Unmanned robot dog, future-proofed crypto chips: Homegrown defence tech innovations

The DSO's robot dog Harrier (left) can team up with other robots like Foxhound to generate maps of unknown areas. PHOTO: ST FILE

Lim Min Zhang
Assistant News Editor

PUBLISHED JUL 25, 2022, 5:00 AM SGT

SINGAPORE - From a future-proofed cryptography chip to artificial intelligence (AI) models that can detect unknown malware, these are some of the latest defence technology projects the DSO National Laboratories is working on to guard against future threats.

They were unveiled in a recent exhibition at the DSO Complex to mark the defence research and development organisation's 50th anniversary.

Autonomous robot dog can team up with other bots for surveillance

Surveillance of unknown areas, especially urban environments, can be made safer and more efficient in the future with the use of robots such as the four-legged Harrier.

The unmanned vehicle, which resembles a dog, can navigate tight spaces and climb stairs while generating 3D maps of its environment in real time.

It is also able to operate in areas which do not have access to the Global Positioning System (GPS).

The key innovation lies in the "brains" of the Harrier, called the autonomy payload kit, developed by a team led by robotics system engineer Elaina Koh, 37.

Ms Koh said the team from DSO is working on enhancing the robot's intelligence so that it can better respond to changing situations in the environment.

"Let's say there is one entrance that is blocked in the unknown area. With upgraded intelligence, the Harrier will know how to find an alternative route to get to the destination," she said.

The Harrier can also team up with other robots, such as the Foxhound - a larger unmanned vehicle on wheels - to explore areas without the need for operator control.

Both robots can complement each other, said Ms Koh.

The Foxhound, which has more power and computing capacity, can store information fed to it by the Harrier, for instance. But the Harrier, being smaller, can manoeuvre more easily in indoor areas.

While the DSO team is currently experimenting with teams of two or three robots, "in the future, we are thinking of scaling it up to maybe five, six, or even 10", added Ms Koh.

Cryptography chip stays robust against quantum computers

The need for secure communications led a DSO team to develop its first cryptography chip.

The chip, which encrypts and decrypts data, can be embedded and integrated in multiple devices.

The team began developing the chip in 2014 and it is currently in use, but details cannot be revealed due to security reasons.

The chip is about five times smaller and five times lighter, and consumes five times less power, than an over-the-counter equivalent.

Dr Ti Yan Bo, 33, a senior cryptography research engineer at DSO, said creating the chip in-house allowed the team to control the entire developmental process.

"We are... more confident that there are no malicious bugs in them," he said.

Dr Ti, who has been with DSO for nine years, added that another advantage is versatility.

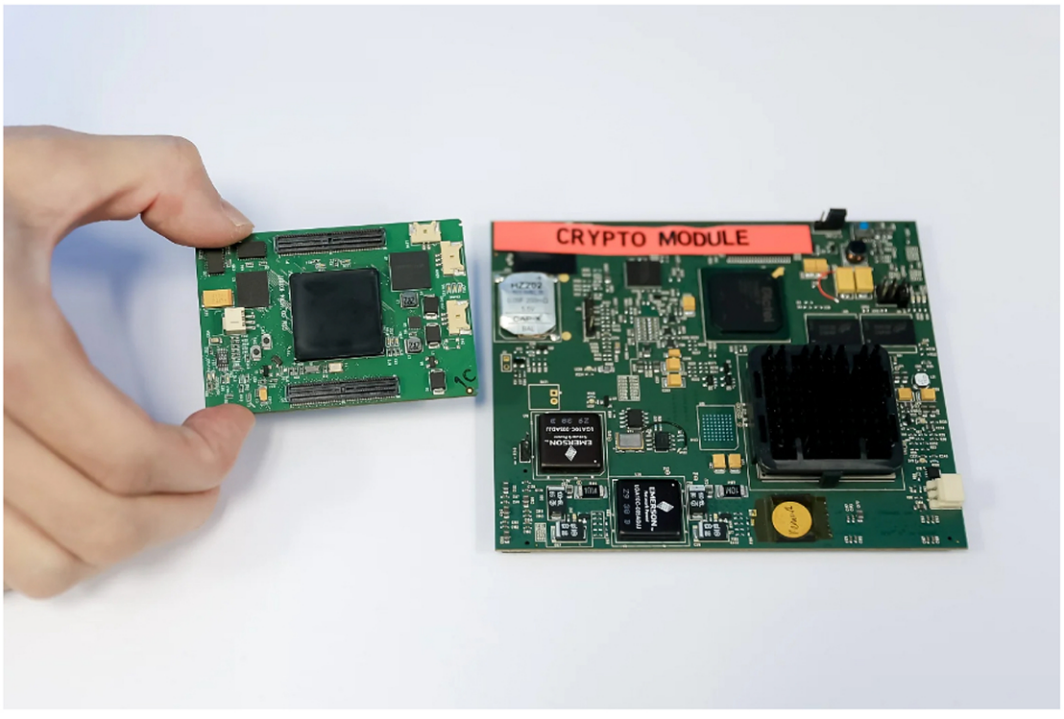
Using custom algorithms allowed the encryptors to be used on more platforms.

Cryptography techniques allow secure communication over insecure channels. This is done by rendering messages unintelligible to third parties. Only authorised parties with the right keys will be able to unscramble the messages.

But advances in quantum computing present future challenges for the chip. Quantum computers are machines that can solve mathematical problems that are difficult for conventional computers, and could break many of the cryptography systems currently in use.

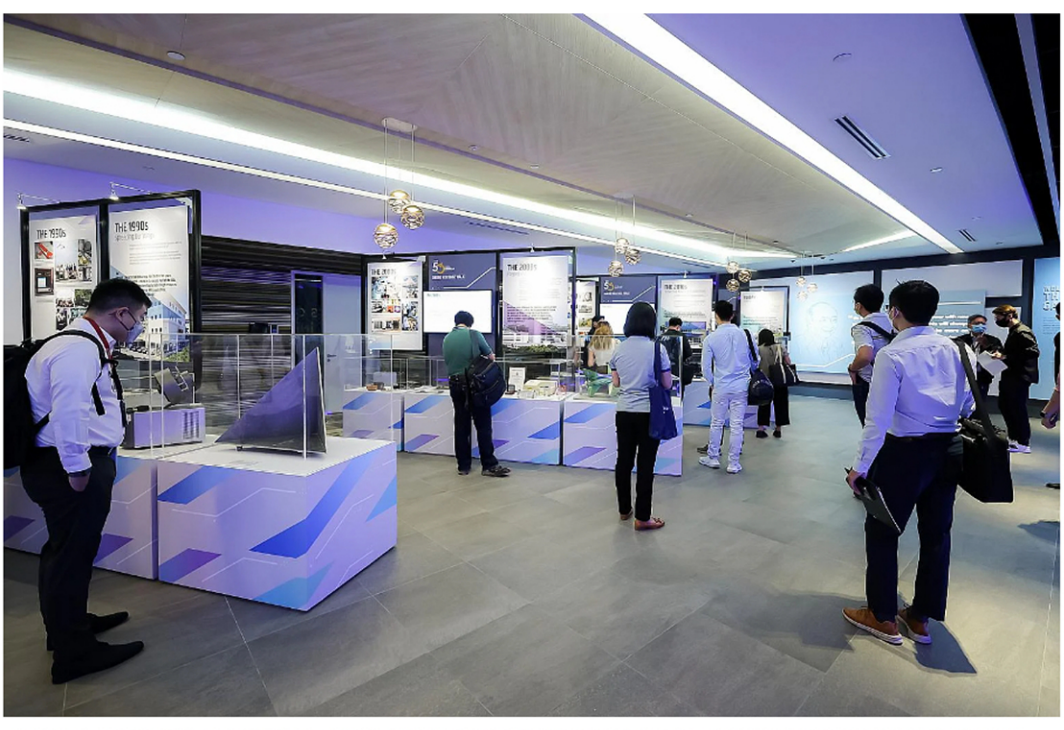
Dr Ti said the DSO team has identified that quantum computers will target certain structures in current systems or schemes.

"We are sure that the crypto chip is robust, but we must not rest on our laurels and keep innovating," he added.



The DSO crypto chip module (left) compared to the commercially available crypto module. PHOTO: ST FILE

Detecting and analysing unknown malware using AI



Engineers are applying AI-powered techniques to detect abnormal behaviours in an organisation's computer systems. ST PHOTO: GAVIN FOO

While commercial anti-virus software can detect known malware, unknown malware engineered by sophisticated attackers, such as state-sponsored ones, could evade such detection.

Traditional anti-virus solutions use databases of known malware signatures to identify and deal with the malware. But signatures are not available for unknown ones.

To solve this problem, DSO engineers are applying a technique known as behavioural analysis, powered by AI, to detect abnormal behaviours in an organisation's computer systems.

This method is based on the knowledge that malware would have to interact with the system to achieve its goals, such as stealing information.

"Such behavioural deviations provide us a way to detect unknown malware," said Dr Teo Hong Siang, 50, a principal cyber-security researcher at DSO.

This system is being piloted across government agencies.

AI is being used not just in detection, but also in analysing malware to identify its capabilities.

Dr Khoo Wei Ming, 44, who is also a DSO principal cyber-security researcher, said going through hundreds of pages of code in a typical malware sample is a tedious and labour-intensive process that can take days or weeks.

The team developed a code-matcher to significantly reduce the amount of code that needs to be analysed manually. This is based on the insight that programmers, including malware authors, reuse and copy code.

Testing this method on a malware program called PingPull, the DSO team reduced the code that needs to be analysed by 77 per cent. This reduction allows analysts to analyse the malware with much less effort, said Dr Khoo.