THE MURKY ALLEYS OF DIGITAL BLACK MARKETS

India has implemented extensive steps to address the growing cyber threats, bringing the National Cyber Security Policy, training the police to deal with cybercrimes and launching a National Cybercrime Reporting portal to tackle child pornography

Sameer Patil

A series of recent US government advisories alerting financial institutions and E-commerce websites about the growing menace of online drug trafficking raises pertinent questions about whether India is doing enough to combat this area of crime in its own backyard. The answer: New Delhi can–and should–be doing much more than it has so far.

The Digital Black Market

The online drug business has thrived on digital black markets, or darknet marketplaces, which have become the mainstay of online illegal activity, after operating in the shadows for years. Accessible only through an encrypted browser technology, The Onion Router (TOR), these sites sell not just the narcotics but also other prohibited goods such as firearms, stolen personal and financial data, malware and computer viruses. These sites also serve the extreme perversions of the human mind such as contract killing and child pornography. Payments are made in crypto-currencies like Bitcoin and Monero. This year alone Bitcoin transactions on digital black markets are expected to be worth US$1 billion.

The US government advisories were targeted at American financial institutions and E-commerce websites, but they are relevant to India too. Sites like Tochka and Empire have India-based vendors, offering opium, Xanax bars, Ketamine, hashish and prescription pills, to customers in India and abroad. Between 2015 and 2017, the Narcotics Control Bureau had interdicted four cases of online drug purchases. But this is just the tip of the iceberg, as vendors use the most ingenious tricks to prevent seizures of contraband shipments.

Adding to the threat of expanding drug sales and cybercrimes, terrorist groups are making increased use of darknet and digital black markets. Islamic State's virtual propaganda on darknet platforms has regularly featured India. In the Kashmir valley, the Al-Qaeda-affiliated Ansar Ghazwatul Hind regularly advisesits cadres to use Virtual Private Networks (VPN) and TOR-based browsers to avoid government surveillance.

Besides anonymity, digital black markets offer these groups a platform for fund-raising and easy access to weapons. Vendors on sites like Berlusconi, offer weapons and 3D printing blueprints for parts of handguns, which can be combined with other widely available components, like pistol grip and trigger assemblies, to make firearms.

At the national level, India needs to –

- Set up a group of technical experts to monitor technologies which enable digital black-market activity–not just TOR and encryption technologies but related technologiestoo like 3D printing.
- Work with crypto-currency exchanges and VPN providers to track illicit transactions. Thought should also go into setting up a bug bounty programme, which will encourage and reward software developers for unlocking encryption technologies.

At the diplomatic level, India must –

- Make digital black-market activity a focus of bilateral cybersecurity dialogues with the US, UK and Canada, whose national security agencies have carried out crackdowns against black marketplaces.
- Joint strategies to discredit black marketplaces should also be developed.

At the multilateral level, India must

- Work with like-minded countries to tackle specific dimensions of digital black-market activity like drug smuggling and arms trade. This can be done by shaping new agreements, dealing with specific dimensions of the problem and
- By amending existing agreements to cover emerging issues such as the Arms Trade Treaty, which seeks to reduce illicit weapons trade.

"Digital black markets offer easy access to stolen personal and financial data, malicious software, software vulnerabilities, and hacking tools, in turn used to commit cybercrimes. Sites such as Dream Market (now shut) had facilitated sale of stolen and forged identification documents, including Aadhaar cards, PAN cards, voter ID cards and passports. Whether these have been used to commit cybercrimes remains unclear, but clearly, India's vulnerability is growing."
—Sameer Patil, Fellow, International Security Studies Programme, Gateway House

In recent months, this shadowy world of black markets has witnessed an upheaval with many leading sites going offline including Dream Market (shut down by administrators), Silkkitie/Valhalla and Wall Street Market (taken down by the Europol). But these are temporary setbacks, with new sites popping up to replace those that were shutdown. These newer iterations have learned from the experience and mistakes of their predecessors, becoming tougher and more complex to track and crack. Their resilience and constant innovation make digital black markets a complex challenge to India's national security and its nascent digital economy.

India has implemented extensive steps to address the growing cyber threats, bringing the National Cyber Security Policy, training the police to deal with cybercrimes, and launching a National Cybercrime Reporting portal to tackle child pornography, to name a few initiatives. Yet law enforcement agencies lack a comprehensive understanding of digital black-market activity and the requisite technological and forensic investigation skills.

India needs to take a three-pronged approach to address this threat.

The author is Fellow, International Security Studies Programme, Gateway House