THE HINDU

BUSINESS

Law enforcement in the digital era

Pronab Mohanty

MARCH 06, 2017 00:00 IST
UPDATED: MARCH 06, 2017 03:57 IST

One consequence of the recent demonetisation was a push towards the digitisation of the economy — a move that will create transparency in the financial system.

But this digital push must be accompanied by greater security of digital transactions to deal with the tsunami of cybercrimes that is bound to follow. India's enforcement mechanisms, laws and policies must be re-examined immediately to ensure that the theft of data or money is dealt with severely, swiftly and transparently.

A recent ASSOCHAM-PwC study found that cybercrime in India surged almost 300% between 2011 and 2014. The Indian Computer Emergency Response Team (CERT-In), the national agency tasked with maintaining cybersecurity, reported more than 50,000 security incidents in 2015. With the push towards digital transactions, this number will only grow. As smartphones become the preferred mode of transactions, hacking, phishing and malware based attacks are serious concerns. The Nokia malware report showed a 96% surge in mobile device infections in 2016.

The logistical burden these incidents will place on law-enforcement the judiciary, will be enormous. Our police infrastructure, which doesn't yet have the capacity to handle existing cybercrimes, will be strained to breaking point in the coming surge.

Dealing with cyber offences necessarily means upgrading the capabilities of law enforcement, either through new recruitment or by imparting technical training to existing personnel. But this prescription comes with its own problems, not least being the supply of qualified people.

Given the salaries and perquisites in the public services vis-a-vis the private sector, hiring qualified people will be difficult. A differential pay structure or fast-track promotions will be problematic in the current system, which is strictly hierarchical. If existing personnel are trained rigorously, on the other hand, there is the danger that they will be poached by the private sector.

The more promising option is a Public Private Partnership (PPP) to combat cybercrime. Such a partnership will draw upon the skills in the private sector to train the police, while providing practical experience in dealing with cybercrimes to corporate employees. Such models already exist and are fairly successful.

One example is the National Cyber Forensic Training Alliance (NCFTA) in the U.S., a non-profit platform that tackles cybercrime through partnerships with subject matter experts in the public, private, and academic sectors. A similar set-up in India is the NASSCOM-affiliated Data Security Council of India (DSCI). The DSCI sets up cyberlabs in different cities and imparts training. This model is now ripe for scale-up across the country and can be tapped into by the jurisdictional police.

In addition, we must reshape our current cybercrime laws to address the likely surge in offences relating to digitisation. Given the borderless nature of cybercrimes, state police agencies need to be able to pursue offenders without worrying about jurisdiction. To allow for this, a pan-India cyber-enforcement force must be considered.

Such a force can become a one-stop-shop for digital monetary fraud and will go a long way in assuaging the concerns of cyber-fraud victims. Such a force will also be able to identify trends and stop entities that prey on the gullibility of uninformed citizens transitioning to the digital economy.

(The views of Pronab Mohanty, IPS, DDG-UIDAI and Jai Asundi, Research Coordinator, CSTEP are personal)

Public-private partnership is critical to training the police