The new face of crime is artificial

Interpol races to stay ahead as criminals use fast-evolving AI technology

New tech: (Above) A file photo of analysts working at the Interpol cybercrime intelligence unit and, (left) drones used for research at the innovation centre's digital forensic lab at the Interpol facility in Singapore on Jan 29. — AFP

Singapore FROM perfectly spelt phishing emails to fake videos of government officials, artificial intelligence is changing the game for Interpol's cat-and-mouse fight against cybercrime at its high-tech war rooms in Singapore.

Their foe: crime syndicates, structured like multinational firms, which are exploiting the fast-evolving technology to target individuals, states and corporations for billions of dollars.

"I consider the weaponisation of AI by cybercriminals ... the biggest threat we're seeing," Neal Jetton, Interpol's Singapore-based director of cybercrime, said.

"They are using it in whatever way they can," added Jetton, who is seconded to Interpol from the US Secret Service, the federal agency in charge of presidential protection.

AFP was granted a look inside the global organisation's multi-pronged cybercrime facility, where specialists pore through massive amounts of data in a bid to prevent the next big ransomware attack or impersonation scam.

Jetton said the "sheer volume" of cyber attacks worries him the most.

"It's going to only expand, and so you just need to get the word out to people," so they understand "how often they're going to be targeted", he said.

AI technology is allowing criminals around the world to create sophisticated voice and video copies of well-known figures to endorse scam investments, and helping make dodgy online messages appear more genuine.

Jetton warned that even low-skilled criminals can purchase ready-made hacking and scamming tools on the dark web – and anyone with a smartphone can be a target.

Black market

The facility is part of the Interpol Global Complex for Innovation, not far from the Singapore Botanic Gardens.

It is the organisation's second headquarters after Lyon in France, and houses the Cyber Fusion Centre, a nerve centre for sharing intelligence of online threats among 196 members.

Another office in the complex studies emerging online threats, while a digital forensics lab extracts and analyses data from electronic devices like laptops, phones and even cars.

A command-and-coordination centre, like a mini space mission control with staff facing big screens, monitors global developments in real time during Asian hours.

Intelligence analysts scrutinise millions of data points – from web addresses and malware variants to hacker code names – that could provide leads in active investigations.

Christian Heggen, coordinator of the Cyber Intelligence Unit, said they are up against a "large ecosystem of cyber criminals" who use "a number of different attack vectors".

"They get quite creative.

"It's a whole black market of spying and selling stolen data, buying and selling malware. We have to understand that ecosystem," he said.

To strengthen its capabilities, Interpol partners with private firms in finance, cybersecurity and cryptocurrency analytics.

"It's always a cat-and-mouse game, always continually developing. That's why a department like this is quite important, because we can provide the latest intelligence and information," Heggen said.

AI has no soul

Last year, Interpol's cybercrime directorate coordinated "Operation Secure" in Asia, which saw 26 countries work together to dismantle more than 20,000 malicious IP addresses and domains linked to syndicates to steal data.

Another anti-cybercrime operation across Africa, called "Operation Serengeti 2.0" coordinated from Singapore, saw authorities arrest 1,209 cybercriminals who targeted nearly 88,000 victims. More than US$97mil (RM384mil) was recovered and 11,432 malicious infrastructures were dismantled.

Jetton said Interpol supported the crackdown on the online scam centres in South-East Asia through intelligence-sharing and resource development.

The Innovation Centre's head, Toshinobu Yasuhira, a Japanese officer seconded from the National Police Agency, said advances in deepfake technology have become a growing concern, but one of his deeper worries lies ahead: AI acting beyond human control.

"Should we arrest people who programme the AI, or who utilise AI, or should we arrest the AI itself?" he said in an interview.

"It's kind of very difficult because AI doesn't have any soul, heart."

Paulo Noronha, a digital forensics expert from Brazil's Federal Police, demonstrated some of the lab's high-tech tools designed to keep investigators a step ahead.

Experts at the lab are working on the further use of virtual reality, augmented reality and quantum technology against cyber criminals.

"It's up to us to stay ahead of criminals," he said.

"That's why we have systems like these."

For Jetton and his colleagues, the fight rarely enters the public eye, but is vital to global security.

"We try to be as confidential as we can," one intelligence analyst said.

"We're providing key support for operations and investigations around the world." — AFP