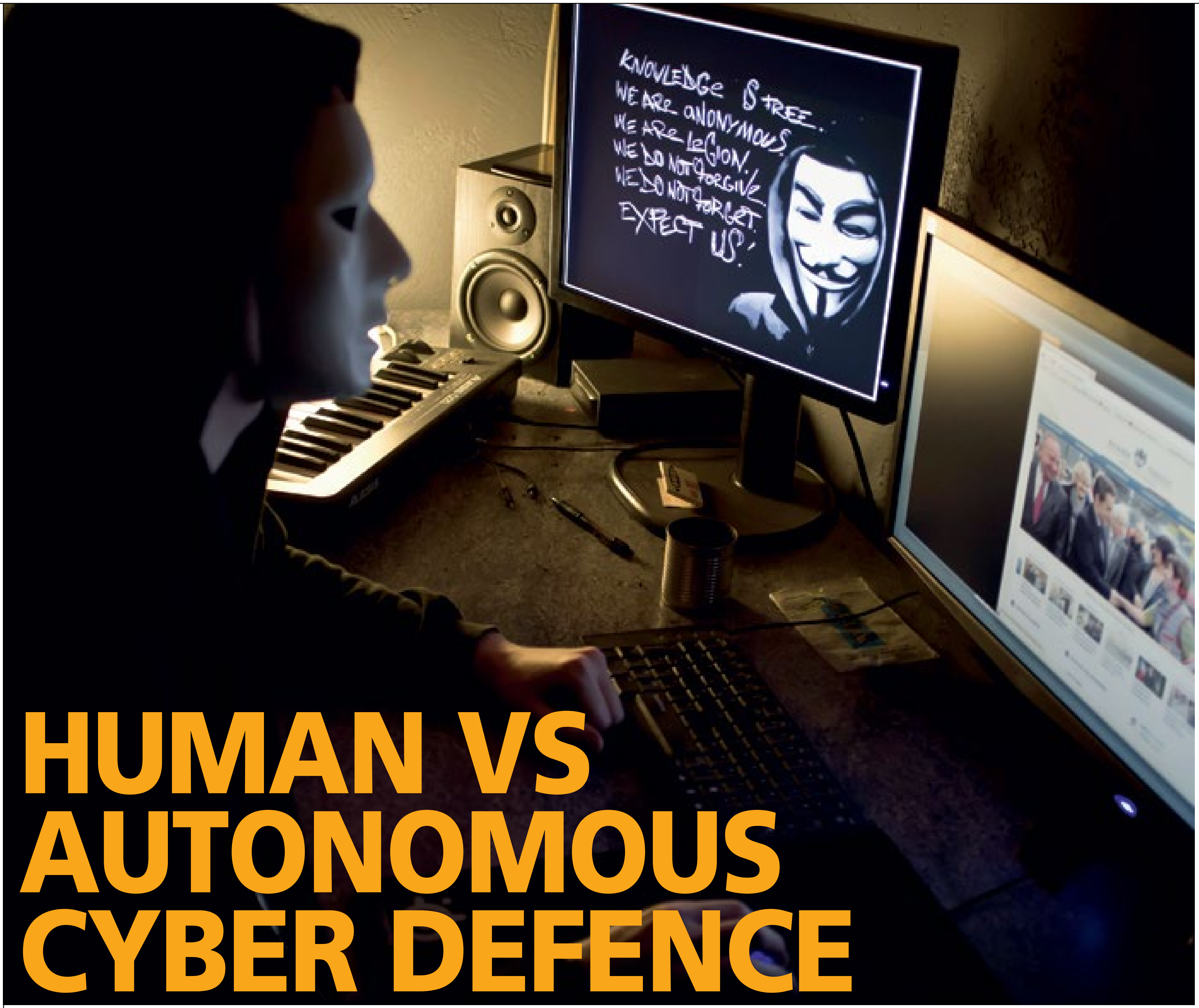

Picture credit: Getty

HUMAN VS AUTONOMOUS CYBER DEFENCE

Paul Theron *examines the importance of cyber defence specialists and why it's vital that the shortfall is made up as soon as possible*

There's an estimated shortage of 50,000 cyber defence specialists in the UK, and up to two million worldwide. In July 2018 the UK Parliament's Joint Committee on the National Security Strategy published a report describing a 'chronic' lack of digital skills, even when it came to the Government's own security bodies. While the UK may have one of the most advanced digital economies, there isn't the foundation of skills to provide protection for the organisations and individuals investing their faith and their funds into it.

Despite the obvious career opportunities and salaries estimated to be 15 percent above other comparable IT roles, the number of young people opting for IT-related qualifications in schools is falling (down 17 percent this year says the British Computer Society). In 2018 UCAS reported fewer students interested in taking STEM subjects in general. We want a digital economy, we want to be consumers of slick IT services, but at the same time we don't necessarily want to be stuck dealing with its ugly complexities, the breakdowns and crises. What doesn't help is the lack of a well-known and recognised career pathway of training and development into cyber security careers.

MATCHING SKILLS TO DEMAND

On the back of its report, the Joint Committee on the National Security Strategy is pushing for a national cyber-skills strategy, calling for the Government to work with industry to put together a skills education policy that matches with actual organisational needs for the long-term, alongside more continuing professional development for educators to ensure skills are moving to the right levels, in the right ways, for this fast-evolving domain. There are plans for attracting the necessary 'critical mass' of new younger recruits, for up-skilling and re-skilling of general IT staff in cyber security, as well as using aptitude rather than qualifications as a basis for recruitment. In a bid to reinforce the status of people and their skills in the field, The Department for Media, Culture and Sport is involved with setting up a professional body that can grant royal chartered status to cyber security professionals. But it's also been admitted that this will take time, 10 years or more, to have the necessary effect. And in the meantime, in the UK and across global networks, IT systems used by many organisations – both old and new – are looking more stretched, more exposed and more fragile. While larger enterprises have the resources to invest in the range of monitoring, protection and defence tactics, they will continue to be exposed through their supply chains of smaller partners, by growing levels of collaboration, new forms of interconnectivity and the adoption of data-sharing technologies.

> THE NUMBER OF YOUNG PEOPLE OPTING FOR IT-RELATED QUALIFICATIONS IN SCHOOLS IS FALLING

The scale and level of organisation behind the threats will look very different by then. There has already been a sharp evolution of cyber attacks from hobby to organised, targeted and strategic activity, and this will only accelerate. Cyber attacks have increased in number and the cyber threat is today's 'new normal'. Attackers' goals are increasingly ambitious; they tend to multiply attack vectors and targets and to continuously increase the sophistication and diversity of their attacks. They attack cyber defence mechanisms themselves to perpetrate in-depth attacks, with low-key wide-ranging attack strategies used with a view to generating severe systemic impacts. Attack technologies have improved from simple programs overriding systems' functionalities, to scripted pervasive software capable of replication and designed to take control of systems' security privilege management functions, and finally to remotely controlled software agents that can be activated by a command and control server which is masked behind layers of camouflage, false IP addresses and routes.

This 'new normal' creates a climate of permanent uncertainty and distrust both in systems and societal forces, and even in people operating or simply using systems. As technology makes progress, attack technologies will progress again, with reports that Autonomous Intelligent Agents for cyber attacks are already being developed to defeat current cyber-defence technologies and to increase attackers' strike power against teams of human experts. Cyber defence involves some tricky tactics. A clumsy response from a cyber response team, looking to just switch off a system or stop a piece of malware, can spark even more damaging retaliation in terms of wiping data or causing IT paralysis. Humans can be good at developing responses, but are mostly late and slow, especially when it comes to complex systems.

Besides, the focus of research and development in cyber security is too much skewed towards the area of protection: to the upgrading of security measures, like cryptography, firewalls, anti-virus software, authentication methods, *etc*. All of these are important building blocks for cyber security. However, organisations need more specialist people to deal with breaches of those basic security systems, working on a response to attacks, and to ensure lessons are learned. Cyber resilience needs to include both cyber security and cyber defence.

AUTONOMOUS SYSTEMS

Developing autonomous cyber defence systems can provide the next level of sophistication needed to monitor and manage this escalation. The growing use of big data and machine learning techniques will provide the 'always on' supervision power that any number of skilled cyber professionals couldn't compete with. There's the potential for swarms of proactive, self-learning cyber defence agents to be used to work across the web on the side of national infrastructure and lawful activities.

Multi Agent Systems are made of a set of individual agents. Its multiple agents, while acting locally on the basis of their individual knowledge and rules, cooperate together towards a common goal, which requires some form of collective intelligence. They are close to naturalistic behaviours such as ants and bees, their connectivity is in line with the doctrine of information superiority through high connectedness, their versatility implies a vast number of configurations and functions for a wide variety of issues, they help the decentralisation, distribution and sharing of resources and decisions.

They are a set of software or hardware (possibly human) entities, including sensors, actuators, repositories, cyphers, transmitters, cognitive functions. The agents embed their own methods, policies, self-management capabilities, resources, energy-generation features and capacities for hiding, detecting and understanding attacks and their various signals; they are capable of devising their own reaction plans, keeping 'Situation Awareness' for sense making and changing or optimising reaction plans as and when circumstances require. They use local and distributed resources to perform or optimise tasks, collaborating with human operators as and if needed, at the same time as learning and improving their own capabilities.

The autonomous system of agents interacts through rules and methods, interfaces, communication and cooperation protocols, discovery and invocation procedures, runtime enablers – in this way creating collectively the intelligence. So not just exchanging data but building together their own emerging capabilities required to carry out cyber defence missions, able to adjust their goals and make decisions and choices in response to the changing context. They work according to a set of *ad hoc* policies, either administrator-defined, or devised or optimised according to actions and circumstances.

SPOTTING PATTERNS

As a result, these can be designed to recognise patterns of actual and potential attacks and the agents can be used to manage the most appropriate forms of counter measures for each individual attack. The report of their activity can be used by experts to recommend and implement adaptations based on greater breadth and depth of knowledge. These autonomous agents will flag only when expert human intervention or a key judgment call is needed – so merely requiring occasional oversight and input.

This is one future of cyber defence that can offer a through-life and affordable option for supporting large-scale and complex systems, like the Internet of Things, as well as for civil and military operations. It's an approach that needs serious testing before being put into practice on the live web. With this in mind, Cranfield University is creating a large-scale Internet of Things simulator, involving interactions with and between millions of objects. It will provide the kind of rich, complex and fast-moving cyber environment that's needed for replicating modern levels of Internet of Things transactions and those still more advanced to come.

Autonomous cyber defence is for the medium-term – we're talking in terms of being operational within seven to 10 years – but this approach needs to be part of cyber-defence planning now, for taking a pro-active, future-looking stance rather than being in a position of always chasing problems, generating ever more interest from cyber criminals. It will also become essential in a context where the attacks are being run through their own Multi Agent Systems, which would be impossible to defend against with solely human expertise.

HUMANS CAN BE GOOD AT DEVELOPING RESPONSES, BUT ARE MOSTLY LATE AND SLOW

We're still at the stage where fundamental, blue sky research is urgently needed to turn a collection of principles and smart ideas into working technology. That means, therefore, the early attention and involvement from a wide range of beneficiaries: from Governments with the key responsibility for defending national infrastructure and economic security, to state defence institutions, national intelligence agencies and the wider defence and security industry ●

Paul Theron is Professor of Cyber-secure Engineering Systems and Processes at the Manufacturing Informatics Centre, Cranfield University. Paul continues to be an active member of NATO's IST 152 Research & Technology Group on Autonomous Intelligent Agents for Cyber Resilience.