old-fashioned smooth-talk.

Youths from Jamtara who are engaged in cyber-enabled crime are mostly school drop-outs who have not studied beyond the sixth grade.¹³¹ Nonetheless, they pride themselves on being street-smart and techno-savvy. They relish the respect that falls to them from members of the local community. Much like in Russia and China, coaching classes are now being offered to those who want to become cybercriminals. However, instead of learning how to hack computers, students learn how to win the confidence of a victim during a telephone conversation and get them to share private information. Police officials who have been monitoring these classes observe two things: people from outside the local community cannot enrol, thus making it difficult for the classes to be infiltrated; and much of the training seems to be based on the kind of scripts used by illicit call centres to scam foreign nationals.¹³² Only some details are tweaked to adapt the talking points to an Indian context.

Differences between those identified in call-centre scams in large cities and the small-time crooks of Jamtara primarily concern age and education level. As the illicit call centres have to masquerade as legitimate businesses and also must demand a basic level of education if their staff are to deceive foreigners, the average call-centre scammer is in their mid-20s. Those arrested in Jamtara are younger, usually between 15 and 25 years old. What they have in common with their urban counterparts is a desire to be successful and fast.

The Jamtara scammers

The district of Jamtara is spread over 1 800 square kilometres of semi-arid land and has a population of roughly 800 000. About 100 of its 1 161 villages are on barren land, meaning that agriculture (the main source of work in a region that already has a high unemployment rate) is not feasible. These 100 villages have no real source of livelihood, but, bizarrely, in a sign of how lopsided developmental projects have been, they have good mobile and internet connectivity. The latter is provided through mobile data services, since the population is for the most part not computer literate.

At any point in time, local police have the technical capability to monitor a call made from just one of the dozens of mobile-phone towers that are spread across the district. At least 10 of these towers are thought to be the conduits through which phone scams are conducted. One tower is estimated to dispatch up to 3 000 calls daily, while the average for the population density in its area of reception would be about 800. Tellingly, most of these calls go to other provinces, instead of local numbers, as might be expected.¹²⁶

The modus operandi used by scammers in Jamtara is much cruder than that adopted by illicit urban call centres, such as the one in Thane. No call-spoofing technology or fake American accents are needed, since the victims are other Indians. Although reports vary on the size of these criminal outfits, groups of between two and 14 people seem to be the norm.

As with the Mira Road operation, scamming here begins with data theft. A gang member purchases lists of mobile-phone numbers that have been stolen elsewhere in India.¹²⁷ (From available accounts, it does not appear that anything other than the phone numbers themselves are needed to begin with. Dogged persistence, and not technical sophistication, is the key to making these scams pay off.) The gang

meet in a forest clearing on the outskirts of their village, where they are able to hear any police vehicles approaching. They divide the number lists between them and pair up. Each two-person team has a smartphone and a normal mobile phone, both equipped with disposable SIM cards. They begin dialling numbers, with the person holding the normal phone introducing himself as a representative of ATM headquarters or the bank manager of SBI main branch.¹²⁸ (SBI is an abbreviation for the State Bank of India and it is a safe identity to assume because the odds are high that at least some of the call recipients will be SBI customers.) The caller says that the recipient's bank account has come up for verification and asks for his or her debit-card number. Accompanying this message is a warning that if the information is not provided, the debit card may be blocked.

Although, normally, a call recipient with common sense and a basic knowledge of banking procedures would hang up at this point; if that is the case, with hundreds of phone numbers to go through, the scammers move onto the next one. When a potential victim shares their debit-card number, either out of stress or ignorance (or both), the second scammer immediately keys it into an e-wallet that has been set up on the smartphone. The e-wallet would have been created using forged documents presented to a local bank in the Jamtara area, or any other place where the scammers have might friends and relatives who agree to help launder money.¹²⁹ Once the debit-card number is punched in, a one-time password is automatically generated by the digital-payment system and dispatched as a text message to the victim's phone. All that the first scammer now has to do is tell the victim to read that password aloud, claiming that this would verify the authenticity of the victim's bank account. As the unsuspecting target does so, the password is keyed into the e-wallet and the transaction is completed.¹³⁰

One alleged organizer of the Mira Road scam was a 23-year-old who had previously hawked software. His name was Sagar Thakkar but in true 'gangsta-style' he was known as 'Shaggy'. He spent lavishly on girls, apartments and cars. Originally portrayed in some media reports as an evil genius, he turned out, in the words of a police officer to be more a 'greedy youngster than a hardened criminal'.¹³³ A stint in jail clearly offended his petit-bourgeois sensibilities, if an interview that he later gave to a journalist is anything to go by.¹³⁴ Such individuals are likely to be just opportunistic hoods, not mafia-type dons.

Even so, there is clearly a level of organization present in both kinds of cyber-enabled crime seen in India – both in the scams directed at fellow citizens and those targeting Western nationals. Police tracking domestically focused cybercriminals, such as the Jamtara scammers, have observed that such criminals set up bank accounts on behalf of unemployed persons and then 'rent' these by paying a monthly fee to the nominal account holder. Using the debit cards that come with the account, they withdraw cash that has been deposited as pay-outs by scam victims.¹³⁵ Another method is to open accounts using forged documents. One group of 11 cybercriminals from Jamtara was found to be operating 150 bank accounts across India to launder money.¹³⁶

Another sign of organization is the seemingly endless number of disposable mobile-phone SIM cards that these rural scammers appear to have. With the illicit call centres located in cities, levels of compartmentalization are more intricate. Sagar Thakkar gained his larger-than-life reputation partly because he was able to stay on the run for a while before being arrested. This might be more a reflection of the difficulty of pursuing a fugitive in a heavily populated and sparsely policed country. It is still not clear what his role was relative to that of the 21 co-conspirators who have been convicted in the US for involvement in the Mira Road scam.¹³⁷

It seems as if the proceeds of illicit call-centre scams are more unevenly divided than with the cottage-industry-type operations run by rural scammers. Since the village youth of Jamtara district work only for themselves and not as part of a larger corporate entity, they know perfectly well that the law takes a dim view of their activities. For this reason, they seem to be egalitarian about sharing the spoils, seeing the situation as one of them against the world. The same might not be true of urban operations, where it is possible for organizers to hide behind corporate identities and launder money internationally. For all the revenue that the Mira Road scammers allegedly generated, none of their lives seem to have been radically transformed for the better by it.

POLICY IMPLICATIONS – REMEDY THE ECONOMICS, BUT DO NOT FORGET THE POLITICS

This paper set out to examine two questions. First, is cybercrime a top-down and coordinated activity conducted within a hierarchical structure, or does it represent bottom-up entrepreneurship by groups of individuals with technical skills? Second, are there unique characteristics of this particular kind of crime that distinguish it from offline criminality as well as state-sponsored instances of cyber espionage and cyber attacks?

Going by the example of India, it appears that cybercrime is largely (but not exclusively) a bottom-up phenomenon that draws upon a pool of disempowered working-age youth looking to make a quick buck. These youth may occasionally have technical qualifications; they may be hackers or programmers who steal data online and manipulate search engine results, or they may more often be like the scammers of Jamtara – school dropouts with no skills other than the ability to deceive the already gullible.

In any case, there is a measure of organization even in the flattest cyber-crime networks, since the success of a scam requires knowing about the victims – their (internet) habits, personal weaknesses, level of threat awareness, or even just their contact details. Obtaining this information is a step wholly different from exploiting it, and the continuing sale of private data on the darknet or physical-world markets suggests a measure of functional specialization. But that does not automatically mean that cybercrime is hierarchical. Cases where a top-down pattern of criminality exists are elaborate multi-million-dollar scams where the layering of criminal activity is so

- In India, cybercrime is largely a bottom-up phenomenon that draws upon a pool of disempowered working-age youth looking to make a quick buck.

© Flickr/Debarshi Ray



intricate, and the laundering of proceeds so effective, that the real financiers remain unidentified. But these are rare. For other cases, which constitute the majority of those discussed in this paper, the level of thievery is smaller, and the victims less aware.

The main reason why cyber-enabled scams continue to occur is not that they are difficult to investigate for a determined law-enforcement agency. Often, these cases are too costly to investigate for the small sums of money that are lost by private individuals. Plus, lack of reporting by victims means that the scale of the problem is sometimes not fully appreciated.

Cybercrime is a bit like the illegal, unreported and unregulated (IUU) fishing industry: it has enough latitude to accommodate the activities of both petty crooks and well-heeled ones who on the surface appear to be only generating employment opportunities. Just as IUU fishing is sometimes carried out by small trawlers crewed by trafficked labour and at other times by sturdy vessels that are owned by shell companies and crewed by contracted sailors, it is possible for call centres in India to front for a cybercrime operation that has its headquarters elsewhere. Such a call centre may appear legitimate to those who work there, so long as they do not look too closely at its methods or sources of funding. Yet, there also are fake call centres whose staff know full well that they are engaged in illegal activity and do not care, having convinced themselves that their victims deserve no better.¹³⁸

The second question (as to what makes cybercrime different from all other crimes) is open to conceptual debate. At a time when concerns are mounting over the integrity of election processes across the democratic world, due to the risk that social media can be leveraged by foreign powers to swing voter preferences, it seems that small-scale thievery is less of a policy issue. Yet, in the absence of a 'smoking gun', which is always difficult to find in covert operations (especially those carried out in the virtual world), calling something 'cybercrime' helps mobilize public opinion and law enforcement, without ennobling its motives for being political.

The main issue here is that cybercrime, as it is generally understood, represents a crime against individuals or at most, against specific businesses. It does not represent an attack on the state writ large, or the capability of the state to defend itself. Thus, cybercrime is different from both state-sponsored cyber activity as well as offline, street crime in that it uses confidential information obtained through computerized systems to extract money from private persons. This combination of electronic compromise of data, and the monetization of such data either with or without the victim's knowledge, is the essence of cybercrime.

The case of India is a warning to other developing countries that are now coming online in a substantial way. So far, parts of sub-Saharan Africa (with Nigeria, Kenya and South Africa being notable exceptions) have been spared the worst of such criminality because of the low speed of the continent's internet connections. Many countries in Asia have likewise been protected from social unrest because of their lack of exposure to an industry as sensitive to international market trends as the ITes sector. It was the breakneck pace with which mobile phones and data connectivity spread through India, coupled with the failure of political elites to generate new jobs and protect existing ones, that led to the dramatic increase in cybercrime in the country. In its eagerness to take credit for the economic boom years, the country's leadership failed to plan for the downturn that happened after 2008.

The case of India is a warning to other developing countries that are now coming online in a substantial way.

Not one to learn from past mistakes, the Indian political class is now engaged in a populist race to provide internet connectivity. The local government in Delhi has announced a scheme to create 11 000 free Wi-Fi hotspots – this, in a city where 75% of all cybercrime offences remain unsolved by a police force that is bogged down with performing guard duties for VIPs.¹³⁹ Meanwhile, across India, efforts are under way to link 640 000 villages to the internet by means of low-cost transmission devices. Were such measures to be accompanied by parallel initiatives aimed at boosting computer literacy, the result might be an informed and educated citizenry. Instead, 97% of Indians access the internet via mobile phones – a ready-to-use instrument that is a perfect receptor for cybercrime attacks.¹⁴⁰

At a time when unemployment is at a 45-year high, three indicators in particular portend of a future wave of cyber-enabled crime. The first is that joblessness is highest among the most educated segment of the Indian population, a statistic that runs contrary to all expectations. It is easier to find employment in India if one is less qualified than if one is more so. The second sign is that urban unemployment is higher than rural unemployment, a consequence of unrestricted rural-to-urban

migration, flooding cities with surplus labour and placing stress on civic amenities as well as the job market. And the last sign is that unemployment is highest among the 15–29 age group, or exactly the demographic that, according to previous research, is most likely to participate in cybercrime.¹⁴¹

What makes the Indian case ominous is that the IT and ITes sectors themselves haven't actually stopped growing; they have just grown at a much slower rate than was initially projected. In real terms, the economy has continued to do well by international standards, but the slowdown in hiring coupled with job losses outside the IT and ITes sectors has built up societal pressures, which have worsened.

Recent reports suggest that cybercriminals in the country are now becoming more technically sophisticated.¹⁴² While still relying on social engineering, the refinements in their methods suggest that India is slowly going the way of Eastern Europe. By failing to provide a conducive environment for IT start-ups (owing to, for instance, harsh tax laws that make small enterprises unprofitable even before they can be fully operational), the government has slanted the IT sector in favour of established giants. Many of these have been discreet beneficiaries of government favours, such as tax breaks and discounted sales of land for developing into office complexes. In the process, small and medium enterprises have been kept from gaining a foothold in the domestic IT market. It is unsurprising in this situation that Indian youths are sceptical about whether they can ever become wealthy if they stay wholly within the letter of the law as salaried employees.

Governments across the developing world need to take heed of lessons from the Indian experience of cybercrime. First, there has to be encouragement for domestic research and development; dependence on Western antivirus products and computer hardware only pushes up the cost of acquisition and discourages local businesses from investing in cybersecurity.

Secondly, more effective efforts must be made to spread out the educational curriculum base of young workers and prevent a glut of technical experts who later cannot find work.

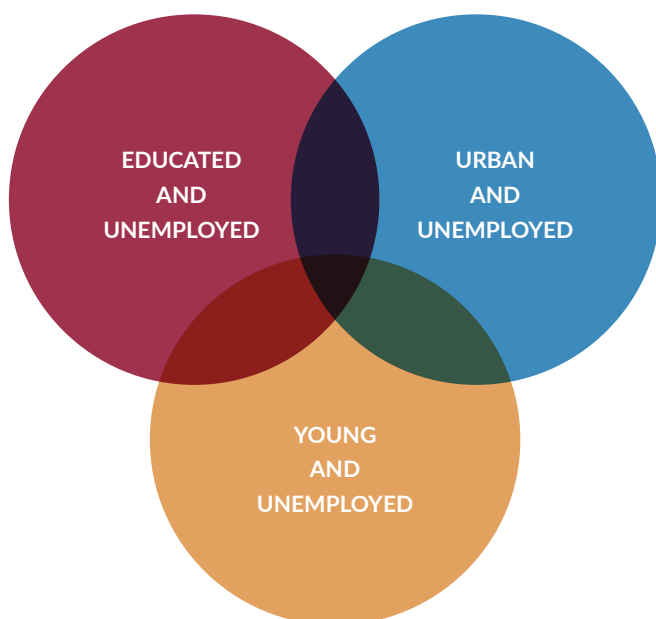


FIGURE 5 These three indicators point to a future wave of cyber-enabled crime in India



Cybercrime sensitization class for Jharkhand police.

© Jharkhand Police Website

Thirdly, police units need to be trained to handle cybercrime investigations on par with more serious acts of criminality, such as those associated with 'traditional' organized crime, including extortion and protection rackets.

And, finally, there needs to be a concerted effort to sensitize the general public to the risks of cybercrime. Sharing information on techniques favoured by online criminals is unlikely to prompt a threat rise so huge as to outweigh the benefits of a more aware population. The biggest enabler of cybercrime is lack of security-consciousness on the part of victims. Although there have been some calls for making digital negligence a punishable offence (such that if an employee clicks on a phishing email, he/she would be liable for prosecution or damages caused), a better approach might be to educate potential victims.¹⁴³

The above measures are of an economic and administrative nature; but there is another dimension that is also relevant: the political. Many Indian cybercriminals who scammed Westerners did so out of personal resentment. At one level, such ire was prompted by plain envy over the better quality of life enjoyed by Western societies (especially their social-welfare systems, which have no counterpart in India).¹⁴⁴ But, on another level, there is a growing sense of awareness that for all the admiration that

Indian youth have for American popular culture, and for all the improvements in strategic ties between New Delhi and Washington, little personal benefit would come of them. The story of how a segment of India's urban demographic went from loudly mimicking its American counterpart to quietly resenting it within the space of a decade offers an important lesson in managing public expectations. An appropriate comparison might be made with the European Union: if viewed as both a political and economic project, then one of the pillars of European integration is free movement of labour, along with capital, goods and services. Giving the working classes an option to relocate to where jobs are concentrated, or where wages are higher, is integral to convincing them that globalization has trickle-down effects and does not only benefit a narrow sliver of business elites.

Multinational companies need to remember that outsourcing jobs to poorer nations can lead eventually to all manner of inter-personal clashes and disappointed hopes. Moving backroom jobs to India merely because the cost of labour was cheaper inflicted an injustice upon American workers and customers alike. The poor quality of service endured by the latter was only to be expected because, as one commentator pointed out, 'India became the call-centre capital of the whole world but it was often built on a cost-saving agenda, not a quality agenda.'¹⁴⁵

On the flip side, from 2005, racial abuse of legitimate Indian call-centre workers generated what a lawyer for these workers at the time referred to as a 'searing anger' among people who felt they were insulted for merely trying to earn a livelihood.¹⁴⁶ Following the 2008 economic crisis, when job losses in the IT and ITes sectors combined with growing press coverage of anti-immigrant politics and labour protectionism in the US, some Indian call-centre workers realized that there would never be an American Dream for them. No longer having to think about applying for a US visa in the future, they had no compunction about committing a felony against US citizens. Other governments would do well to take note: integration into Western-led production chains requires a concerted effort to calibrate worker expectations of rising living standards. Should this process be neglected, there could be a working-class backlash, as has been the case in India.

NOTES

- 1 Nicole Lindsey, Cyber fraud by Chinese hackers makes headlines in India, *CPO Magazine*, 21 January 2019, <https://www.cpomagazine.com/cyber-security/cyber-fraud-by-chinese-hackers-makes-headlines-in-india>.
- 2 On jobs, India behind Pak, Bangla, Afghan..., *The Telegraph*, 18 January 2020, <https://www.telegraphindia.com/india/on-jobs-india-behind-pak-bangla-afghan/cid/1736855>.
- 3 Adaobi Tricia Nwaubani, Letter from Africa: Why Nigeria's internet scammers are 'role models', *BBC*, 23 September 2019, <https://www.bbc.com/news/world-africa-49759392>.
- 4 Sumati Yengkhom, I stood nowhere even after a 7-year stint: Former BPO executive, *Times of India*, 11 October 2011, <https://timesofindia.indiatimes.com/city/kolkata/i-stood-nowhere-even-after-a-7-year-stint-Former-BPO-executive/articleshow/10298512.cms>.
- 5 Abuse and stress: What Indian BPO workers have to undergo on a daily basis, *Economic Times*, 26 November 2017, <https://economictimes.indiatimes.com/jobs/abuse-and-stress-what-indian-bpo-workers-have-to-undergo-on-a-daily-basis/articleshow/61806162.cms?from=mdr>.
- 6 Shweta Punj, Welcome to jobless growth: Why India is facing an unemployment crisis, *India Today*, 20 April 2016, <https://www.indiatoday.in/magazine/cover-story/story/20160502-employment-scenario-job-crunch-jobless-growth-economy-828782-2016-04-20>.
- 7 Snigdha Poonam, *Dreamers: How Young Indians Are Changing Their World*. Gurgaon: Penguin, 2019, p 239.
- 8 Vincent Achuka, How Kenyan scammers stole over \$3 million from US firms, *The East African*, 22 September 2019, <https://www.theeastafrican.co.ke/news/ea/Kenyan-scammers-stole-from-US-firms/4552908-5282734-7oumyx/index.html>.
- 9 Sasha Fedorenko, New research signals snowballing threat of cybercrime on marketplaces, *Tamebay*, 11 September 2019, <https://tamebay.com/2019/09/new-research-signals-snowballing-threat-cybercrime-ecommerce.html>.
- 10 Preeti Soni, Indian police stations are struggling to access computers as cybercrime zooms, *Business Insider*, 13 September 2019, <https://www.businessinsider.in/indian-police-stations-are-struggling-to-access-computers-as-cybercrime-zooms/articleshow/71105648.cms>.
- 11 Swaminathan Ramanathan, India's urban moment: The pressing need for a new thought architecture, *Observer Research Foundation*, 6 June 2019, <https://www.orfonline.org/research/india-urban-moment-pressing-need-new-thought-architecture-51710/>, and Akash Gulankar, Number of People in India's Cities Will Overtake Rural Population in Next Three Decades, Says Report, *News18*, 21 June 2019, <https://www.news18.com/news/india/number-of-people-in-indias-cities-will-overtake-rural-population-by-2050-says-report-2197025.html>.
- 12 Gautam S. Mengle, Credit, debit card details of 4 lakh Indians up for sale on dark net, *The Hindu*, 8 February 2020, <https://www.thehindu.com/news/national/credit-debit-card-details-of-4-lakh-indians-up-for-sale-on-dark-net/article30766138.ece>.

- 13 Sramana Mitra, The death of Indian outsourcing is imminent, *Huffpost*, 6 May 2017, https://www.huffpost.com/entry/the-death-of-indian-outsourcing-is-imminent_b_59357886e4b06c4693fb770a.
- 14 Ananya Bhattacharya, Most Indian techies quit their startup jobs within two years, *Quartz India*, 14 August 2018, <https://qz.com/india/1347207/indian-startups-have-an-employee-retention-problem-worse-than-bpos/>.
- 15 Durga Prasad Sunku, Hyderabad: Don't Google for customer care numbers, warn experts, *Deccan Chronicle*, 24 September 2019, <https://www.deccanchronicle.com/nation/crime/240919/hyderabad-dont-google-for-customer-care-numbers-warn-experts.html>.
- 16 'Cybercriminal' refers to anyone who uses an internet-linked device to repeatedly carry out a criminal offence. So, individuals who commission one-off crimes, such as assassination of a business partner by hiring a hitman on the darknet, have been excluded. But individuals using smartphones to run e-banking scams are included, because these smartphones are linked to the internet.
- 17 Charles Cooper, Is the Mafia Taking Over Cyber Crime? Not Really, Symantec, 15 August 2018, <https://www.symantec.com/blogs/feature-stories/mafia-taking-over-cyber-crime-not-really>. That Eastern Europe is an exception, where cybercriminals have strong ties to organized-crime groups, was noted by a veteran Indian police official in 2004; see RK Raghavan, Catching the cyber criminal, *Frontline*, 5–18 June 2004, <https://frontline.thehindu.com/static/html/fl2112/stories/20040618004211300.htm>.
- 18 Snigdha Poonam, *Dreamers: How Young Indians Are Changing Their World*. Gurgaon: Penguin, 2019, p 247.
- 19 Kriangsak Kittichaisaree, *Public International Law of Cyberspace*. Cham: Springer, 2017, pp 265–266; Al Jazeera English, *Hacked: The Bangladesh Bank Heist*, 24 May 2018, <https://www.youtube.com/watch?v=6Y9UaLkZQ0> (relevant portion is from 22.02 minutes to 23.18 minutes).
- 20 Mark Button, Editorial: economic and industrial espionage, *Security Journal*, 26 September 2019, <https://link.springer.com/article/10.1057/s41284-019-00195-5>.
- 21 Rick Sarre, Laurie Yiu-Chung Lau and Lennon YC Chang, Responding to cybercrime: current trends, *Police Practice and Research*, 19, 6, 2018, pp 515–516.
- 22 Ayeshea Perera, Why India's financial system is vulnerable to hacks, *BBC*, 15 November 2019, <https://www.bbc.com/news/world-asia-india-50401008>.
- 23 Jaskiran Bedi, China never had to learn English like India because its economy relied on manufacturing, *The Print*, 7 February 2020, <https://theprint.in/pageturner/excerpt/china-never-had-to-learn-english-like-india-because-its-economy-relied-on-manufacturing/361198/>.
- 24 Dominic Casciani, Briton who knocked Liberia offline with cyber attack jailed, *BBC*, 11 January 2019, <https://www.bbc.com/news/uk-46840461>.
- 25 Soumyo D Moitra, Cybercrime: Towards an assessment of its nature and impact, *International Journal of Comparative and Applied Criminal Justice*, 28, 2, 2004, p 106.
- 26 This exception has been put forward because there are video-sharing websites on the internet (especially the darknet) where sexual abuse of children, as well as violent rape of adult women, is monetized. Since the victims, whether children or women, have no control over what happens to them and might well have been abducted off the street and filmed against their will, they can in no way be said to have been susceptible to deception.
- 27 Michael McGuire, *Into the Web of Profit*, study sponsored by Bromium Inc, April 2018, https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf.
- 28 Garrett M Graff, China's hacking spree will have a decades-long fallout, *Wired*, 11 February 2020, <https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/>.
- 29 Alice Hutchings, Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission, *Crime, Law and Social Change*, 62, 1, 2014, p 4.

- 30 E Rutger Leukfeldt, Edward R Kleemans and Wouter P Stol, Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis, *Crime, Law and Social Change*, 67, 1, 2017, p 42.
- 31 E Rutger Leukfeldt, Edward R Kleemans and Wouter P Stol, A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists, *Crime, Law and Social Change*, 67, 1, 2017, p 29.
- 32 David Décary-Héту and Benoit Dupont, Reputation in a dark network of online criminals, *Global Crime*, 14, 2–3, 2013, p 177.
- 33 Srinath Srinivasan, Cyber Security: Are IoT deployments in India safe from hackers?, *Financial Express*, 19 August 2019, <https://www.financialexpress.com/industry/technology/cyber-security-are-iot-deployments-in-india-safe-from-hackers/1679046>.
- 34 Alice Hutchings, Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission, *Crime, Law and Social Change*, 62, 1, 2014, p 11.
- 35 Nir Kshetri, *The Global Cybercrime Industry*. Cham: Springer, 2010, pp 46–48.
- 36 Rob McCusker, Transnational organised cyber crime: distinguishing threat from reality, *Crime, Law and Social Change*, 46, 4–5, 2006, p 265.
- 37 Ibid., p 268.
- 38 Peter Grabosky, Organised Crime and the Internet, *The RUSI Journal*, 158, 5, 2013, p 23.
- 39 Jonathan Lusthaus, Trust in the world of cybercrime, *Global Crime*, 13, 2, 2012, p 84.
- 40 Benjamin Wallace, How Two Scammers Built an Empire Hawking Sketchy Software, *Wired*, 27 September 2011, https://www.wired.com/2011/09/mf_scareware.
- 41 Jim Finkle, Inside a global cybercrime ring, Reuters, 24 March 2010, <https://www.reuters.com/article/us-technology-scareware/inside-a-global-cybercrime-ring-idUSTRE62N29T20100324>.
- 42 Andy Greenberg, Global Takedown Shows the Anatomy of a Modern Cybercriminal Supply Chain, *Wired*, 16 May 2019, <https://www.wired.com/story/goznym-takedown-cybercrime-supply-chain>.
- 43 Diego Gambetta and Steffen Hertog, *Engineers of Jihad: The Curious Connection between Violent Extremism and Education*. Princeton: Princeton University Press, 2016, pp 44–50.
- 44 Nir Kshetri, *The Global Cybercrime Industry*. Cham: Springer, 2010, pp 178–179.
- 45 Thomas J Holt, Olga Smirnova, Yi Ting Chua and Heith Copes, Examining the risk reduction strategies of actors in online criminal markets, *Global Crime*, 16, 2, 2015, p 83.
- 46 Nir Kshetri, Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers, *Crime, Law and Social Change*, 60, 1, 2013, pp 47–48.
- 47 Amitendu Palit, Dragon in the Elephant's Backyard: Chinese Imports in India's Mobile Revolution, *Pacific Affairs*, 85, 3, 2012, p 545.
- 48 Sourav Majumdar, Data and the new India, *Fortune India*, 6 November 2018, <https://www.fortuneindia.com/opinion/data-and-the-new-india/102658>.
- 49 Ian Jack, India has 600 million young people – and they're set to change our world, *The Guardian*, 13 January 2018, <https://www.theguardian.com/commentisfree/2018/jan/13/india-600-million-young-people-world-cities-internet>.
- 50 Ben Crair, Maniac Killers of the Bangalore IT Department, *Bloomberg*, 15 February 2017, <https://www.bloomberg.com/news/features/2017-02-15/maniac-killers-of-the-bangalore-it-department>.
- 51 Mihir Sharma, India's burgeoning youth are the world's future, *LiveMint*, 8 September 2017, <https://www.livemint.com/Opinion/2WSy5ZGR9ZO3KLDMGiJq2J/Indias-burgeoning-youth-are-the-worlds-future.html>.
- 52 Suchi Kedia, Sriram Gutta, Terri Chapman and Vidisha Mishra, Here's what young Indians really want from life, *World Economic Forum*, 5 October 2019, <https://www.weforum.org/agenda/2018/10/here-s-what-young-indians-really-want-from-life/>.
- 53 94% of engineering graduates are not fit for hiring, says this IT stalwart, *Times of India*, 4 June 2018, <https://economictimes.indiatimes.com/jobs/only-6-of-those-passing-out-of-indias-engineering-colleges-are-fit-for-a-job/articleshow/64446292.cms?from=mdr>.

- 54 Sumeet Mehta, In India's 'post-memory' society, rote learning has become an anachronism, *Business World*, 14 January 2020, <http://www.businessworld.in/article/In-India-s-Post-Memory-Society-Rote-Learning-Has-Become-An-Anachronism/14-01-2020-182009/>.
- 55 Michael McGuire, *Into the Web of Profit*, study sponsored by Bromium Inc, April 2018, https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf, p 26.
- 56 Nir Kshetri, Cybercrime and cyber-security issues associated with China: some economic and institutional considerations, *Electronic Commerce Research*, 13, 2013, pp 52–53.
- 57 Heli Tiirmaa-Klaar, Botnets, Cybercrime and National Security, in H Tiirmaa-Klaar et al. (eds.), *Botnets*. Cham: Springer, 2013, p 13.
- 58 Thomas J Holt and Adam M Bossler, An Assessment of the Current State of Cybercrime Scholarship, *Deviant Behavior*, 35, 1, 2014, p 21.
- 59 Catherine D Marcum, George E Higgins, Melissa L Ricketts and Scott E Wolfe, Hacking in High School: Cybercrime Perpetration by Juveniles, *Deviant Behavior*, 35, 7, 2014, p 582.
- 60 Urvija Banerji, Women Are The Main Targets of Cybercrime. There's a Solution for That., *The Swaddle*, 19 April 2018, <https://theswaddle.com/more-women-needed-in-cybersecurity-write-up>.
- 61 Peter Grabosky, The Global Dimension of Cybercrime, *Global Crime*, 6, 1, 2004, p 149.
- 62 Chris Pogue, *The Black Report 2018: Decoding the Minds of Hackers*, Nuix, https://cdn2.hubspot.net/hubfs/85462/2018/THIS%20WEEK/report_nuix_black_report_2018_web_us.pdf, p 10.
- 63 Jeremy Wittkop, *Building a Comprehensive IT Security Program*. Cham: Springer, 2016, p 11.
- 64 Jaime Ibarra, Hamid Jahankhani and Stefan Kendzierskyj, Cyber-physical attacks and the value of healthcare data: facing an era of cyber extortion and organised crime, in H Jahankhani et al. (eds.), *Blockchain and Clinical Trial*. Cham: Springer, 2019, p 121.
- 65 Richard Mahapatra, How India remains poor: Has poverty become 'hereditary', *Down to Earth*, 4 January 2020, <https://www.downtoearth.org.in/news/economy/how-india-remains-poor-has-poverty-become-hereditary--68790>.
- 66 Debarshi Dasgupta, Call centre scams highlight woes of India's jobless youth, *Straits Times*, 9 December 2018, <https://www.straitstimes.com/asia/south-asia/call-centre-scams-highlight-woes-of-indias-jobless-youth>.
- 67 Nir Kshetri, Cybercrime and cybersecurity in India: causes, consequences and implications for the future, *Crime, Law and Social Change*, 66, 3, 2016, pp 324–325.
- 68 RK Raghavan, The house is burning, *Frontline*, 15–28 January 2011, <https://frontline.thehindu.com/static/html/fl2802/stories/20110128280210100.htm>.
- 69 V Sridhar, A dream in decline, *Frontline*, 23 June 2017, <https://frontline.thehindu.com/cover-story/a-dream-in-decline/article9721030.ece>.
- 70 James Crabtree, *The Billionaire Raj: A Journey Through India's New Gilded Age*. Noida: Harper Collins, 2018, p 21.
- 71 Ibid.
- 72 Ravi Sharma, Pain of separation, *Frontline*, 23 June 2017, <https://frontline.thehindu.com/cover-story/pain-of-separation/article9721113.ece>.
- 73 Tushar Kaushik, Bengaluru is India's cybercrime capital, *Economic Times*, 1 February 2019, <https://economictimes.indiatimes.com/tech/internet/bengaluru-is-indias-cybercrime-capital/articleshow/67769776.cms> and Tushar Kaushik, Cybercrimes rocketing in Bengaluru, police straining to catch up, *Citizen Matters*, 24 January 2020, <http://bengaluru.citizenmatters.in/bengaluru-cybercrimes-credit-debit-card-fraud-ccps-new-police-stations-41758>.
- 74 Aishwarya Rakesh, Just 20 constables to tackle 4 000 cybercrime cases, *Deccan Herald*, 28 June 2018, <https://www.deccanherald.com/city/top-bengaluru-stories/just-20-constables-tackle-4000-677553.html>.
- 75 There was one case, in June 2006, where payment information of British customers of HSBC bank was sold by an employee of HSBC's Bangalore call centre. However, subsequent references to the city in media reporting on call centre scams have been noticeably rare. Miles Brignall, HSBC call-centre man held over data theft, *The Guardian*, 28 June 2006, <https://www.theguardian.com/business/2006/jun/28/accounts.money>.

- 76 Bhumika Khatri, Internet In India 2019: Equal Split Of Internet Users In Rural And Urban Areas, Inc42, 27 September 2019, <https://inc42.com/buzz/internet-in-india-2019-equal-split-of-internet-users-in-rural-and-urban-areas>.
- 77 Snigdha Poonam, *Dreamers: How Young Indians Are Changing Their World*. Gurgaon: Penguin, 2019, p 239.
- 78 Morgan Hartley and Chris Walker, The culture shock of India's Call Centers, *Forbes*, 16 December 2012, <https://www.forbes.com/sites/morganhartley/2012/12/16/the-culture-shock-of-indias-call-centers/#511ec35272f5>.
- 79 MG Arun, India's about to hang up on call centre culture, *India Today*, 25 March 2013, <https://www.indiatoday.in/magazine/business/india/story/20130325-bpo-industry-call-centre-culture-dying-in-india-762765-1999-11-30>.
- 80 Vikhar Ahmed Sayeed and A Saye Sekhar, High and dry, *Frontline*, 28 February–13 March 2009, <https://frontline.thehindu.com/static/html/fl2605/stories/20090313260501400.htm>.
- 81 Amelia Gentleman, Indian call staff quit over abuse on the line, *The Guardian*, 29 May 2005, <https://www.theguardian.com/world/2005/may/29/india.ameliagentleman>.
- 82 Seetha Parthasarathy, *The Backroom Brigade: How a Few Intrepid Entrepreneurs Brought the World to India*. New Delhi: Penguin, 2006, p. 173. See also Sudhin Thanawala, India's call-center jobs go begging, *Time*, 16 October 2007, <http://content.time.com/time/business/article/0,8599,1671982,00.html>.
- 83 Andrew Marantz, My summer at an Indian call centre, *Mother Jones*, July/August 2011, <https://www.motherjones.com/politics/2011/07/indian-call-center-americanization>; Amrit Dhillon and David Harrison, India has last laugh in call centre sitcom, BBC, 29 January 2006, <https://www.telegraph.co.uk/news/worldnews/asia/india/1509124/India-has-last-laugh-in-call-centre-sitcom.html>.
- 84 Jason Hickel, How Britain stole \$45 trillion from India, *Al Jazeera*, 19 December 2018, <https://www.aljazeera.com/indepth/opinion/britain-stole-45-trillion-india-181206124830851.html>.
- 85 Nick O'Malley, Indian call centre staff fed up with racist abuse, *The Age*, 20 March 2006, <https://www.theage.com.au/national/indian-call-centre-staff-fed-up-with-racist-abuse-20060320-ge1yuv.html>.
- 86 Mehdi Boussebaa, Offshore call centre work is breeding a new colonialism, *The Conversation*, 21 October 2014, <http://theconversation.com/offshore-call-centre-work-is-breeding-a-new-colonialism-32999>.
- 87 Rajini Vaidyanathan, India's call centre growth stalls, BBC, 27 September 2011, <https://www.bbc.com/news/magazine-15060641>.
- 88 Zubair Ahmed, Stressed Indians leave call centres, BBC, 29 September 2008, <http://news.bbc.co.uk/2/hi/business/7635889.stm>.
- 89 A 2011 *New York Times* report illustrated this, pointing out that the popular American television sitcom *Friends*, an entertainment staple in the Philippines, was still being used a teaching aid for Indian call-centre workers on how to communicate with Westerners. See Vikas Bajaj, A new capital of call centers, *The New York Times*, 25 November 2011, <https://www.nytimes.com/2011/11/26/business/philippines-overtakes-india-as-hub-of-call-centers.html>.
- 90 V Sridhar, IT collapse would shut paths to social mobility, *Frontline*, 23 June 2017, <https://frontline.thehindu.com/cover-story/it-collapse-would-shut-paths-to-social-mobility/article9721076.ece>.
- 91 David Shaftel and Khushboo Narayan, Call centre fraud opens new frontier in cybercrime, *Livemint*, 26 February 2012, <https://www.livemint.com/Companies/hVjMnKYvqDveiXJEjdJkRN/Call-centre-fraud-opens-new-frontier-in-cybercrime.html>.
- 92 Priya Kale, The impact of corruption on democracy in India, *LSE Blogs*, 17 June 2013, <https://blogs.lse.ac.uk/southasia/2013/06/17/the-impact-of-corruption-on-democracy-in-india/>.
- 93 Abhishek Waghmare, In 2015, Crime In India At 11-Year High, *India Spend*, 1 September 2016, <https://archive.indiaspend.com/cover-story/in-2015-crime-in-india-at-11-year-high-78461>.

- 94 P Sainath, The feel good factory, *Frontline*, 28 February–12 March 2004, <https://frontline.thehindu.com/static/html/fl2105/stories/20040312007800400.htm>.
- 95 Snigdha Poonam, The scammers gaming India's overcrowded job market, *The Guardian*, 2 January 2018, <https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market>.
- 96 Business Insider, Almost every house of these Jharkhand villages has a cyber crook, 29 May 2017, <https://www.businessinsider.in/almost-every-house-of-these-jharkhand-villages-has-a-cyber-crook/articleshow/58892905.cms>.
- 97 RK Raghavan, The mysteries of cyber forensics, *Frontline*, 11–24 September 2004, <https://frontline.thehindu.com/static/html/fl2119/stories/20040924003510500.htm>.
- 98 Somendra Sharma, Cyber crime thrives, detection rate fails to keep pace: RTI, *DNA*, 28 March 2019, <https://www.dnaindia.com/mumbai/report-cyber-crime-thrives-detection-rate-fails-to-keep-pace-rti-2733266>; Arunabh Saikia, Why most cybercrimes in India don't end in conviction, *Livemint*, 29 June 2016, <https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html>.
- 99 Rajiv Kalkod, Bengaluru tops chart in cybercrimes, *Times of India*, 21 October 2019, <https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-tops-chart-in-cybercrime/articleshow/71694693.cms>.
- 100 These figures are for the period 1 January 2019 to 12 December 2019. Akhil Kadidal and Umesh R Yadav, Cyber fraud: Online crimes overtake offline crimes, *Deccan Herald*, 15 December 2019, <https://www.deccanherald.com/specials/insight/cyber-fraud-online-crimes-overtake-offline-crimes-785648.html>.
- 101 Kiran Parashar, Bengaluru: Cybercrime police station re-opens, *Times of India*, 11 December 2019, <https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-cyber-crime-police-station-re-opens/articleshow/72476837.cms>.
- 102 400 cybercrime cases cleared in 15 days, *The New Indian Express*, 9 February 2020, <https://www.newindianexpress.com/cities/bengaluru/2020/feb/09/400-cybercrime-cases-cleared-in-15-days-2101091.html>.
- 103 Theja Ram, Why conviction rate for cyber crime cases in Karnataka is abysmally low, *The News Minute*, 1 October 2019, <https://www.thenewsminute.com/article/why-conviction-rate-cyber-crime-cases-karnataka-abysmally-low-109803>.
- 104 TRAFFIC, Training programme in India helps officials fight back against cybercrime, 2 January 2019, <https://www.traffic.org/news/training-programme-in-india-helps-officials-fight-back-against-cybercrime>.
- 105 RK Raghavan, Crimes in cyberspace, *Frontline*, 23 November–6 December 2002, <https://frontline.thehindu.com/static/html/fl1924/stories/20021206005111000.htm>.
- 106 Nir Kshetri, Cybercrime and cybersecurity in India: causes, consequences and implications for the future, *Crime, Law and Social Change*, 66, 3, 2016, p 321.
- 107 Ananya Bhattacharya, India ranks among the worst in the world for cybersecurity, *Quartz*, 7 February 2019, <https://qz.com/india/1544739/india-ranks-among-the-worst-in-the-world-for-cybersecurity>.
- 108 MG Arun and Shweta Punj, Show me the black money, *India Today*, 8 September 2018, <https://www.indiatoday.in/magazine/cover-story/story/20180917-show-me-the-black-money-1333206-2018-09-08>.
- 109 Money Control, Financial cybercrime and identity theft in India are increasing, reveals FIS PACE Report, 16 April 2019, <https://www.moneycontrol.com/news/technology/financial-cybercrime-and-identity-theft-in-india-are-increasing-reveals-fis-pace-report-3838901.html>.
- 110 Post demonetisation, 190 cyber crimes reported in Vijayawada, *The New Indian Express*, 11 November 2017, <https://www.newindianexpress.com/cities/vijayawada/2017/nov/11/post-demonetisation-190-cyber-crimes-reported-in-vijayawada-1698295.html>.

- 111 Telangana: QR code scam can empty your wallet, *Times of India*, 23 December 2019, <https://timesofindia.indiatimes.com/city/hyderabad/qr-code-scam-can-empty-your-wallet/articleshow/72930101.cms>.
- 112 Kaushik Deka, The new battlefield is online. Is India prepared?, *India Today*, 3 September 2017, <https://www.indiatoday.in/magazine/the-big-story/story/20170911-cyber-crime-cyber-attack-malware-cyber-security-1034804-2017-09-03>.
- 113 Stas Alforov and Christopher Thomas, India: Rising cybercrime frontier, Gemini Advisory, 18 April 2019, <https://geminiadvisory.io/india-rising-cybercrime-frontier>; Rajendra Jadhav, India's Cosmos Bank loses \$13.5 mln in cyber attack, Reuters, 14 August 2018, <https://www.reuters.com/article/cyber-heist-india/indias-cosmos-bank-loses-135-mln-in-cyber-attack-idUSL4N1V551G>; Emma Woollacott, Indian gov't breaks ground on dedicated cybersecurity center, *The Daily Swig*, 28 June 2019, <https://portswigger.net/daily-swig/indian-govt-breaks-ground-on-dedicated-cybersecurity-center>.
- 114 Kunle Sanni, Three Nigerians arrested In India for alleged cybercrime, *Premium Times*, 13 June 2019, <https://www.premiumtimesng.com/news/more-news/334984-three-nigerians-arrested-in-india-for-alleged-cybercrime.html>.
- 115 Shashank Bengali, Inside the Indian IRS scam that cheated U.S. taxpayers out of millions, *Los Angeles Times*, 22 November 2016, <https://www.latimes.com/world/la-fg-india-irs-scam-20161027-story.html>.
- 116 Ibid.
- 117 Economic Times, How a 24-year-old pulled off a 'Special 26' to fool scores of gullible Americans, 10 April 2017, <https://economictimes.indiatimes.com/news/politics-and-nation/how-a-24-year-old-pulled-off-a-special-26-to-fool-scores-of-gullible-americans/articleshow/58108701.cms?from=mdr>.
- 118 Debasish Panigrahi, Thane call centre fraud: How 'magic jack' enabled accused to make unlimited calls to US, Canada, *Hindustan Times*, 12 October 2016, <https://www.hindustantimes.com/mumbai-news/thane-call-centre-fraud-how-magic-jack-enabled-accused-to-make-unlimited-calls-to-us-canada/story-P0EnslZ2b8Kzt9SQXdTAYK.html>. The use of 'Magic Jack' has also been reported in 2019 by Indian call centre scammers, see Rakesh Dixit, India's Cyber Crooks, *India Legal*, 22 June 2019, <http://www.indialegallive.com/cyber-security/fraud-on-us-citizens-indias-cyber-crooks-67492>.
- 119 Ananya Bhattacharya, An Indian tech worker's movie shows the anxiety of being an H-1B immigrant in Silicon Valley, *Quartz*, 29 March 2017, <https://qz.com/india/944030/an-indian-tech-workers-movie-shows-the-anxiety-of-being-an-h1-b-immigrant-in-silicon-valley>.
- 120 Rahul Sachitanand, How the American dream is souring for many Indian IT workers, *Economic Times*, 1 September 2019, <https://economictimes.indiatimes.com/nri/visa-and-immigration/how-the-american-dream-is-souring-for-many-indian-it-workers/articleshow/70926993.cms>.
- 121 Tapoja Chaudhuri, An ethnographic account of the intimate lives of the Indian IT-sector workers in the Pacific Northwest, *International Examiner*, 11 February 2020, <https://iexaminer.org/an-ethnographic-account-of-the-intimate-lives-of-the-indian-it-sector-workers-in-the-pacific-northwest/>.
- 122 Mansi Choksi, This Indian cop took down a massive IRS call-center scam, *Narratively*, 24 February 2017, <https://narratively.com/this-indian-cop-took-down-a-massive-irs-call-center-scam>.
- 123 Ellen Barry, India's call-center talents put to a criminal use: Swindling Americans, *The New York Times*, 3 January 2017, <https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html>.
- 124 See 4RealDocumentaries, Indian illegal call centre, 9 September 2017, <https://www.youtube.com/watch?v=Xva3Jq4wSs> (relevant portion of the documentary is from 21.32 minutes to 23.51 minutes).
- 125 Rajiv Rao, This remote, small town is the epicentre of cybercrime in India, *ZDNet*, 19 July 2018, <https://www.zdnet.com/article/this-remote-small-town-is-the-epicentre-of-cybercrime-in-india>.
- 126 Deepu Sebastian Edmond, Phishing in Jamtara: What does it take to carry out online fraud?, *Indian Express*, 13 December 2015, <https://indianexpress.com/article/india/india-news-india/phishing-in-jamtara-what-does-it-take-to-carry-out-online-fraud>.

- 127 Shiv Sahay Singh, The cyber con 'artists' of Jharkhand's Jamtara district, *The Hindu*, 12 August 2017, <https://www.thehindu.com/news/national/other-states/the-cyber-con-artists-of-jamtara/article19476173.ece>.
- 128 Amitabh Srivastava, Phish pond, *India Today*, 27 July 2016, <https://www.indiatoday.in/magazine/nation/story/20160808-cyber-crime-jamtara-jharkhand-829309-2016-07-27>.
- 129 Pankaj Mishra, Jamtara, where India is winning its war on cyber crime, *Factor Daily*, 7 May 2018, <http://factordaily.com/india-winning-war-on-cyber-crime-jamtara>.
- 130 Nitin Jain, Arvind Ojha and Jugal R Purohit, India Today Investigation: Jamtara emerges as the biggest den of digital crime, *India Today*, 3 January 2017, <https://www.indiatoday.in/india/story/india-today-investigation-jamtara-digital-hackers-cyber-crimes-953010-2017-01-03>.
- 131 Anushree Majumdar, What drew me to phishing, as a concept, is that I feel it is a great equaliser: Jamtara director Soumendra Padhi, *The Indian Express*, 3 February 2020, <https://indianexpress.com/article/entertainment/web-series/netflix-series-jamtara-lives-of-small-town-cybercriminals-soumendra-padhi-6247865/>.
- 132 Abhay Singh, Mastermind Mandal lived a king's life in remote Jamtara, *Millennium Post*, 24 May 2018, <http://www.millenniumpost.in/delhi/mastermind-mandal-lived-a-kings-life-in-remote-jamtara-301150>; Faisal Tandel, Online fraudsters from Jharkhand who duped Mumbaiers of lakhs arrested, *Mid-Day*, 25 July 2017, <https://www.mid-day.com/articles/mumbai-news-jharkhand-fraudsters-scam-cheating-case-south-mumbai/18444187>; Ramashankar, Cyber crime schools & trainers stun cops, *The Telegraph*, 13 September 2017, <https://www.telegraphindia.com/india/cyber-crime-schools-amp-trainers-stun-cops/cid/1317436>.
- 133 Kelly Phillips Erb, Indian police allege IRS, FBI, other law enforcement not interested in phone scam arrests, *Forbes*, 24 April 2017, <https://www.forbes.com/sites/kellyphillips/2017/04/24/indian-police-allege-irs-fbi-other-law-enforcement-not-interested-in-phone-scam-arrests/#28d0dc564a3e>.
- 134 Anamika Gharat, Exclusive: Mira Road call centre scam accused Shaggy reveals his side of the story, *Mid-Day*, 25 June 2018, <https://www.mid-day.com/articles/exclusive-mira-road-call-centre-scam-accused-shaggy-reveals-his-side-of-the-story/19546176>.
- 135 Anurag Dwary, Jobless men 'rent' out bank accounts, aid cyber crime in Madhya Pradesh, *NDTV*, 4 July 2019, <https://www.ndtv.com/india-news/jobless-men-in-madhya-pradeshs-bhind-rent-out-bank-accounts-aid-cyber-crime-2063715>.
- 136 Fraudsters from Jamtara gang arrested for duping elderly man, *The Statesman*, 3 February 2020, <https://www.thestatesman.com/bengal/fraudsters-jamtara-gang-arrested-duping-elderly-man-1502852574.html>.
- 137 Christine Hauser, U.S. breaks up vast I.R.S. phone scam, *The New York Times*, 23 July 2018, <https://www.nytimes.com/2018/07/23/business/irs-phone-scams-jeff-sessions.html>.
- 138 John Kelly, Even telephone scammers agree: Don't trust them!, *The Washington Post*, 9 December 2019, https://www.washingtonpost.com/local/even-telephone-scammers-agree-dont-trust-them/2019/12/08/f353c616-17a1-11ea-a659-7d69641c6ff7_story.html.
- 139 Ankit Yadav and Chayyanika Nigam, Cyber crime risk in free public WiFi, *India Today*, 11 August 2019, <https://www.indiatoday.in/mail-today/story/cyber-crime-risk-in-free-public-wifi-1579617-2019-08-11>.
- 140 Nitisha Kashyap, Financial frauds hard to detect as they generally take place over long weekends, say cyber security experts, *News18*, 4 September 2019, <https://www.news18.com/news/india/financial-frauds-hard-to-detect-as-they-generally-take-place-over-long-weekends-say-cyber-security-experts-2297251.html>.
- 141 Amit Kapoor and Anirudh Dutta, Indian economy struggles to expand with rising unemployment rates, stagnant wages, poor female participation in labour force, *Firstpost*, 24 September 2019, <https://www.firstpost.com/india/indian-economy-struggles-to-expand-with-rising-unemployment-rates-stagnant-wages-poor-female-participation-in-labour-force-7392721.html>; Saurabh Mishra, Saru Dhir and Madhurima Hooda, A study on cyber

- security, its issues and cyber crime rates in India, in HS Saini et al. (eds.), *Innovations in Computer Science and Engineering*. Cham: Springer, 2015, p 252.
- 142 Indian Express, Employee's computer hacked, petroleum dealer duped of Rs 5.48 lakh, 20 February 2020, <https://indianexpress.com/article/cities/ahmedabad/employees-computer-hacked-petroleum-dealer-duped-of-rs-5-48-lakh-6276552/>.
- 143 Sanjay Pandey, Digital India's response readiness against cyber attacks is frail, lack of online security awareness biggest weakness, *Firstpost*, 25 June 2019, <https://www.firstpost.com/india/digital-indias-response-readiness-against-cyber-attacks-is-frail-lack-of-cyber-security-awareness-biggest-weakness-6876111.html>.
- 144 Jeremy Nuttall, I don't feel bad. I'm not going to stop. And you will never, ever catch me, says CRA scammer, *The Hamilton Spectator*, 3 December 2018, <https://www.thespec.com/news-story/9059766-i-don-t-feel-bad-i-m-not-going-to-stop-and-you-will-never-ever-catch-me-says-cra-scammer>.
- 145 James Crabtree, India's call-centres make move upmarket, *Financial Times*, 25 June 2012, <https://www.ft.com/content/bd8e769a-b53c-11e1-ab92-00144feabdc0>.
- 146 Mike McPhate, Outsourcing outrage: Indian call-center workers suffer abuse, *San Francisco Chronicle*, 17 November 2005, <https://www.sfgate.com/business/article/Outsourcing-outrage-Indian-call-center-workers-2594713.php>.



GLOBAL INITIATIVE

AGAINST TRANSNATIONAL
ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 500 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net