| CYBER SECURITY |

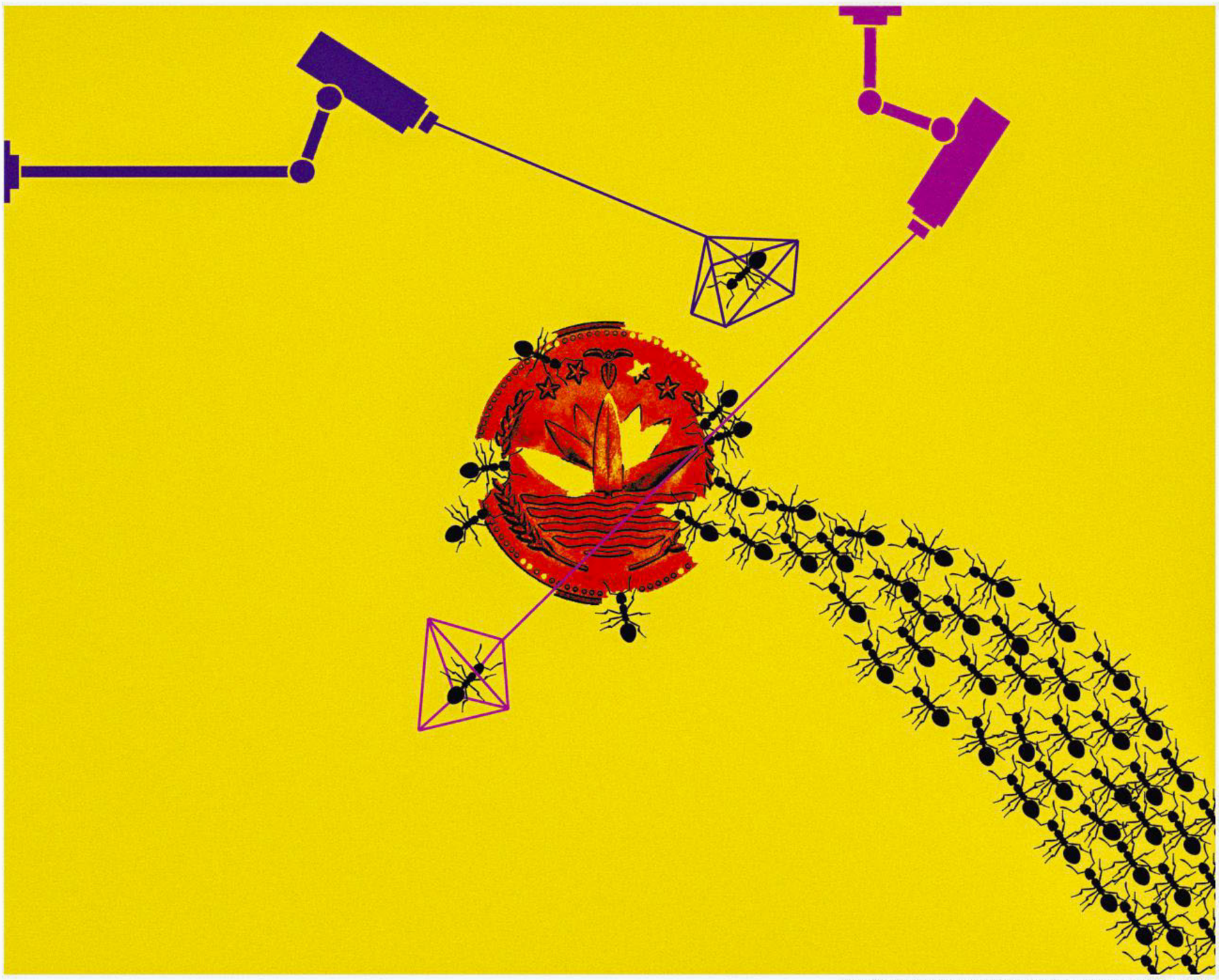

ILLUSTRATION: KAZI TAHSIN AGAZ APURBO

ADDRESSING CYBER SECURITY RISKS IN THE FINANCIAL SECTOR

ERESH OMAR JAMAL

The momentous growth in the digitalisation of the finance industry over the last decade(s) has transformed the sector to a point where an increasingly wide variety of financial services are now becoming available to more and more people, faster than ever before.

Not only is this because digitalisation allowed us to connect across greater distances; but it also expanded our storage and processing power, thereby, enabling our financial (and its subsidiary) systems to get bigger and more complex.

In that regard, what many may not know is that when you increase linearly the intricacies of a complex system, the risk associated with it goes up exponentially, as a consequence. That is why it is always important to have additional safety measures placed into a system that is advancing in complexity, to serve as a counterbalancing force against the heightened systemic risk.

Unfortunately, this is one lesson we have been taught the hard way—or have at least been made to dearly pay for, regardless of whether we've learnt the lesson or not. By that, I am, of course, referring to the Bangladesh Bank (BB) heist, whereby more than USD 80 million was stolen (some of which has been recovered) by hackers from the Bangladesh central bank, via the Federal Reserve Bank of New York, before being transferred to the Philippines and laundered through its casino system—another USD 20 million was successfully traced to Sri Lanka and has since been fully recovered.

Investigations in Bangladesh, the Philippines and the FBI following the BB cyber heist revealed something even more concerning—that hackers were able to exploit weaknesses in the "supposedly secure global money transfer system known as SWIFT", which banks use for major money transfers between themselves, according to *Al Jazeera*. But the specifics of what weaknesses were exploited in the SWIFT system are yet to be made clear.

At one-point SWIFT even refuted this claim, blaming rather weaknesses in the security of the Bangladesh central bank for the breach. According to SWIFT, hackers had used relatively simple malware to target the BB's computer system to bypass the primary risk controls, initiate irrevocable fund transfer processes and tamper with statements and confirmations that would normally act as secondary controls.

Having initially denied SWIFT's claim, BB hired a US-based firm to lead the investigation. And their investigation, similar to SWIFT's, found "footprints" of malware of hackers, which also indicated towards a breach in its system.

An internal forensic investigation by the BB found that this malware was installed within the bank's system sometime in January 2016, and

Continued to page 5

An internal forensic investigation by the BB found that this malware was installed within the bank's system sometime in January 2016, and had been sitting there for a month gathering information on the bank's operational procedures for international payments and fund transfers.