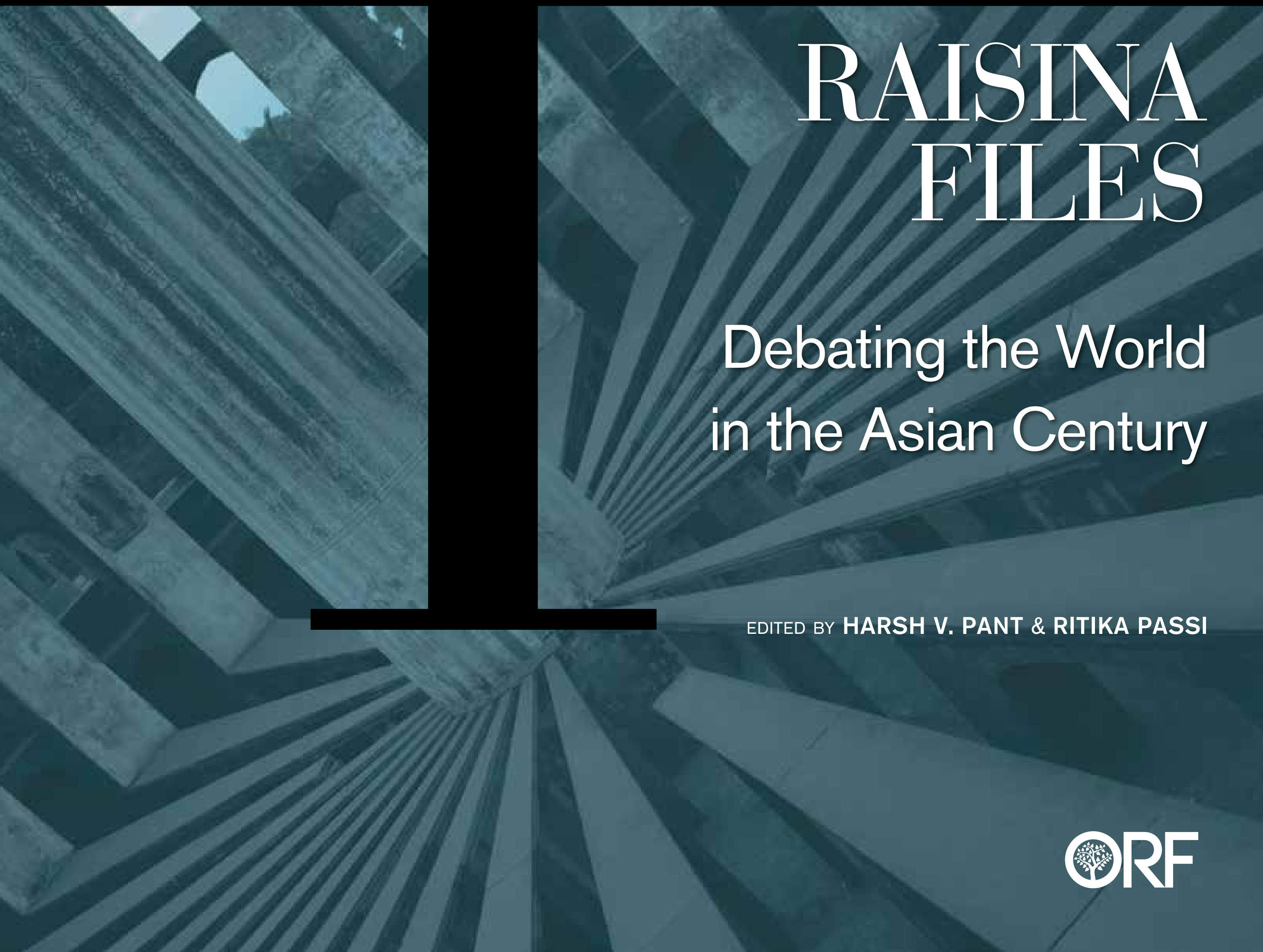
VOLUME 2 ■ JANUARY 2017

rf 2017



RAISINA FILES

Debating the World in the Asian Century

EDITED BY **HARSH V. PANT & RITIKA PASSI**

ORF

BREAKING RANKS WITH ASIA: THE CASE FOR ENCRYPTING INDIA

Bhairav Acharya

Technology Lawyer and OTI Program Fellow,
New America

THERE is no Asian approach to encryption. The Internet transcends conventional borders and so does the encryption that travels with it. But there is a growing Asian security dialogue and an emerging debate on encryption in Asia. That debate has been overshadowed by the disjointed responses of individual countries to specific aspects of encryption. Bahrain, China, Iran, Kazakhstan, Pakistan and Saudi Arabia, amongst others, formally disallow different forms of client-side encryption. A larger list of countries have decryption-on-demand laws. They are not very different from Western liberal democracies where calls for encryption bans and backdoors are commonplace.

In India, the surveillance and encryption debate is marked by contradictions. We are losing out, the claim goes, because the technologies and infrastructure of digital communications are located abroad. We must sacrifice our freedoms, another claim goes, because only high levels of surveillance can protect us. Unfortunately, these reductive arguments, designed to appeal to nationalism and insecurity, have captured the national discourse. They have helped to shape a statist, blunt and control-oriented approach to encryption. Taking their cue from China, several Asian countries including India want to impose their sovereignty on the Internet, strictly license encryption products, have unfettered access to Internet communications and more. This 'Internet sovereignty' approach to encryption will fail.

This essay explains the basics of how encryption works; provides a high-level account of the American crypto-wars and how they manifest in India; looks at how mass surveillance fears have fuelled a new phase of the crypto-wars; and demonstrates the futility of the Indian government's nationalism-laced approach to encryption, particularly in relation to data localisation, Internet sovereignty and the withdrawn National Encryption Policy of 2015. Looking ahead, this essay argues that encryption cannot be stopped; cybersecurity depends on strong encryption; and India's security and prosperity depend on the

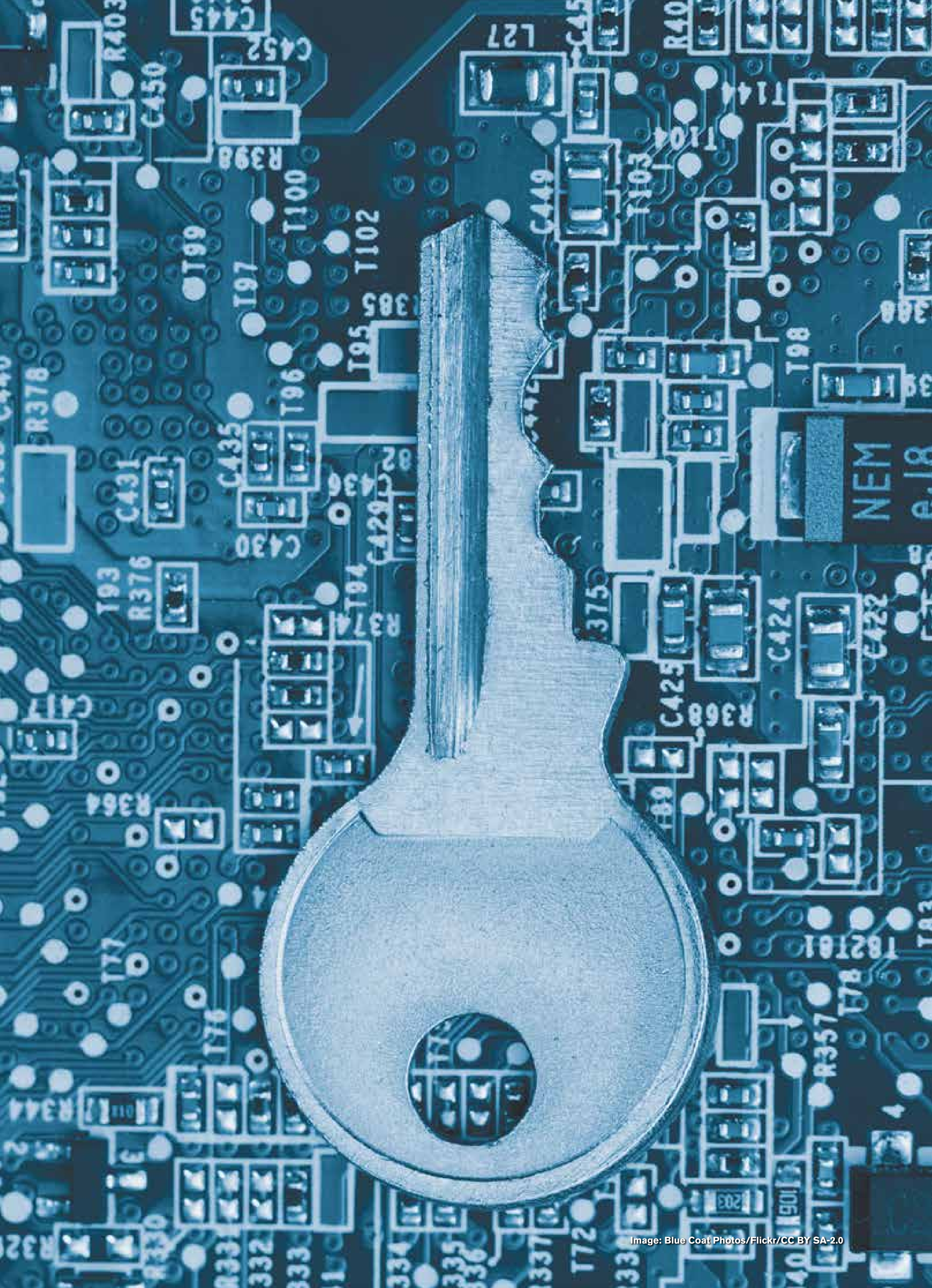


Image: Blue Coat Photos/Flickr/CC BY SA-2.0

widespread adoption of encryption.

If it stopped pursuing the Internet sovereignty approach and supported strong encryption without backdoors instead, India would break ranks with many Asian countries. But since there is no multilateral cybersecurity cooperation regime in Asia that India participates in, that would not be a loss. On the other hand, India should drive the Asian cybersecurity debate towards unbreakable encryption in the interests of its emerging digital economy, democratic values and national security.

The basics of encryption

Encryption is the conversion of intelligible data (plaintext), such as files or messages, into an unintelligible form (ciphertext) and decryption is the reversion of ciphertext to plaintext. Encryption occurs through the application of a cipher, a cryptographic algorithm that links the plaintext and ciphertext. The algorithm contains at least one variable parameter (key) that changes each time data is encrypted. The key is determined by a random number generating algorithm. For encryption to work, the key must be secret. Encryption does not encompass data conversion using a fixed key with no variable parameter (scrambling).[1]

Until the 1970s, both the encrypter and decrypter had to have a pair of identical keys (symmetric-key encryption). The system has two main weaknesses. First, the key has to be shared before the message (key exchange). Second, secrecy is inversely proportional to the number of people in the know—intuitively, not mathematically. Moreover, the sender is not sure that the key reached the intended receiver, and the receiver is not sure that her key was authentic (authentication problem). That is because of the danger of the key exchange being intercepted by a third party who may access the messages as they flow or impersonate either the sender or receiver (man-in-the-middle).

Most key exchange problems were solved by the invention of public key cryptography in the 1970s. Two non-identical but mathematically linked keys are created, one to encrypt a message and the other to decrypt it (asymmetric-key encryption). A receiver makes one of her keys publicly available (public key) but keeps the other one secret (private key). A sender encrypts her message using the receiver's public key which the latter decrypts with her private key. To solve the authentication problem, the sender, who has also made her public key available, signs her message with her private key which can only be decrypted with her public key to verify her signature (digital signature).

When designed and implemented well, public key cryptography is unbreakable. It obviates backdoors because no man-in-the-middle has the receiver's private key. It can assure message integrity by algorithmically assigning the data a fixed value (hashing) which can be verified for consistency. However, public key cryptography is computationally intensive and slow to operate so it is rarely used for real-time communications which continue to be symmetrically encrypted.

The crypto-wars

The encryption debate is United States-centric because, for better or for worse, American laws have shaped the Internet's architecture and the availability of encryption products. Public key cryptography did not begin to find mass application until the 1990s. The primary cryptosystem in regular use, the Data Encryption Standard (DES), developed by IBM in the 1970s, and approved by the NSA, used a symmetric-key algorithm with a weak key. As Internet use grew, businesses improved the security of their products to encourage consumer confidence.

For individuals who did not want to depend on off-the-shelf encryption, the asymmetric-key Pretty Good Privacy (PGP) cryptosystem, developed in 1991, offered client-side encryption for messages. PGP provides unbreakable encryption for messages even when passing through known backdoors. No one besides the sender and receiver can access the plaintext making strong PGP immune to man-in-the-middle attacks (end-to-end encryption).

In the early 1990s, American telecom carriers were upgrading from analogue to packet-switched digital transmissions. The US government pushed carriers to install the 'Clipper chip,' a chipset that used a symmetric-key algorithm to encrypt voice data with a key developed by the NSA. The Clipper chip was to be installed in phones and a key copy surrendered to government to be held in escrow.

There are two fundamental problems with government key escrow. First, escrow of any sort only works when the third-party escrow agent is trusted by the other parties to handle the object of their transaction—in this case, keys. When a government wiretaps a private communication, it is not a third-party; so in a surveillance situation the government cannot by definition perform escrow functions. Second, the key is vulnerable to attack while stored in escrow. When the Clipper algorithms were declassified by the US government, they were swiftly shown to be vulnerable to high-speed, high-volume key guesses (brute-force attack).

At the same time, the US legislature enacted the Communications Assistance for Law Enforcement Act of 1994 (CALEA). It compelled telecom carriers to technologically enable government wiretaps. There were three significant limitations. First, the government was prevented from banning commercial encryption. Second, the law was restricted to the public switched telecom network (PSTN); it did not cover Internet services such as voice-over-Internet-protocol (VoIP) calls. Third, communications carriers were exempted from the duty to decrypt messages (decryption mandate) if they did not have the means to do so.

In 2005, CALEA was extended to cover VoIP and broadband Internet service providers (ISPs) even though they are not PSTN-based. But it still did not cover non-ISP-provided Internet email or over-the-top (OTT) instant messengers. Consequently, while Skype had to have CALEA-mandated backdoors, Gmail or WhatsApp were free from backdoors and the decryption mandate. That set the stage for the second phase of the crypto-wars.

In India, the Central Monitoring System (CMS) corresponds to CALEA in several ways. Until recently, telecom carriers were restricted to 40-bit encryption which was even weaker than the 64-bit key found in the 1980s-vintage A5/1 cipher used in the 2G GSM standard.[2] Some carriers simply did not encrypt and voice calls could be lifted off-the-air. The CMS requires carriers to provide the government with a seamless interception interface irrespective of their network encryption. It covers VoIP and ISPs too. Unless an Indian user uses client-side public key encryption or commercial end-to-end encryption, their communications have permanent backdoors.

The CMS is more than an interception interface. It creates a centralised database which even Britain's recent "snoopers' charter" failed to do. Will Delhi misuse its technological capabilities? We do not know. But we do know that the government has a long history of illegal wiretaps. The issue has been consistently raised in Parliament and covered in the press.[3] Interceptions and decryptions are ordered by bureaucrats with little understanding of the law and no independent oversight mechanism. Private carriers have obeyed even procedurally-irregular interception orders instead of pushing back against irregular surveillance.[4] Nevertheless, the government asks us to trust it to use the CMS in accordance with law. It would not be an unfair assessment to say that businesses and individuals will be more interested in encrypting their communications from now on.

The Blackberry episode

From 2008 the Indian government pressured Blackberry-maker Research in Motion (RIM) to decrypt messages on demand or hand over their key. RIM faced similar measures in Saudi Arabia and the United Arab Emirates. The campaign against RIM was more about enforcing Indian jurisdiction on a foreign company than it was about the national security risks of encryption. There are two kinds of Blackberry services. For companies, RIM installs a local Blackberry Enterprise Server (BES) and employees' emails are routed through the BES with strong encryption. In most cases, RIM does not have the key and cannot decrypt BES messages. In any event, terrorists are not employees, they do not use BES services.

For individuals, RIM has an unencrypted Blackberry Internet Service (BIS) network. This is most likely how terrorists using Blackberrys communicate. BIS emails can be intercepted as plaintext provided the local carrier removes any transport layer encryption it added.[5] Instant messages via the Blackberry Messenger (BBM) app are transmitted on the basis of unique device-specific numbers (PIN). PIN to PIN messaging, another option for terrorists, are not encrypted, they are only scrambled using a single, global key.[6] They can be inter-

> “If the ‘going dark’ campaign reflects the American security establishment’s alarm at the modern encryption business, the Indian authorities are still primarily concerned about Internet sovereignty.

cepted and routed to a third Blackberry quite easily, a textbook man-in-the-middle attack.[7]

Essentially, if the government wanted to intercept someone’s BIS communications, it was free to do so under Indian law. There would have to be an interception order under either section 69 of the Information Technology Act, 2000 (IT Act) read with rule 3 of the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 (Interception Rules), or section 5(2) of the Indian Telegraph Act, 1885 read with rule 419A of the Indian Telegraph Rules, 1951. On the other hand, if, hypothetically, the BIS server was located in India, then access to data on it could be ordered under section 91 of the Code of Criminal Procedure, 1973 (CrPC), a significantly lower threshold.

There is legal uncertainty regarding data access procedures because interception law is largely observed in the breach. Sections 69 and 69B of the IT Act, read with their respective rules, grant access to stored information and communications data, but in 2014 the Central Bureau of Investigation was using section 91 of the CrPC to access communications data. It is likely that other law enforcement agencies were doing the same and still are. There is no transparency and no accountability for legal abuse. In any event, the Interception Rules almost certainly suffer from excessive delegation and are ultra vires their parent statute.

So why did the government go after RIM? Perhaps it was anxious to demonstrate a tough line on security and singled out Blackberry because it was an iconic brand. That was how RIM’s chief executive officer viewed the incident in 2011.[8] It is most likely that the government wanted RIM to install mirror servers in India to fulfil its grievances regarding data localisation. But by singling out RIM, the government scored an own goal. As long as terrorists used the BIS service to communicate, intercepting their unencrypted communications was possible.[9] Now they have probably migrated to more secure services. Witless nationalism, which thoroughly pervades the government’s approach to encryption, damages India’s national security.

RIM has stressed that the “solution” it gave the Indian government does not involve its BES platform, only its unencrypted BIS network.[10] Is there a BIS proxy server in India? Probably not, the repercussions for RIM outweigh any Indian market gains. Does RIM reroute all Indian traffic from its foreign BIS server to India? Maybe, but that would be non-targeted mass surveillance, which is illegal. Did RIM simply guarantee that it would positively respond to every government request for targeted BIS data? This is most likely, but it is not a gain because the government had technological access to it anyway.[11]

The new crypto-war

The race for stronger encryption in America is fuelled by fears of further CALEA extensions to cover Internet services and withdraw the guarantee against the decryption mandate. The push probably began with Edward Snowden’s disclosures of pervasive global Internet surveillance by Western intelligence agencies, which brought privacy to the forefront of public attention. Fears of NSA overreach are not misplaced. In 2013, a random number-generating algorithm that had been recommended for cryptographers had to be abandoned after claims that it contained an NSA-planted backdoor.

In that context, Internet companies began to adopt unbreakable encryption. For transmission, businesses are gradually implementing end-to-end encryption. KakaoTalk, South Korea's most popular messaging app, introduced optional end-to-end encryption 2014. WhatsApp, the most popular messenger in India, rolled out its end-to-end encryption system in 2016. However, WhatsApp's claim to not have the decryption keys has been challenged and, in any event, it does preserve metadata.[12] For storage, phones manufacturers are introducing strong device encryption paired with measures to thwart brute-force attacks including passcode authentication delays, challenge-response tests, and automatic data erasure (device locking).

In 2014, Apple introduced default device locking based on a key which it did not know, thereby voluntarily shutting itself out of the data access process. Soon after, FBI director James Comey delivered his famous 'going dark' speech: "[E]ncryption threatens to lead all of us to a very dark place."[13] Apple refused to obey a court order to jailbreak the phone on the ground that the government could not compel it to write code. A central question in the Apple-FBI dispute is whether the government can enforce the decryption mandate against Internet companies. Apple is not in the telecommunications business, it is an information services company and is therefore exempt from CALEA.

In India, the decryption mandate is contained in section 69 of the IT Act read with rules 5 and 17 of the Interception Rules. However, the rules only apply in respect of a "decryption key holder" and in the case of end-to-end encryption, nobody but the sender and receiver holds the key. Will the Indian government enforce the decryption mandate against individuals and risk violating the fundamental right against self-incrimination under article 20(3) of the Constitution? This issue needs to be authoritatively decided by the constitutional courts. Several Asian countries have versions of the decryption mandate in their laws but, unlike India, many do not have independent judiciaries.

If the 'going dark' campaign reflects the American security establishment's alarm at the modern encryption business, the Indian authorities are still primarily concerned about Internet sovereignty. Both views are misguided but, additionally, the Indian view is detached from reality. In 2014, national security advisor Ajit Doval said: "One of the problems we have is that technologically we have lost out in certain areas where the root servers are all under control of countries [in] the West, mainly the US. […] They are helpful to us in some areas, but not always helpful, particularly in the corporate world."[14] For Doval, the issue is still about extending Delhi's writ to Internet companies. If that happens, we are told, cybersecurity will bloom at the command of the Indian state.

The Internet sovereignty approach to encryption is stuck in a Cold War time warp. It continues to have currency in Asia because of China's success at firewalling its Internet and strictly controlling encryption protocols. But even China was forced to drop a provision in its 2015 anti-terror law which required official vetting of commercial encryption. For India, such an approach is anathema to free markets and free speech. A state-controlled Internet with state-sanctioned encryption would be as counterproductive as a return to the centrally-planned command economy. Instead of trying to achieve an Internet license raj, India needs to promote cybersecurity by encouraging the creation of state-of-the-art encryption products and enabling domestic Internet companies to compete in the global marketplace.

For those anticipating forward-thinking cybersecurity and a vibrant high-technology sector, the draft National Encryption Policy of 2015 was a disappointment. The policy was based on the belief that the Internet ecosystem is a pyramid with the government at the top, businesses in the middle and citizens at the bottom. That is far from the truth. Nevertheless, the policy gave the government the exclusive power to sanction cryptographic algorithms and key sizes, demanded the registration of businesses and apps that used encryption, and banned citizens from encrypting or using commercial encryption without the government's permission. Moreover, whenever anything was encrypted, the policy demanded that a copy of the plaintext was to be stored for three months and surrendered on demand. Such a move would have seriously jeopardised national security.

The policy revealed an abysmal lack of awareness amongst cybersecurity regulators which should concern us all. The government has promised to return with a redrafted encryption policy. It might be better worded but it will likely advocate a government monopoly over encryption, compulsory backdoors, mandatory data localisation and other measures to consolidate state control.

Looking ahead

Governments have long attempted to control encryption and prevent it from crossing borders. Those attempts have failed because the Internet is global. The PGP cryptosystem was classified as a munition and banned from export but its creator published its source code as a book—because books are constitutionally protected—and bypassed the control regime. When the Snowden disclosures revealed governmental attempts to compromise encryption, the private sector responded with end-to-end encryption and device locking. Encryption protects free speech and, like speech, it cannot be perfectly controlled.

Strong cryptography has proliferated well beyond the control of governments. Yet, that has not stopped the Indian government from trying to impose import, use and export controls on encryption products. The withdrawn encryption policy stopped Indians from using cryptography without government approval based on key size. The policy also called for export controls. However, if Indian smartphone makers or Internet companies are bound by a low encryption standard, they will not be able to compete in the global marketplace. Governments cannot stop individuals from using encryption products and should not waste public resources trying to do so. India should do the opposite: encourage domestic cryptographic talent and champion 'Made in India' commercial encryption products.

The debate over backdoors is gathering pace. After the Clipper chip failed, there were proposals for commercial key escrow where the keys would be held by private third-parties. It was opposed because of the inherent risks of key escrow. Eleven leading cryptographers published a seminal paper in 1997 concluding that key escrow would result in "substantial sacrifices in security and greatly increased costs to the end-user."[15] In 2015, the NSA proposed a new split-key escrow system. Create a 'golden key,' the NSA said, split it into several pieces, and distribute the pieces amongst multiple third-parties so that no one alone could use the key. That proposal too has been dismissed by cryptographers.

Last year, a comprehensive group of companies, cryptographers, policy organisations and security experts sent the US president a letter warning him of the dangers of backdoors. The principle is simple—if you build a backdoor, everybody will use it, not just the police. It will also be used by hackers, data thieves, hostile governments, terrorists and criminals. Encryption is either breakable or unbreakable, backdoored or end-to-end—it is one or the other. When a backdoor is installed, it creates a security vulnerability which will eventually be maliciously exploited. The argument that the backdoor will be well-guarded is baseless. There are numerous reports of protected systems being broken in to through backdoors. For example, in 2010, China exploited a US government backdoor to hack Gmail.[16]

India does not have a data breach law so we simply do not know how often our government has been hacked. Be under no illusions: India's public cybersecurity is in shambles. There are continuous reports of hacks, mostly attributed to China, including breaches of defence servers carrying military secrets.[17] Even the official digital certificates repository has been breached.[18] There have also been a string of unreported incidents including hostile interceptions of communications, numerous brute-force attacks on weak encryption and malware on government servers. The bottom line is that there is no realistic way that the Indian government can secure any backdoors it may be given. The state's cybersecurity capabilities may increase in the future but backdoors will never stop being dangerous.

The quickest path to cybersecurity is for India's private sector to take the lead. The future promises massive network-dependent and data-intensive projects piloted by the private sector. The nascent Aadhaar-based, digital payments system will revolutionise the financial technology sector. Increasing broadband penetration has made India the world's fastest-growing smartphone market that is catalysing the telecommunications and Internet sector. The 'Digital India' programme for Internet delivery of government services will exponentially increase the volume of sensitive traffic. These projects and India's economy as a whole can only be secured through the pervasive use of unbreakable encryption. That would have a cascading effect on the rest of the Indian Internet.

Setting encryption standards to secure India's future should be a collaborative exercise. The open competition to choose the Advanced Encryption Standard (AES) remains the gold standard in cryptographic adoption. NIST, the US government's cryptographic standards agency, prescribed neutral minimum requirements and called for algorithmic proposals. Fifteen proposals were received, transparently tested, rigorously cryptanalysed, and their findings openly discussed in conferences. The process represented NIST's acceptance that it did not possess the monopoly of cryptographic expertise as well as the view that everybody has a stake in encryption, not just the state.

In India, barring a few civil society organisations, unbreakable encryption has no champions. The argument for India is not that we should sacrifice national security for stronger encryption. The truth is that to protect our national security, we need unbreakable encryption. Since encryption is key to cybersecurity which, in turn, is the foundation of the emerging digital economy, strong encryption will promote prosperity. Ultimately, what is best for Indian citizens and businesses is also best for the Indian government: an Internet with unbreakable encryption. If there is ever an Asian approach to encryption, let it be the same.

[1] C.C. Mann, "A Primer on Public-key Encryption," The Atlantic, September 2002, http://www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574.

[2] B. Acharya, "The Short-lived Adventure of India's Encryption Policy," Berkeley Information Privacy Law Association, December 1, 2015, https://www.ocf.berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption-policy/.

[3] For a recent parliamentary intervention, see Shadi Lal Batra, Rajya Sabha, Unstarred Question No. 2556, Illegal Phone Tapping and Monitoring of Phone Calls, March 20, 2013.

[4] P. Prakash, "Misuse of Surveillance Powers in India," Centre for Internet & Society, December 6, 2013, http://cis-india.org/internet-governance/blog/misuse-surveillance-powers-india-case1.

[5] "Comparing BIS and BES," Blackberry Knowledge Base, August 15, 2015, http://support.blackberry.com/kb/articleDetail?ArticleNumber=000003652.

[6] R. Halevy, "FAQ: Blackberry Messenger and PIN Messages are Not Encrypted," Berry Review, August 6, 2010, http://www.berryreview.com/2010/08/06/faq-blackberry-messenger-pin-messages-are-not-encrypted/; C. Parsons, "Decrypting Blackberry Security, Decentralizing the Future," Citizen Lab, November 29, 2010, https://citizenlab.org/2010/11/decrypting-blackberry-security-decentralizing-the-future/.

[7] What is peer-to-peer message encryption?," Blackberry Knowledge Base, August 15, 2015, http://support.blackberry.com/kb/articleDetail?articleNumber=000010498.

[8] "RIM CEO calls a halt to BBC Click interview," BBC, April 13, 2011, http://news.bbc.co.uk/2/hi/programmes/click_online/9456798.stm.

[9] See R. Halevy, "FAQ: What Communication is Encrypted on Your Blackberry," Berry Review, August 6, 2010, http://www.berryreview.com/2010/08/06/faq-what-communication-is-encrypted-on-your-blackberry/.

[10] Quoted from J. Horwitz, "After a lengthy battle, BlackBerry will finally let the Indian government monitor its servers," TNW, July 10, 2013, http://thenextweb.com/asia/2013/07/10/after-a-lengthy-battle-blackberry-will-finally-let-the-indian-government-monitor-its-servers/.

[11] See B. Schneier, "UAE to Ban Blackberrys," Schneier on Security (blog), August 3, 2010, https://www.schneier.com/blog/archives/2010/08/uae_to_

ban_blac.html, Aug, 3, 2010.

[12] M. Ganguly, “WhatsApp backdoor allows snooping on encrypted messages,” *The Guardian*, January 13, 2017, https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages.

[13] J. Comey, “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course,” FBI, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[14] Quoted from P.M. Vincent, “NSA flags corporate control over cyberspace,” *The Hindu*, November 23, 2014, http://www.thehindu.com/todays-paper/tp-national/nsa-flags-corporate-control-over-cyberspace/article6626059.ece.

[15] H. Abelson et al, “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption,” Schneier on Security (blog), May 26, 1997, https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf.

[16] B. Schneier, “U.S. enables Chinese hacking of Google,” CNN, January 32, 2010, http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/.

[17] M. Balachandran, “The Chinese government may have been spying on India’s leaders and defence companies for a decade,” Quartz, April 13, 2015, https://qz.com/381897/the-chinese-government-may-have-been-spying-on-indias-leaders-and-defence-companies-for-a-decade/.

[18] L. Constantin, “Digital certificate breach at Indian authority also targeted Yahoo domains, possibly others,” CSO, July 10, 2014, http://www.csoonline.com/article/2452595/security/digital-certificate-breach-at-indian-authority-also-targeted-yahoo-domains-possibly-others.html.