NewStatesman

Spotlight

CYBER SECURITY: PROTECTING THE ECONOMY

Ciaran Martin / Margaret Beckett / Margot James

Politicians should read more sci-fi

In August 2013, a cognitive neuroscientist called Andrea Stocco sat down in front of a computer in his department at the University of Washington. On the screen was a simple computer game. Stocco cleared his mind and waited until, without warning, his hand twitched on the keyboard, pressing a key to fire a cannon in the game.

This experience, while it might have appeared mundane, was a milestone in Stocco's field. It may even be this century's equivalent of Alexander Graham Bell's first call. Because, as Stucco explained, "it wasn't my brain that was moving my hand". His hand had pressed the key in response to an impulse transmitted from the brain of another scientist, the computer science professor Rajesh Rao.

At the time, Rao described the experiment as "a very small step" on the long road to brain-to-brain communication. But in the five years since, more small steps have been taken. In 2015, Stocco successfully demonstrated that people wearing caps that measure and alter electrical activity in the brain could transmit the answers in a game of "20 questions", using thought alone. Last month, Stocco and his colleagues completed a paper on what they have called "BrainNet", which they say paves the way for "a 'social network' of connected brains".

Consumer technology based on this research is decades away. But the one constant of technology policy in the digital era has been that it is always at least one step behind innovation itself. From mass surveillance to cryptocurrency to deepfakes and digital propaganda, the risks technology represents to life and free societies are described in the pages of sci-fi novels before they are rewritten into research papers, patents and, eventually, legislation. As technology grows more and more powerful, it will not be sustainable for politicians to wait and see. If the technology of tomorrow could offer the means to interface – and therefore also to intrude – on the inner citadel of human thought, then it is time to decide the principles that govern its use today.

NewStatesman
Standard House
12-13 Essex Street
London, WC2R 3AA
Subscription inquiries:
sbrasher@
newstatesman.co.uk

Account Manager
Ché Hennessy
+44 (0)20 3096 2272

Commercial Director
Peter Coombs
+44 (0)20 3096 2268

Special Projects Editor
Will Dunn

Special Projects Writers
Rohan Banerjee
Augusta Riddy

Design and Production
Leon Parks

Cover illustration
Sam Falconer

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017 WINNER

***Spotlight* is the British Society of Magazine Editors' 2017 Launch of the Year.**
First published as a supplement to the *New Statesman* of 19 October 2018. ©New Statesman Ltd. All rights reserved. Registered as a newspaper in the UK and US. The paper in this magazine is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.
This supplement can be downloaded from: newstatesman.com/page/supplements

News

PAUL ELLIS/AFP/GETTY IMAGES

Facebook's new eye comes with a patch

Will Dunn

The social media giant announced two new "Portal" video-calling devices last week, each with a surprisingly low-tech add-on – a plastic clip that can be placed over the camera to prevent hackers spying on users' homes.

A button on the device also "physically disconnects the camera and microphone", says the Portal website, which also explains that the device "does not use facial recognition" or "listen to, view or keep" calls.

In 2016, a picture posted to Instagram by Facebook founder Mark Zuckerberg drew widespread attention when a laptop seen in the background was shown to have its camera and microphone obscured by tape.

The launch came just ten days after the site's "View As" feature was found to have allowed the theft of "access tokens" used to log in to nearly 50m accounts. Weeks earlier, a Pew Research survey of more than 4,500 Americans found that more than a quarter had deleted the Facebook app from their phone in the last year, and more than half had adjusted their privacy settings.

Heathrow loses £120k on USB stick

Will Dunn

The Information Commissioner's Office has fined Heathrow Airport Limited (HAL) £120,000 after a USB stick containing highly sensitive information was found on a street in West London and handed in to the *Sunday Mirror*.

The newspaper reported that the device, which was not protected by passwords or encryption, contained 2.5GB of information including maps of secure rooms, CCTV cameras, maintenance tunnels, radio codes used in emergencies and personnel who were exempt from screening processes.

However the ICO's fine concerns HAL's failure to protect personal data held among the more than 1,000 files on the stick, which included passport details and other information "sufficiently detailed to facilitate identity fraud". While the ICO accepted that the blunder was not deliberate, it noted that just two per cent of the airport's 6,500 staff had any data protection training. While the ICO found that HAL knew the dangers involved, it "failed to take any" of the reasonable measures available to protect the data.

The fine will be reduced to £96,000 if paid without appeal by 5 November.

Conservative app compromises MPs

Augusta Riddy

The first day of the 2018 Conservative Party conference was marred not by collapsing slogans, but collapsing privacy controls. The conference app, which included information on events and speeches, suffered from a serious glitch which allowed anyone to log in to a delegate's account with their email address and no password. Once logged in, it was possible to access the personal details, including phone number, of that account holder.

Delighted Twitter users claimed that Boris Johnson's app picture had briefly been changed to something very unministerial indeed, and pornographic.

Arriving in Birmingham, Theresa May declined to comment on the mess. Labour MP John Trickett did not miss the opportunity to suggest that "the Conservative Party should roll out some basic computer security training to get their house in order."

SHUTTERSTOCK/JULIUSKIELAITIS

FCA fines Tesco over 2016 breach

Dorothy Musariri

The Financial Conduct Authority (FCA) issued its first cyber security-related fine to Tesco Bank for failing to protect their customers in a 2016 breach. The ruling comes after an attack that stole £2.26m from around 9,000 account holders.

The watchdog said the bank failed to show "due skill, care and diligence" in protecting its personal current account holders in a "largely avoidable incident".

Mark Steward, executive director of enforcement and market oversight at the FCA, said: "In this case, the attack was the subject of a very specific warning that Tesco Bank did not properly address until after the attack started. This was too little, too late. Customers should not have been exposed to the risk at all."

He added that banks must ensure their financial crime systems and those who operate them work to reduce the risk of such attacks occurring in the first place. Tesco said it fully accepts the findings.

Academic hacks come from within

Rohan Banerjee

Analysis of cyber attacks against UK universities has suggested that many breaches to their computer systems are likely to be orchestrated by disgruntled staff or students. The government-funded education agency, Jisc, found that in 850 attacks in the last 12 months, there has been a "clear pattern" of attacks happening during term times and office hours.

Jisc's research into academic network breaches concludes that there are "suspicions that staff or students could be in the frame", motivated by factors such as poor experiences with campus administration, bad grades, low pay, or simply for the thrill of causing "chaos".

In one case, a distributed denial of service (DDoS) attack against a university network took place across four nights, specifically targeting the internet connectivity in one hall of residence. In this instance, a student hacker was found launching an attack to disadvantage a rival on an online multiplayer game.

But universities and colleges should dismiss the possibility of more advanced threats "at their peril", according to Jisc's Dr John Chapman. He said: "It's likely that more sophisticated attacks are designed to steal intellectual property, targeting sensitive and valuable information held at universities and research centres."

SHUTTERSTOCK/BEE BRIGHT

China steps up cyber aggression

Augusta Riddy

China has replaced Russia as the most prolific state sponsor of cyber attacks on the West, according to analysts. Crowdstrike, one of the largest cyber security firms in the world, has analysed thousands of attacks this year, and reported that the attacks targeted at firms, universities, governments and NGOs amongst other organisations, are motivated by a desire by the People's Republic for commercial gain rather than political leverage.

More than a third of attacks that occurred in the first six months of 2018 were waged on technology firms, with biotechnology firms particularly experiencing a spike in threats.

Crowdstrike had reported a decline in Chinese cyber espionage after September 2015, when presidents Xi Jinping and Barack Obama held talks to lower cyber tension and form a tentative, informal truce between the two countries. However, the recent cyber attack findings show that the mood has shifted again and "China is back," according to co-founder of CrowdStrike Dmitri Alperovitch. "They are back to stealing intellectual property on a massive scale."

The chief executive of the National Cyber Security Centre, Ciaran Martin, talks to Will Dunn about protecting the UK's businesses

"People could lose confidence in the digital economy"

There are two types of risk with which the National Cyber Security Centre, the public-facing arm of GCHQ tasked with making this country "the safest place to live and do business online", must contend. The first is the kind of attack that makes headlines – a "national-security type of attack", says Ciaran Martin, explaining that such attacks target "critical national infrastructure, hard infrastructure like electricity systems, and soft infrastructure like the press and the electoral system." Defending against such attacks, he says, "will always be a critical function of the state."

But there is another risk that, because it is more amorphous, makes fewer headlines. While a cyber attack on, say, a power station is "strategically significant in and of itself," says Martin, "attacks on individual businesses and small business normally aren't. But when you add them all up, the cumulative effect is of a significant and potentially very serious national challenge."

It does not follow, in this case, that small crime is necessarily less serious. Because malware can be endlessly duplicated at no cost to the attacker, a single programme could affect a large proportion of the 5.7m SMEs that employ 60 per cent of Britain's workforce. Even a small proportion could affect the wider market, says Martin. "If ordinary citizens are getting letters all the time saying, 'as required by law... your personal data has been breached', then there's a risk that people could lose confidence in the digital economy. Cumulatively, I think there is a significant, national-level risk from the aggregation of low-sophistication but very high-volume cyber crime."

Nor is smaller crime easier to defend against. In fact, Martin says it's actually "harder to organise ourselves as a country to defend against this sort of thing. It's easy, conceptually, to organise ourselves to defend the state. It's hard to do operationally, but conceptually it's just, we've got some adversaries out there, let's contest the space. This is much more difficult. This is about how you get a level of security that's good enough, that means that most digital services are safe enough, without imposing onerous costs that smaller businesses can't afford."

With pervasive, low-level cyber crime, it's important to recognise that most cyber criminals are themselves in business, often in a fairly small way. It is, says Martin, "fundamentally about return on investment." To send out large numbers of unsophisticated "phishing" attacks, he says, "carries very low costs. If organisations or individual networks are weakly defended, and the attacker

One exploit could affect thousands of businesses

gets in and can gain some advantage, that's going to be a successful route of attack for them. They'll keep coming back, and will be encouraged to attack similar targets in the UK. If, on the other hand, you make it that little bit harder – they might go somewhere else, frankly."

While sole traders and microbusinesses are at risk from indiscriminate viruses and ransomware – especially as their equipment is often older and less likely to be updated – larger businesses represent a more profitable target for direct attacks. Martin says he "wouldn't rule out a household name going out of business" in the near future due to "the desertion of customer confidence that might ensue" from a major cyber attack.

It's for this reason that the NCSC has released a "board toolkit" for businesses, in the form of five intelligible questions board members can ask their heads of information security. Martin sees no reason why board members can't get "a little bit technical" in these discussions. "Most companies will have extremely technical discussions about the implications of their pension liabilities," he notes. "They all seem fluent and conversant in that type of risk."

At the same time, Martin says the NCSC is "not asking anybody to be able to code. I am asking people to be able to leave the board meeting, confident that they've understood what they've heard."

Simply hiring a chief information security officer and giving them a seat on the board, says Martin "doesn't take care of the problem. It's what this person does and the support they have from the rest of the corporate leadership – which entirely depends on how much the corporate leadership understands what this person is talking about."

The five questions are aimed to provoke "plain English" discussions about cyber-hygiene subjects such as phishing, authentication and access to privileged accounts, but they also cover management subjects that board members should be familiar with, such as relationships and contracts.

These are issues where good decision-making is crucial. For example, organisations in both the private and public sectors are often locked into contracts, he explains, that limit them to a certain number of updates per year. "But with vendors offering patches all the time, we have heard of organisations using up all their requests for change by the end of January. It costs money to change these contracts. So then the board-level discussion you have to have is, for the remaining 11 months, what is the sensible risk balance? Should we buy ourselves out of this contract and take the hit, or should we let it run, and run at risk until we renegotiate? Those are the business decisions we're trying to equip people to take."

For businesses in the UK to make sensible decisions about cyber threats, however, they do at least need to be aware of those threats. Last month, it was reported that GCHQ and the Ministry of Defence were developing a 2,000-strong

Does "offensive cyber" mean more risk of friendly fire?

"offensive cyber force". This is a point of concern for some in the business community, because the tools developed by organisations such as GCHQ in pursuit of national security can directly affect civilian software and services.

Martin responds that the issue is "way more complicated than that, and there are very robust mechanisms for overseeing it. I'm not in charge of offensive cyber capabilities… but, for example, there are technologies out there which are very specialist, sold on the criminal market, that are used exclusively by child pornographers. Now, if we find a flaw in *that*, is it really against the national interest to withhold knowledge of that, and not fix it?"

No-one could reasonably object to the state cracking software used by paedophiles to mask their crimes. But in a least one case, security services may have developed a tool that threatened the operating systems of more than 80 per cent of the world's desktop computers.

Last year, current and former agents of the US National Security Agency (NSA) told the *Washington Post* that in 2012, they exploited a weakness in Microsoft's code that allowed them to access older Windows systems, used by hundreds of millions of computers worldwide. Rather than telling Microsoft, the NSA continued to use the exploit, which they called EternalBlue, for more than five years. Microsoft was not able to release a patch for the vulnerability until March 2017. Two months later, with huge numbers of PCs still unpatched, a piece of malware called WannaCry used the exploit to infect more than 200,000 machines in a single day. In the NHS, an estimated 70,000 devices were affected, including equipment used in surgery and blood storage. Production at the UK's largest car factory came to a halt.

The UK-USA agreement, which originates from the end of WW2, commits the NSA and GCHQ "to the exchange of the products" of surveillance, including "acquisition of information regarding communications organisations, procedures, practices and equipment." This has led the Open Rights Group, among others, to infer that GCHQ knew about EternalBlue. Neither security agency has confirmed or denied the accusations, but after the attack Michael S Rogers, then the director of the NSA, told President Obama that the NSA "failed to build an environment that protected these extraordinary secrets". Can the security services develop these "extraordinary capabilities" without endangering businesses and the public?

"We would never", responds Martin, "leave UK business and the UK population wide open to attack like that. Our job is to protect the UK; that's not the sort of thing we do."

The final element in the cyber security of the UK's businesses are the consumers that buy the products of those businesses. Martin says the NCSC is "trying, with DCMS, to do more to enable consumers, whether they're individuals or corporate consumers, to make choices based on evidence about the standards of security." One planned result will be "the equivalent of food packaging for internet of things devices. I think that's a really good idea. At the moment, in many areas, it's hard to differentiate on security as a consumer." Intel has forecast that internet-connected devices will soon outnumber humans by more than 20 to one; with such a huge market emerging, perhaps the best way to ensure businesses build security into this new world of "smart objects" is by guiding the power of consumer behaviour.

For businesses of any size that find themselves compromised or under attack, Martin says the single greatest mistake they can make is to attempt to cover it up. "In nearly five years as the head of operational cyber security for the UK, I've never seen an organisation benefit by being secretive, by closing ranks when they're faced with a cyber security problem, not contacting the authorities for help, or refusing help. I've never seen it end better."

And he reiterates that NCSC was established to help. Business, he says, "needs and deserves support from the government on this issue."

The power of partnerships

Collaboration is crucial to cyber security – but it's easier said than done, writes Professor Keith Martin, director of the Information Security Group at Royal Holloway, University of London

Much has been said about the need for academics, businesses and the government to work together to address the future cyber security challenges that society faces. This is a sensible proposition, as cyber security affects everyone, and each sector brings different strengths and capabilities. But words and aspirations are one thing; making these partnerships work is something else entirely.

Full credit must be paid to the UK government for setting the ball rolling with a number of initiatives, most of which stem from the National Cyber Security Strategy. The Academic Centre of Excellence in Research (ACE-CSR) scheme makes it easier for external partners to identify academic institutions with a critical mass of cyber security research capability and experience. The National Cyber Security Centre (NCSC) certified degree programme provides welcome pointers towards quality academic cyber security education programmes. And the NCSC's CyberInvest encourages partnerships between external funders and academic research institutions. All these contribute to a more cohesive cyber security environment.

Collaboration has a lot to offer. Meeting new people and finding out what they're doing is interesting, and working across sectors can be both satisfying, and good for your profile.

There are two barriers that fruitful partnerships must overcome. The first is a question of expectations. The motivations for academia, business and government are not always the same, so successful engagement requires the identification of common ground. The second, arguably more significant, issue is that good relationships need time to grow. And time is something we all seem to lack these days.

One of the initiatives that emerged from the first National Cyber Security Strategy was the establishment of two Centres for Doctoral Training (CDTs) in cyber security, one at Royal Holloway and the other at Oxford. Since 2013, these centres have funded over 100 doctoral students to undertake PhD research. The programmes involve a first year of immersive cyber security training, before students undertake three years of research. The first graduates from these programmes are now emerging to take up leadership roles across the cyber security profession.

The CDTs in Cyber Security have been extremely successful initiatives, not just because they are producing cyber security leaders, as intended, but because they demonstrate a vehicle for constructive cross-sector collaboration. External organisations actively support the training programme (this year the Royal Holloway CDT made full-day visits to the NCSC, KPMG, HP Labs and Thales), host three-month internships (recent hosts included IBM, NATO and The Cabinet Office) and play an active role in governance (advisory panel representatives include Roke Manor, PwC and DCMS). Through these relationships students have, amongst other successes, worked with Mozilla to develop the new TLS1.3 standard, improved performance of CloudFlare technology, and designed cyber wargames for boardrooms. Through these collaborations, CDT students make a real difference.

However, none of this has come easily, nor quickly. Good partnerships require investments from all sides – financially, emotionally and in terms of time. In cyber security we need more mechanisms for true partnerships to be given both the freedom and the time to develop, nurture and grow.

IN ASSOCIATION WITH

ROYAL HOLLOWAY
UNIVERSITY OF LONDON

How can finance be flexible, as well as secure?

In this age of financial services, customers expect a service that can be accessed anytime, anywhere. David Matthews, global director of sales, security solutions at Unisys, argues that this modern approach doesn't have to come with extra risks

IN ASSOCIATION WITH

UNISYS | Securing Your Tomorrow™

With the rise of cloud computing, the internet of things, and mobile and connected devices, financial services companies have been presented with a big challenge: reassessing and reviewing their existing approach to infrastructure security. Banking organisations need to protect their network infrastructure from a wide and varied range of attacks. Therefore, how can these organisations protect themselves when their customers are mobile, using a range of devices to connect to their platforms and services?

Excitingly, we now live in an age of 24/7 banking that can be accessed anytime and anywhere. However, the crucial question is how can financial services deliver frictionless banking to their customers whilst remaining secure? Increasing regulation and the rise of Open Banking presents new challenges to the existing model, while reputational and financial damage, caused by any data breach, can have a lasting impact.

The traditional firewall-based network security is expensive to deploy and manage at scale, which can be offputting for lots of companies. Trying to protect thousands of end points which can potentially leave critical data exposed, allowing an attacker to find a way in, is a daunting struggle, and one which many organisations are not on top of. Adding additional layers will only serve to frustrate the customers' experience and ultimately increase costs overall.

Operational and business issues which Stealth enables businesses to address

Unisys' Stealth programme focuses on network micro-segmentation that isolates critical assets, and also serves as a protective layer should the unthinkable happen.

The Unisys Stealth software suite protects an organisation's valuable assets with identity-driven microsegmentation. It is trusted by government and commercial organisations to secure sensitive systems, and it prevents and minimises the impact of cyber attacks across networks, environments and devices from inside and outside the perimeter.

As the product is identity-based, it enables your customers to have the flexibility they desire, irrespective of device or location, which is an essential quality in this age of service. Encryption is not just at the trusted end points, but at all points in between, for data privacy and integrity, and importantly that peace of mind.

How Unisys can help

Organisations and businesses working in financial services recognise that the mobility and flexibility of online services are central for delivering a frictionless customer experience. Unisys has worked with major banks globally to deliver innovative and class-leading solutions for the banking sector, enabling them to maintain the flexibility their customers desire while ensuring critical infrastructure is secure. Stealth is a scalable solution which can address your most demanding issues, whilst at the same time allowing your organisation the flexibility to tailor its services to your overall business process.

For more information, contact David at david.matthews2@gb.unisys.com

People are the key to a cyber-secure UK

Margaret Beckett, chair of the Joint Committee on the National Security Strategy, asks what good is new technology, if people don't understand how to use it?

Since 2010, the government has categorised major cyber attacks on the United Kingdom and its interests as a top-tier threat to our security. Given the series of attacks in 2017 affecting the NHS and the UK and Scottish parliaments, as well as reported attacks on British energy, communications and media infrastructure, it is not difficult to see why. The government's plans for an offensive cyber capability – through the joint MoD-GCHQ taskforce announced in the wake of the poisoning of the Skripals – and the exposure of a campaign of global cyber attacks by Russia's military intelligence service highlight that this important issue is not going away.

At the end of last year, the parliamentary committee I chair, the Joint Committee on the National Security Strategy, launched an inquiry into the cyber security of the UK's "critical national infrastructure" (CNI) – such as government, communications, energy, transport, water and health provision – which is essential to the smooth running of daily life and to keeping our citizens safe.

Cyber security is not just about technology. It is also about people. And during our inquiry we heard that a shortage of skilled people is one of the greatest challenges facing CNI operators and regulators in securing UK infrastructure against cyber threats. Our witnesses described a talent pool limited not only by the sheer scarcity of people with the precise mix of technical expertise required, but also by a failure to tap unused potential.

The present cyber security talent pool is notably lacking in diversity. For example, only a tenth of the cyber security workforce are women. Faced with this scarcity, we were told that, in addition, CNI sectors seeking to recruit were being priced out by the cyber salary packages offered in the private sector. Simply put, there are not enough people in the UK who both possess cyber

There is no analysis of the skills we lack

SHUTTERSTOCK/ JACOB LUND

security skills and are able and willing to work in the CNI sector.

Yet, despite identifying cyber attacks as a top-tier threat, the government shows little urgency in tackling this issue. Its own 2016 National Cyber Security Strategy (NCSS) identified the need to develop cyber security talent and the profession more broadly. Its key commitment was the creation of a standalone skills strategy, but the government told us that this strategy would not be published before December – an inexplicable delay of more than two years.

We were so struck by the scale and immediacy of the problem, and by the government's worrying lack of focus in addressing it, that, in July, we published an interim report on our CNI inquiry which was dedicated entirely to cyber security skills.

So, where should the government begin? By defining the problem. We were told in our inquiry that no comprehensive analysis exists of the types of security skills in shortest supply in the UK, the sectors of the economy (including CNI) most affected, or where – at the strategic level – these gaps leave the UK most vulnerable. There is also no conclusive analysis of how the UK compares with its international peers – its main competitors in economic and security terms.

Moreover, there is no single, shared understanding of what counts as "cyber security skills". Our inquiry found that it covers a range of specialisms. At one extreme is the deep technical expertise required to secure systems and devices (skills possessed by network architects and penetration testers, for example).

More widely, there are the skills required by the many whose jobs now involve a cyber security element (such as teachers, HR directors, lawyers and company directors). Then there is the basic cyber "hygiene" for which all employees are responsible. We concluded in our report that this analysis of this disparate range of skills is the obvious and essential place to start, as the government cannot hope to address the problem properly until it has defined it more rigorously.

We also highlighted the importance of involving industry in tackling the skills deficit. It is itself a source of expertise and is uniquely placed to articulate its current and future skills needs. The government should work in close partnership with both industry and academia, not only to put in place measures to meet short-term demand for cyber skills, but also to develop a longer-term pipeline.

Such measures should include: using education, both inside and outside the classroom, to create a strong foundation for the future skills base; industry being more creative in how it recruits and reskills employees, albeit with government support; professionalising the relatively immature cyber security industry through achieving Royal Chartered status; introducing robust cross-government coordination and accountability; and identifying a minister with clear lead responsibility for developing cyber security skills.

We also encouraged the government to extend already-effective programmes more widely. For example, the CyberFirst Girls Competition could be used as a model for future programmes designed to attract mothers returning to work into the cyber security profession. The Defence Secretary's recent announcement on "cyber cadets" in schools, who will learn the fundamentals of cyber security, might be also seen in this light.

Nevertheless, piecemeal efforts such as these will not in themselves provide the range and depth of skills required to defend our CNI against cyber threats. Without a stand-alone skills strategy, the government risks pursuing a number of individually worthwhile but disparate initiatives that fail to add up to more than the sum of their parts.

It is essential that the government, in partnership with industry and education, makes a concerted effort to address the yawning gap between the supply of and demand for cyber security skills – and does so urgently. There is much work to be done.

A home for cyber security innovators

LORCA is hoping to propel the next generation of cyber security solutions onto the market. Augusta Riddy heads to Stratford to meet the cyber saviours of tomorrow

From the exit to Stratford tube station, a free shuttle bus is available to take you to Here East, a "digital quarter" located in the Queen Elizabeth Olympic Park. Bespectacled millenials hop on board, clutching Pret coffees and tote bags. The bus pulls up at a set of airport-like glass buildings around a landscaped space where food trucks congregate. During the Olympics, these were the press and broadcast centres for the Games. Now, they're home to the London Office for Rapid Cyber Security Advancement, or LORCA.

Set up by the Department for Culture, Media and Sport, LORCA is an "accelerator" to foster promising cyber security firms that are expected to have a significant impact on the safety of UK business, the state, and civil society. Its first "cohort" of nine small cyber security companies joined the centre in July 2018. LORCA's director, Lydia Ragoonanan, explains that the firms will embark on "six months intensive support, [then] six months follow-on support to help them get to market quicker and have a real impact".

LORCA chooses which startups to support, Ragoonanan says, by identifying gaps in security."LORCA is focused on really understanding wider industry challenges, using those challenges as a way to articulate need and, based on that need, selecting scaling organisations." The inspiration, she says, was the 2016 National Cyber Security Strategy, in which the government committed to make Britain "secure and resilient in cyberspace". The strategy called for "an industry-led, industry-informed innovation centre based in London," explains Ragoonanan, "and for that centre to play a key role in developing new and emerging cyber security innovations." Alongside the innate value

LORCA

LORCA aims to be financially self-sustaining in three years

of security itself, cyber security's contribution to the economy – "high growth, high-earning jobs" was a motivation for setting up the accelerator.

This year's cohort was selected on the basis of three identified industry needs: privacy and making trust "a competitive advantage"; orchestration and gaining oversight "of everything going on within your architecture"; and using automation to "assist and help where the threats are". Next year's cohort will be based on cyber threats in utilities, such as energy and water, and the centre will be running a "needs accelerator" to understand specific issues in these areas.

DCMS has pumped £13.5m of initial investment into the centre, but the aim is for it to be self-sustaining after three years. To do this LORCA is "engaging a range of different corporate partners". So far Lloyds and Deloitte have joined forces with the centre, offering commercial support to its members and enabling them to conduct product trials.

As well as having the opportunity to work with industry titans, the "innovators" have access to a legal team, and technical and engineering support from the Centre for Secure Information Technologies (CSIT). Each company has the chance to go abroad on a trade mission, to "understand and be prepared for international markets when they need to be," says Ragoonanan. Perhaps most importantly, LORCA comes with plenty of contacts. Ragoonanan says the office makes "warm introductions for our cohort to industry leaders where we know that they have a need that we can match them with".

Finally, they have use of the swanky Here East, complete with an indoor "park" and open-plan modern working spaces designed to encourage collaboration. For many in the cohort, this is a significant advantage as it allows them to host meetings and work in close proximity to their colleagues without paying for an office. Tim Ward, director of cohort member Think Cyber Security, admits that his team are "digital nomads, working at home", but he uses the space to meet potential investors and industry contacts.

Think Cyber Security is "applying behavioural science" to cyber security with its Red Flags product, which drip-feeds security training "30 seconds at a time" to employees for lasting, more effective security awareness. "The research shows that 90 per cent of cyber attacks start with the human user… your people really need to be your last line of defence," says Ward. "There's lots of theory, behavioural and learning science out there that's not really being applied."

LORCA does not provide any funding to the companies in its cohort, unlike some other accelerators, and Ward concedes it would be "quite good" if it did. However, "instead they're giving us help, and I suppose the onus is on us to utilise the help, and get as much out of it." Think Cyber Security, he says, has benefited particularly from the work it's been able to do with Deloitte. "They

“A founder’s journey is quite lonely”

LORCA

steer us and give us advice, and they’ve created lots of connections for us.”

Before joining LORCA, Think Cyber Security won an Innovate UK grant, and was “starting to get a little bit of sales traction, so it felt that it was the right time to engage with something like [LORCA] to get publicity, and to get support on scaling.” With such a results focus – LORCA wants to grow up to 2,000 jobs and bring in £40m of investment over three years – the accelerator looks to companies that are “programme fit”, meaning that they are not startups, but ready to be grown and “make a material difference,” explains Ragoonanan.

John Tolhurst, chief commercial officer at Iotech, which has developed a software solution that secures internet-of-things (IoT) devices using encryption and authentication, says that the stakes for his organisation are “very, very high. It’s kind of win or lose.” He is currently on the hunt for a “seed fund”, and is using LORCA’s contacts for that purpose. “We need to commercialise the business; that’s what LORCA is about for us,” he explains. “It’s that rapid advancement, traction in the marketplace.”

“The programme is fantastic,” he says. For an organisation of Iotech’s size, getting a key meeting could take three to six months, whereas “we could achieve it in a fortnight here”. What he wants to get out of LORCA is clear: “The marker [of success] will be that we are funded with the seed fund we’re seeking now; we’ll achieve that by securing a number of proof-of-concept projects.”

For Ward, getting the most out of the accelerator will mean maing the most of its opportunities for having “some trials running, if not completed, with either Deloitte or Lloyds, because the trial data is very useful for us.”

By the time they leave, Ragoonanan wants the cohort innovators to have “more clients, more revenue” and to be more financially stable. “One would hope they feel geared in a better informed, better position to be able to adapt to new markets.” However, she is also hopeful that they will feel “part of a community”. “A founder’s journey is quite lonely,” she reflects, “so feeling like this is somewhere you can come back to is important.”

Ragoonanan has plans to transition the accelerator into a “cluster”, where cyber security professionals and fledgling companies can gather, interact, and take advantage of the services LORCA provides. “I think one of the benefits of a cluster effect, and a benefit of having an actual location to do this,” she says, is that it can be “a home for those innovators to come to.”

AI: friend and foe for IT security

Machine learning will shape the future of both cyber attacks and successful cyber security, writes Bharat Mistry, principal security strategist at Trend Micro

IN ASSOCIATION WITH

TREND MICRO™

AI is a classic double-edged sword: a technology that can be used by both attacker and defender to improve success rates. So what can AI offer the white hats?

Fundamentally, it's the ability to learn normal behaviour and then spot patterns in network data and threat intelligence feeds that human eyes might miss, enabling analysts to take action or automating threat detection and response. This is particularly important given the security skills shortages facing firms. It was claimed last year that the UK is heading for a skills "cliff edge" as older professionals retire without newer talent coming through to replace them. The shortfall globally is predicted to reach 1.8m professionals by 2021.

Security analysts are expensive and hard to come by, so by automating the discovery of threats with AI, you free up their time to focus on more strategic tasks, whilst improving the effectiveness of your cyber security posture. Speed is also of the essence when it comes to threat detection. The longer you leave a threat actor inside the network, the more data they can exfiltrate and the more expensive the resulting breach.

Speed is also important in spotting ransomware, which works even faster to encrypt an organisation's most mission-critical files. Machine learning can spot inconsistencies and subtle changes in the way the malware works to encrypt your files, which would otherwise be lost in the noise.

Pre-execution machine learning can even help firms to block malicious files before they've had a chance to infect the organisation. False positives are sometimes a challenge, which is why such tools are often run in combination with run-time analysis to ensure that what you're blocking is definitely unwanted.

However, on the flipside, there's huge potential in AI for malicious use. In fact, it could have made historic cyber attacks and breaches far more impactful than they were. Take WannaCry: it might have caused headlines around the world and disrupted a third of the NHS, but as a piece of malware it failed. It was too noisy, attracting the attention of security researchers soon after launch, and failed to provide its masters with a decent ROI.

AI could correct this. By installing learning tools on a target's network, attackers could listen in and baseline user behaviour, understand network traffic and communications protocols and map the enterprise. This would make it easy to move laterally inside the organisation to the targeted data or user – all without raising the alarm.

Social engineering is also much easier if you use AI tools to understand users' writing styles, and the context of their communications. Just think about a document review process. A hacker could monitor communications between remote employees and then insert a malware-laden document at just the right time, using an email with just the perfect tone and language to convince a user to open it. This is spear-phishing like you've never seen it: attacks that even the experts would have a hard time spotting.

AI is in many ways the cyber security arms race writ small. The only way we can manage the inevitable wave of black-hat tools designed to circumvent security filters and increase the sophistication of phishing, is to fight back in kind. It's going to be a bumpy ride.

Oscar Williams asks experts and Minister of State for Digital and Culture Margot James about why cyber security could provide opportunities for people with neurodiverse conditions

BEN BIRCHALL - WPA POOL / GETTY IMAGES

Thinking differently about cyber security

When Steve Morgan was 17, he devised a plot to steal his teachers' passwords. It was simple in theory, but more complicated in practice. Morgan wrote a copy of his college's terminal software, burned it on to a chip and replaced the original CPU with his own. A few days later, he covered his tracks by putting everything back in its place, and then passed on a list of redacted passwords to his college.

"No one could work out how I'd done it," he tells *Spotlight*. The college enlisted the support of IBM, whose staff were so impressed they offered Morgan a full scholarship to study in the United States. But there was a catch; he would have to spend seven years working for the company after graduation. "When you're 17 years old, seven years is a very long time," he recalls. "I didn't sign."

Reflecting on the hack more than 30 years later, Morgan says he was driven by curiosity alone. While some students may have used the data for nefarious means, the satisfaction of gaming the system was enough for him. "I'm curious," he says. "I have to know everything about everything."

The 49-year-old has always seen the world differently, but it was only recently that he discovered why. Earlier this year, Morgan was diagnosed with a form of autism known as Asperger's syndrome, after his sister saw the symptoms of the condition described on TV.

In the United Kingdom, just 16 per cent of autistic adults are in full-time work. While some such as Morgan show an exceptional talent for problem solving and pattern spotting, people with autism may struggle with interviews, away-days and the other trappings of office life. The world of work can seem at best intimidating and, at worst, impenetrable.

There is, however, a growing recognition in Whitehall that some employees with autism and other neurodiverse conditions can carry out specific tasks at a level that few others can match. In the right environment, people with autism flourish, and ministers now hope they could help solve some of the country's most pressing and complex problems.

Earlier this year, the Department for Digital, Culture, Media and Sport quietly

launched a six-month pilot fund aimed at boosting the number of women and people with neurodiverse conditions working in the cyber security industry. Women make up just 17 per cent of the British technology workforce, while the unemployment rate among people with autism in Britain is several times higher than the national average. Harnessing their skills could, the government hopes, help the UK to close the cyber skills gap and meet the rising threat posed by hostile states and cyber criminals.

"Companies, governments and public services are under almost constant attack through the cyber sphere, so it's absolutely vital for our national security and the protection of our public services and businesses that Britain has a really strong cyber security sector," says the Minister of State for Digital and Culture, Margot James. "But one of the biggest problems we've got now is the lack of skills. We have therefore taken a very proactive approach in looking at the sort of routes that have not necessarily had enough investment in them for people to come forward and opt into careers in cyber security."

The pilot initiative, dubbed the Cyber Security Immediate Impact Fund, provides funding for training centres to deliver courses equipping people with the skills needed to quickly find a job in the sector. Seven centres around the UK are currently participating in the scheme. Two focus exclusively on training people with neurodiverse conditions, while one targets women and another lone parents.

In June, Morgan became one of the first people to enrol in the scheme. After turning down IBM while he was at school, he forged a successful career as a tech professional in London before becoming a consultant at NatWest at just 25. But he found the world of work challenging, at times. "It's mainly from not understanding what my thoughts were," he says. "I loved the things that everyone else hated and hated things that everyone else seemed to love." After suffering a crisis of confidence, Morgan has been working in the local ambulance service for the last few years. He is now eager to make a return to the industry in which he first found his feet as a teenager three decades ago.

"The course provides a level of training you just don't normally get," he says. Immersive Labs, a direct recipient of the fund, delivers the learning modules, while a range of speakers, from chief security officers to researchers at cyber security vendors, make guest appearances every week. Morgan is one of 15 trainees taking part in the scheme at the Community Cyber Security Centre in Worcester.

James says the pilot has been so successful that the government is now investing a further £500,000 in the scheme and expanding it to other underrepresented groups around

Just 16% of autistic adults are in full-time work

the UK. “The pilots we’ve run so far have demonstrated a real passion for these capabilities and people are really responding well to the opportunity that this training investment is providing,” says the minister. “So we’re dramatically stepping up the investment to enable this to be rolled out across the country.”

In 2001, the journalist Steve Silberman wrote a groundbreaking report for *Wired* magazine titled “The Geek Syndrome”. The story documented the unusually high rate of autism diagnoses among the children of Silicon Valley workers. Its key message – that the region had attracted people with “autistic genes” – sent shockwaves through the California tech comunity. But for some tech workers, it came as little surprise. In the previous year, Microsoft had started paying for behavioural training for the autistic children of its employees.

Closer to home, the signals intelligence agency GCHQ has a long and proud history of employing neurodiverse staff, stretching back to the Bletchley Park era. Today, around 120 of its employees have a neurodiverse condition. “We are well known for celebrating neurodiversity and have many staff on the autistic spectrum,” the agency’s then director Robert Hannigan said in 2016. “They are precious assets and essential to our work of keeping the country safe.”

GCHQ employs around 120 neurodiverse staff

But not everyone shares Hannigan’s enthusiasm. Nearly 17 years after “The Geek Syndrome” was published, it’s feared British businesses are still failing to appreciate the value in employing neurodiverse staff. Emma Philpott runs the Worcester centre Morgan is enrolled in. Over the next few weeks, the government’s investment in the scheme will run dry, and Philpott has been asking businesses to plug the gap.

“I’m not sure that will be possible,” she says. “We get referrals from the police, the Department for Work and Pensions and the NHS every week or so. The need is there, but I don’t think the funding is there. Also, I realise the will is not really there for commercial companies to employ people who need a bit of extra support; they say it is, but it isn’t. For some companies it is, but employees have to be located near them, and it’s really hard.”

But for the businesses that are willing to invest in autistic workers, the payoff is huge, says Philpott. “The trainees are very talented, they’re lower cost than people who have been in the system for a long time and they tend to be very loyal, so there’s many, many things that make them particularly good as employees,” she says. “But they need some training and support to get them to the point where they can be employed. By investing in the scheme, businesses would really be investing in future employees.”

In lieu of big corporate backers, Philpott’s business, IASME – a cyber accreditation body – is putting £180,000 into the centre. The funding will secure employment for around a dozen people on the scheme for 12 months.
“The centre’s main aim is going to be providing affordable internet protection for the most vulnerable in society, who are targeted by criminals at the moment,” Philpott explains. “But also we’re going to act as a sort of temping agency. We’ve already had a company give us a discrete small package of cyber security work which can be done remotely.”

While Philpott has struggled to find a backer in time for when the government funding ends, she points out that “if it wasn’t for that grant, we wouldn’t have got going in the first place. It’s brilliant really. We’re going to run the centre for a year and see if we can cover our costs.”

Morgan is due to spend two days a week getting the security operations centre up and running, but he doesn’t see himself working there forever. “Looking back over my career, I love the project environment – being able to put in massive effort, get something working perfectly and then moving on to the next project.” What might that be? “I’m not actively applying for jobs, but I’m meeting so many people from so many organisations, I just have this feeling that the right thing will come along.”

Your cybersec is your business rep

In the eyes of consumers, hacks and data breaches are no longer down to just unscrupulous crooks; they're the fault of feckless organisations too, warns SysGroup chief executive Adam Binks

Yahoo, eBay, Sony, AOL, JP Morgan Chase, Uber. These aren't just some of the best-known brands around the world. They also share the dubious honour of being victims of some of the biggest known hacks and data breaches ever.

Yahoo can attest to the fact that size matters where breaches are concerned. In short, the bigger the breach, the bigger the potential recovery costs, legal costs and fines – and the firm's 2013 hack sits well apart from any other (that we know of). Every single one of its user accounts was affected, a staggering three billion in total.

But even after taking the numbers out of the equation, not all breaches are made equal. The extent of damage to an organisation's reputation is impacted by factors such as existing public perception, when a breach happens, and what industry an organisation is in.

Rightly or wrongly, Yahoo's troubles were exacerbated by its supposed position (and a self-perpetuated one) as a trailblazing internet outfit. The sort that should be savvy to such threats. Likewise, its reputation would have suffered less had the breach come to light in 2013 when it occurred, rather than later in 2016, with public opinion having become less forgiving with every new breach.

Conversely, last year's 146m customer breach at Equifax – the recently announced £500,000 ICO fine for which can be arguably be seen as a lucky escape, given the subsequent introduction of the GDPR – hasn't just been viewed in terms of whether the US credit rating agency should have known better, but whether it should have had more measures in place.

Organisations dealing in more sensitive information are, of course, obliged to have a higher level of security in place than others. For the public – regardless of whether the appropriate security is in place – a breach at any such organisation begs the question: should they be trusted with your information?

While it follows that consumers have become more hard-nosed about organisational cyber security, it is also quantifiably the case. A survey of US consumers last year by PwC found that "just 25 per cent of respondents believe most companies handle their sensitive personal data responsibly", with only 12 per cent trusting companies more than they did a year prior.

It is less and less the case that organisations can point the finger at the perpetrators of cyber crime and expect immunity – or even simply just have appropriate measures in place. Mitigating reputation damage means being prepared to demonstrate that best practice has been observed, communicate what measures have been in place and detail how they've performed.

Indeed, beyond mere damage limitation, Capgemini has found that cyber security is now a tangible "competitive advantage." Its research indicates that over three-quarters of consumers now view cyber security as the third most important factor when choosing retailers. Consumers, it says, are willing to spend more with retailers they trust, and trusted retailers can expect to see annual revenue increase by up to five per cent.

This is an era in which cyber security is no longer purely about systems self-defence. It's about reputational defence too. Like it or not, cyber security is now part of the communications mix.

Read more at www.sysgroup.com

Jonathan Lusthaus, director of the Human Cybercriminal Project in the Department of Sociology at the University of Oxford, explores a dangerous and evolving trade

Cyber criminals are not who you think they are

At the turn of the millennium, a group of Russian-speaking cyber criminals founded a website called CarderPlanet. This forum became a key online marketplace in the global trade of stolen credit card data, along with other illicit goods and services. One could view it as a criminal eBay of sorts, which significantly predated the much-hyped "Darknet" forums that dominate today's media coverage.

Led by a mercurial figure known by the handle "Script", it succeeded in establishing a professional model for how cyber criminal trade could be professionalised. Users could publish product reviews. Arbitration was provided for the site's vendors and customers who came into dispute. Meanwhile, other members could choose to more safely trade through an escrow service. An interesting feature of the site was that the forum officers adopted existing mafia ranks such as *Capo* (short for the Italian *Caporegime* which means Captain). The network appeared to be appropriating the mystique of both traditional organised crime groups and their popular depictions in films and TV.

This self-ascribed association perhaps contributed to a number of commentators and security professionals conflating cyber crime and organised crime. And, in some sense, it has now become a mainstream position. For instance, one expert quote in a CNN article stated: "The Russian mafia are the most prolific cyber criminals in the world." But how much empirical evidence actually supports the view that organised crime is taking over cyber crime?

I carried out a seven-year study into the organisation of cyber crime. The findings suggest that cyber criminals aren't necessarily who we think they are. And, with regard to the example above, they may not even be who they think they are. As part of this study, I conducted 238 interviews with law enforcement, the private sector and former cyber criminals – across some 20 countries, including fieldwork in purported cyber crime "hotspots" such as Russia, Ukraine, Romania, Nigeria, Brazil, China and the United States.

While I was open to the possibility of heavy mafia and organised crime involvement in cyber crime, I was surprised by how few cases of this I encountered. There are certainly instances where there is such a crossover. But there are many others where cyber criminals operate on their own.

One Eastern European former cyber criminal I interviewed called Andrey (all names have been replaced with pseudonyms), suggested: "All the relations between traditional mafia and gangs are eventual and personal, so there

SHUTTERSTOCK/THEA DESIGN

Hacking is a multi-million dollar industry

are no more connections than in any other industry or enterprise. Some individuals do, and if they do, they use it. Others don't." He went onto explain that, "of course, regular criminals show interest in certain aspects of cyber crime, but they show interest in many other things. More advanced carders and hackers, however, usually show strong disgust to 'traditional' criminals and usually join whatever cause there might be on a temporary basis. In turn, 'traditional' criminals often regard cyber criminals as 'milk cows' and nerds."

Another former cyber criminal in the region, Ivan, stated that he had never encountered a direct connection between cyber criminals and traditional organised crime groups. In South America, Thiago said that he and his collaborators never engaged with organised criminals, and actively avoided them.

Of the cases of organised crime involvement I did encounter, there appeared to be four key roles that serious criminals can play in cyber crime: protector; investor; service provider; guiding hand. These are largely tied to their existing skill sets and resources.

In terms of protection, one of the few cases can be found in Brian Krebs' book Spam Nation. Krebs recounts an episode of violent behaviour between cyber crime competitors. In it, a Belarusian cyber criminal called Alexander Rubatsky, formed an alliance with a group of heavies, associated with the "The Village" organised crime group in Minsk. In one instance, these men posed as local police and then kidnapped Rubatsky's main rival, holding him for ransom.

Yet such examples proved rare in my research. One of the surprising findings from the data was that it is not common for mafias and organised crime groups to provide protection for cyber criminals. Instead, it seems that law enforcement agents and political figures are more frequently providing this service. After all, bent politicians and police are in a much better position to shield cyber criminals from arrest.

The evidence suggests that in lieu of trying to control, or govern, the entire world of cyber crime – as they have done with various illicit industries in the past – organised crime groups are more likely to play a smaller role within it. The more common ways they choose to involve themselves is either as a service provider or guiding hand in various enterprises.

For example, the money side of cyber crime is a plausible point of entry for organised crime involvement. One interesting example I encountered was a Los Angeles street gang converting prostitution operations into cyber fraud schemes. "Fraud pimps" send women out to make purchases with counterfeit credit cards, rather than to turn tricks.

While such evidence shows involvement in cyber crime, we should seriously call into question the popular perception of cyber crime as predominately run by violent, organised criminals. And that is not the only problematic stereotype we need to contend with. At the other end of the spectrum, is the ingrained view that cyber crime is driven by nerdy and socially awkward hackers – the archetypal hooded teen in his parents' basement.

Returning to the example of CarderPlanet, these cyber criminals were clearly organised and sophisticated. While few of the leaders had past lives as mafia members or serious histories of violent crime, neither were they isolated geeks without social skills or any management ability.

They were the pioneers of the multi-million dollar "carding" industry and adopted commercial principles that we might expect to find in corporations across the world. They even organised a number of offline gatherings, including at least two business conventions held in Odessa, Ukraine, in 2001 and 2002. That was then. The cyber crime industry and its professionalisation have only grown since then. As US Law enforcement agent Terry summed up the threat: "They are businessmen."

Jonathan Lusthaus is author of Industry of Anonymity: Inside the Business of Cybercrime*, published next month by Harvard University Press*

A heritage approach to modern cyber threats

BlackBerry, famous for developing secure mobile devices and operating systems, is using its considerable expertise to help clients overcome cyber attacks and increase their cyber resilience. Global head of cyber security delivery **Campbell Murray** explains why the company's approach is unique

IN ASSOCIATION WITH

BlackBerry

SHUTTERSTOCK/MICHAEL TRAITOV

BlackBerry began developing a cyber-consulting stream in February 2016, when it purchased my company Encription Ltd. Encription had built up a well-established UK cyber consultancy business, winning key customers in the public and private sector. By late 2016, we had started making people aware that BlackBerry is now able to provide an expanded consultancy offering to a much wider audience. BlackBerry has always been known for being a pioneer in developing secure code, secure operating platforms and networks. Now we are leveraging our 30 years of exceptional experience to offer our unparalleled knowledge to clients as a software and services business with a specialist cyber security consultancy. As a global leader in cyber security, some of the world's largest organisations trust BlackBerry; customers include 100 per cent of the FTSE 100 commercial banks, all of the ten largest law firms, and 16 of the G20 governments.

As global head of cyber security delivery, I head up a team delivering "boots-on-the-ground" consultancy focused on cyber resilience from planning to recovery. We are a "360 degrees" operation, meaning that we go into organisations if they've had a breach, and we also conduct penetration testing and training, as well as offering general cyber security services and consultancy in risk and compliance, such as making sure companies are on top of GDPR.

Because BlackBerry is a developer of secure software and operating systems, the consultancy we offer is special in a number of ways, and one is our work with organisations that are looking to develop their own solutions. We work with them long term, to make sure they are following best practice, that their developers are trained to develop code securely, and we provide checks and balances at key milestones all along their cyber security journey to make sure they're regulatory compliant, and that their systems don't get a nasty surprise somewhere down the line.

In short, what we offer is more than consultancy; it's a holistic service based on our 30 years of knowledge that is not just there when things go wrong, but well before that point. Crucially, every service we provide is different and produced on an in-depth partnership

basis, without boxed solutions. For example, when a client unveils its app we've been involved in the development process from the start, right up until the product release, and as such we have a motto in the company: "We'll do it right, and we'll do it right the first time".

Central to our approach is the assumption that you have most likely already been hacked, and if you haven't then you almost certainly will be at some point in the future. Working with our clients, we lead them through five stages of defence: prepare, protect, detect, respond, and recover. As a company that has been building cyber products for decades, BlackBerry understands that it's not easy to get security right; we have the empathy and the understanding, but also the experience, to guide our clients in not making those mistakes. We equip companies with the know-how to react when things go wrong, but also to develop the underlying resilience that will prevent these issues from arising.

As a whole, the UK is making amazing things happen in the world of cyber security. I personally believe, having travelled around the world talking to different governments and organisations, that the UK is ten years ahead of every other country in its cyber security maturity. The government has form, after pioneering the UK Government Connect Secure Extranet (GCSx) almost ten years ago, which has since evolved into the Public Service Network. These developments have pushed government, state and local, as well as public bodies onto a safe platform. BlackBerry is proud to be working within, and supporting, the much broader effort to keep the UK safe, and the worldwide fight against cyber threats. We are developing our knowledge transfer capabilities, and continue to advise governments and organisations around the world.

BlackBerry is keenly aware of the growing threat posed by connected devices, and the internet of things (IoT). We refer to it as the "enterprise of things", and believe it signals the introduction of a fourth internet, in addition to the already established regular internet, corporate internet, and dark web. The enterprise of things represents a whole new category of risk, as it increases an organisation's threat surface exponentially. There are billions of hackable, connected products being added to the market every year, and our strategy and motives are to secure the enterprise of things going forward. We view this as an absolute priority, and this year at the BlackBerry London Security Summit the company launched a new platform called "Spark", which is aimed at securing communications across disparate networks. Spark is a management and security platform that allows you to take medical devices in a hospital, or other connected devices in a hotel, office and so on, and place them in a secure layer. It's an incredibly exciting development, and one we are proud of.

Although the underlying motivation of cyber attacks are the same as they always were – the theft of either data or funds from victims – the way an attack is mounted shifts over time. I believe we are currently in a phase where applications are increasingly hard to hack, because detection systems have greatly improved. However, this has led to attackers falling back to access via social routes, such as good old-fashioned phishing emails. And in turn, there will come a time when cyber professionals are so focused on preventing phishing that they've forgotten about intrusion detection. BlackBerry advises clients to maintain a good balance, and prepares them for an attack from all angles.

At this company, we are in the unique position of having "been there". The company has been building products over the last three decades that we had to keep safe, and we understand the huge challenge that poses. Using that considerable experience to make other organisations safer seems like a natural next step in the company's journey.

How can “smart cities” guard against cyber crime and protect people’s sensitive information? Rohan Banerjee investigates

Is a smart city really a smart idea?

According to a report by the United Nations, 55 per cent of the global population lives in urban areas. By 2050, this figure is expected to increase to 70 per cent. Within the context of the overall growth of the world’s population – which is also living longer than it used to – the UN expects a further 2.5bn people to be living in cities in the next 32 years. In order to cope with the pressures of urbanisation, cities need to do more than just build more houses.

“The underlying concept of a smart city,” explains Tom Symons, principal researcher in policy at Nesta, “is to align the advances of technologies with age-old urban problems, for instance the challenge of reducing traffic on roads. This is important from an environmental perspective, just as it is in terms of the logistics of space. These are not new questions, but new technologies are offering new answers, which are needed when you think about financial challenges and limited resources.”

The common vision for smart cities is to make use of the “internet of things”, which is the interconnection via the internet of computing devices in everyday objects that makes them able to send and receive information. Smart city initiatives can include self-assessing electricity grids that are used to address power outages. These grids provide the basis for other projects, such as smart traffic lights that prioritise cyclists and ambulances; more energy-efficient buildings that adjust power use according to information from sensors; and city-wide electronic vehicle charging points.

But new technologies bring new challenges. And the “interconnectivity between physical and digital infrastructure”, according to the associate director of cyber security consultancy firm Control Risks, Jayan Perera, gives rise to “a range of evolving security risks”. In addition to malware, data manipulation or ramsomware, smart cities can be susceptible to signal jamming, phishing and phony emails posing as local authorities, all the while placing a huge amount of faith in technological resistance to these threats. For Cesar Cerrudo, chief technology officer at IOActive and founder of the *Securing Smart Cities* blog, smart cities create “huge attack surfaces.... As geopolitical tensions escalate, nation states, terrorist groups and the like could start targeting cities with ransomware, for example, with the intention of disrupting services and having a big impact on populations.”

Cerrudo highlights one particularly

SHUTTERSTOCK / IR STONE

> “Government must consult with industry”

damaging instance of ramsomware that happened in Atlanta earlier this year. There, a hacker group known as “SamSam” encrypted the city’s municipal court’s files, locking access to online services and prevented it from processing legal cases and warrants. The office lost the use of almost all of its 77 computers, while the police force lost all of its dashcam footage. “SamSam” demanded $51,000 in Bitcoin to stop the attack. Whether Atlanta’s authorities paid the ransom is unknown. Services are now back online, but the estimated cost of the clean-up is, at the time of writing, in excess of $10m. “Cyber criminals are organised and their attack techniques continuously evolve,” says Cerrudo. “Smart city technology is vulnerable because almost everything in a city is or will soon be running software inside.”

While many cities are desperate to experience the benefits of digitalised services, Cerrudo warns that too often authorities will “not do the proper testing” on the technologies they install. “Sadly, cities are implementing new technologies without first testing cyber security. Although cities usually rigorously test devices and systems for functionality, resistance to weather conditions and so on, there is often little or no cyber security testing at all, which is concerning.”

To ensure effective cyber security in Smart cities, London’s chief digital officer Theo Blackwell argues, “a clear set of standards must be pre-agreed” between different parties. “Government, the public sector and the private sector should consult with one another,” he says, “before any technologies make their way into the city.” Blackwell, appointed by Sadiq Khan to oversee the UK capital’s Smart city ambitions last year, says that the government-funded London Office for Rapid Cyber Security Advancement (LORCA), is “working closely with the Mayor of London’s team to guide companies on the best digital practices.”

Machine to machine (M2M) communication, which forms the bedrock of a smart city, is a double-edged sword. M2M systems can automate processes and services, but with the absence of human operators, the risk of a “cascading error”, as Control Risks’ Jayan Perera calls it, is increased. “What this means,” he explains, “is that an unchecked mistake has the potential to spread through a system. A minor computer error that’s caused a smart [electricity] meter to give an inaccurate reading to its control centre, could lead to an automated, and incorrect, reading that a particular location require an increased amount of electricity. This would require routing some of the existing energy supply to this location which, in turn, could result in increased costs and a reduced energy supply for others.”

There is a temptation, Perera says, “to assume that because digital services are usually an improvement on what they replace, they aren’t going to fail, but of course they have the potential to.” To mitigate for a “component failure” –

Smart cities can use data for "civic benefit"

when one aspect of a digital system stops working – Perera recommends that smart cities should prioritise installing "rapid component replacement" options. "It makes sense to have back-ups in place. Essentially, if you've got a system and you have a baseline level of performance, which constitutes normality, then you know whether something has gone wrong. So if you can automate a system to check itself for things that get away from that baseline, then it can replace those components as needed, without it spreading. Obviously for more critical components, which would cause a system failure, you'd need to prepare something different, but on a smaller scale, this could work. Smart cities can benefit from installing behaviour-based cyber security measures."

Alongside any technical concerns attached to smart cities, of course, is the contentious issue of privacy. Smart cities need data to thrive, but there is a difference between data collected from monitoring technologies, such as air quality or temperature, and data that is more personalised, such as shopping habits, dates of birth or marital status. Who decides what data is relevant and to whom? How can smart cities garner the trust of their citizens? Nesta's Tom Symons says that the success of any smart city hinges on its "ability to demonstrate why and how data is being collected" in a way "so that citizens can understand the point of it. Smart cities, collectively, need a consensus on clear ethical principles relating to citizen data. The bottom line is that citizens need to be in control of what is going on with that data, and that probably means some sort of opt-in or opt-out mechanism. A 'data wallet', in the form of an app on their smartphone, could help citizens to manage what parts of the smart city they choose to engage with. Maybe they'll be OK with sharing how often they use their bike, maybe they won't. The smart city has to let citizens have some binary control over whether they share, and the conditions attached to that. Maybe they only want to share that data if it isn't used for commercial purposes."

While "privacy is obviously hugely important", Theo Blackwell says that in an ambitious smart city such as London, "we could argue that some data is being under-exploited". He is keen to stress the potential of data to be used "for civic benefit", and to encourage "a culture of data exchange" in London. "The key point is thinking about collaboration, data, and the needs of citizens. If companies were convinced to share their data, of course with some caveats about privacy, then London could benefit from the more informed decisions that were made. If Transport for London gave insight into passenger journeys – how long, how often and so on – then that could help local businesses." Of citizens' willingness to share their data, Blackwell says: "I think if data collection comes with an explicit description of what it's being used for, how long it's being held, then people will usually recognise that it's a worthy trade-off to receive better services."

Technology can cut operational costs and enhance services. Against the backdrop of rapid global urbanisation, both will be necessary. Smart cities, however, are far from the finished article, and challenges in establishing a set of technical standards along with an ethical guideline for data collection are ongoing. Risk management is not an admission of defeat, insists Perera, who views the need to "prioritise some smart city assets over others" as a natural consideration for "any cyber security budget". But, as Cerrudo argues, the long-term aim for any smart city would be to eliminate these risks entirely by ensuring that the technology is fit for purpose in the first place. "Technologies used by cities must be properly security audited to make certain that they are secure before they are implemented. To fail to do so is reckless. When we see that the data that feeds smart city systems is blindly trusted and can be easily manipulated, that the systems can be easily hacked, and there are security problems everywhere – that is when smart cities become dumb cities."

Creating security as mobile as modern threats

With more access for threats than ever before, is perimeter-based security suitable for today's work patterns and the IoT age, asks David Matthews, global director of sales, security solutions at Unisys

IN ASSOCIATION WITH

UNISYS | Securing Your Tomorrow™

Many organisations still see IT-focused security as a barrier to the flexible, mobile ways of working they are embarking on. Traditional security approaches could fail because of the shift to cloud/mobile-enabled working and the proliferation of internet-of-things (IoT) devices. These changes are becoming incompatible with the traditional network perimeter approach to security, "bolted on" to existing IT infrastructures, assuming access should be infrastructure based, not user- or device-driven. This new cloud/mobile model of working, and the increase in internet-enabled devices, are creating a world of "device sprawl" that means the surface available for attack is larger, and the network management costs to manage it are higher. There are also increasingly critical regulatory and reputational issues, such as the impact of GDPR and high-profile data breaches that can shake a citizen's faith in an organisation.

Today's security solutions need to enable, not prevent, more efficient ways of working and information sharing, as well as protecting IoT devices. In the health sector this "device sprawl" includes devices such as health monitors, control systems, surveillance cameras and IV pumps. According to Gartner, "legacy medical devices that were not designed to be internet-accessible are now being connected to the internet as part of healthcare initiatives, increasing risks and the attack surface." Gartner recommends organisations "create zones to proactively house connected medical devices and identified micro-segmentation as one of its "top technologies" for information security in 2017.

By joining a defined, secure community of interest, devices are shielded from unauthorised access, reducing the attack surface. Jeff R Livingstone, vice-president and global head of life sciences and healthcare at Unisys, explains: "In the USA, zero-trust security for medical devices has become a mandate for healthcare organisations, since would-be attackers began using ransomware to target vulnerable medical devices, with IoT devices such as health monitors and IV pumps… it is more important than ever for organisations to reduce their attack surface and increase data protection, to better safeguard data and ultimately the livelihood of the patients." Unisys has developed its innovative Stealth security solution further to meet these needs. As well as addressing the demands of securely accessing and inputting information, regardless of device or location, as a network overlay it requires no changes to existing networks and applications. Being scalable and software-based, it offers cost efficiencies and easily accommodates organisational changes.

The latest version of Stealth has given the medical profession an innovative device security solution that brings together identity -based microsegmentation, encryption and cloaking that can move from the cloud to the hospital floor and the operating room seamlessly, regardless of location or type of device. This innovative solution led to Unisys being awarded *Philadelphia Business Journal*'s "2018 Healthcare Innovator of the Year".

For more information, please contact adam.britz@unisys.com

CYBER SECURITY

The latest contracts, jobs and training

THESE CONTRACTS ARE NOW OPEN FOR TENDERS

1. The Guinness Partnership Limited
Data centre services
Bid deadline: 5th November
Tender value: £500,000
Guinness is inviting bids for a cyber security partner to manage and protect its client and asset information at its data centre in Salford Quays. The proposed contract is over five years.
Contact: procurement@guinness.org.uk

2. Dorset Fire & Rescue Authority
Internal audit services
Bid deadline: 7th November
Tender value: £125,000
Dorset Fire & Rescue Authority is looking to undertake a review of its computer network, covering its payroll system, treasury management and communications security.
Contact: clare.mccallum@dwfire.org.uk

3. Future Cities Catapult
Knowledge management platform – processing and data repository
Bid deadline: 12th November
Tender value: £100,000
Future Cities Catapult, a consultant on smart city initiatives, is looking to award a contract for the design, provision and maintenance of its data storage systems.
Contact: nwhittaker@futurecities.catapult.org.uk

Tender and framework data supplied by

tussell

4. Golding Homes Limited
GB Maidstone: Provision of Board Portal Solution
Bid deadline: 16th November
Tender value: £25,000
Golding Homes Limited, a Kent-based housing association, seeks a cyber security partner to help protect its new mobile app service.
Contact: procurement@goldinghomes.org.uk

THE LARGEST PUBLIC SECTOR CONTRACTS OPEN FOR BIDS SOON

"Pre-Information Notices" give advance warning of contracts that will soon be open for tenders.

1. NHS Calderdale CCG
Information technology and networking services
NHS Calderdale's Clinical Commissioning Group will seek cyber security on a seven-year contract to deliver new IT systems to serve several West Yorkshire trusts. Services will include data storage and management, and email protection.
PIN Value: £25.3m

2. Ministry of Defence
Serapis Framework
The MoD will seek a partner to design and maintain a new network platform for secure data exchange between its different research arms, including the Defence Science and Technology Laboratory.
PIN Value: TBC

3. NHS Shared Business Services
Link: Cloud and Cyber Security
NHS SBS is consulting on a proposal to tender the provision of cloud software used to support NHS organisations across the country.
PIN Value: TBC

4. Local Government Association
Web-based tool for recording data processing activities
The LGA is looking for a web-based data processing tool to use while conducting market research.
PIN Value: TBC

CYBER SECURITY JOBS NOW OPEN FOR APPLICATIONS

Cyber Security Policy and Standards Lead, Home Office
Salary: £39,333-£40,380 p.a.
Location: Croydon, Sheffield or Manchester
Closing date: 21st October
The Home Office seeks an experienced cyber security consultant to assess and develop the critical IT systems used to support policing and counter-terrorism.

Security Architect, Home Office
Salary: £48,836-£56,405 p.a.
Location: Croydon, Sheffield or Manchester
Closing date: 22nd October
The Home Office is looking for experienced cyber security technicians to design and maintain software and hardware for the government's homeland security, public safety, border control and citizenship databases.

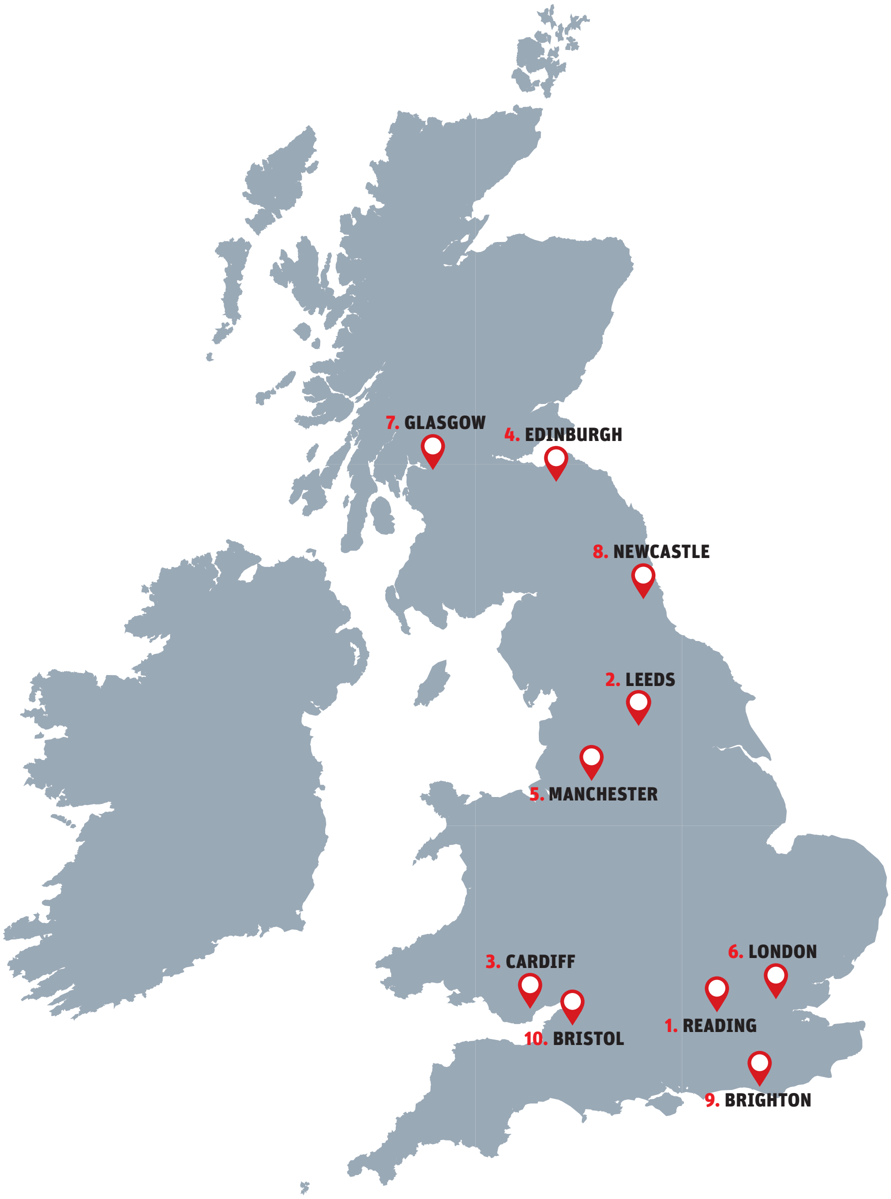
Information Assurance Manager, National Crime Agency
Salary: £43,439-£54,727 p.a.
Location: London
Closing date: 22nd October
Working within the NCA's Chief Data Office, the successful candidate will oversee strategies in acquiring, managing and protecting sensitive data, used to

inform law enforcement.

Cyber, sensor and information warfare scientists, Defence Science and Technology Laboratory
Salary: £31,000-£52,000 p.a.
Location: Porton Down, Salisbury, Fareham
Closing date: 11th November
Dstl, the technology arm of the Ministry of Defence, is recruiting for multiple roles to carry out specialist work on developing and securing new military technologies from compromise.

THE UK'S TOP TEN CITIES FOR ATTRACTING CYBER SECURITY TALENT

Crucial Academy's Cyber Security City Ranking for 2018 considers the best places in the country to set up cyber security companies. The study analysed several factors including salary, affordability, job availability and tech sector potential growth.



TRAINING OPPORTUNITIES

Short course in Introduction to Cyber Security, City, University of London
This ten-week course, comprising ten two-hour evening classes, aims to give business managers an overview of the cyber security risks most likely to affect them. It covers staff training, risk management and communication security.

MSc Cyber Security, University of Southampton
This one-year full-time postgraduate degree, accredited by the NCSC, teaches on risk management for public and private institutions, the sociology of the internet and the evolving regulatory landscape relating to data protection.

MSc Information Security, Royal Holloway, University of London
Delivered through the University of London's International Programmes as a distance learning course, this part-time MSc course is aimed at mid-career IT professionals. It covers cryptography, programming network security, ethical data acquisition and digital forensics.

PhD studentship in assessing behaviour change strategies in Cyber Security, Bournemouth University
Bournemouth University is offering a PhD studentship to carry out research into the role of human psychology and staff training in implementing business-based cyber security.

SHUTTERSTOCK/ MERTSALOFF

ADVERTORIAL

How will AI change the rules of cyber security?

Pete Burnap, professor of data science and cyber security at Cardiff University, answers four key questions on the opportunities presented by machine learning

IN ASSOCIATION WITH

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

How does AI differ from a traditional antivirus programme when it's looking for malware?

Traditional antivirus uses signatures to match potentially malicious software samples onto a database of previously seen malware profiles. The problem with this is that cyber criminals are creating malware variants that can change their features to avoid detection. Each new variant can be produced very quickly, and will look different, as far as the antivirus is concerned, to the previous version. Artificial intelligence differs in that it can be used to represent the malware in different ways and to make approximate matches more effectively. For instance, we have shown it is possible to produce representations of malware behaviour while it is running on a computer system that effectively mirrors those of human DNA. Then we use AI to produce a matching score. We don't need an exact match, we can say a sample is behaving in a slightly different, but very familiar, way to malware that has previously been seen.

What else can AI detect?

AI can also be used to detect malicious activity in a range of settings, such as network traffic running over Internet of Things (IoT) devices and on critical control systems. We've shown that it is possible to use AI to detect malicious web links on Twitter, within seconds of clicking the link, which could help to reduce users' exposure to malicious web servers.

Could AI predict threats before they occur? How?

It is difficult to use AI to detect all threats before they occur, because the threat landscape is very wide and dynamic. However, AI is very useful for monitoring and modelling the evolving cyber threats landscape. We can detect emerging threats rapidly and then use this information to improve cyber situational awareness using AI. For instance, we've linked emerging cyber threats to dynamic risk models that can tell you, in real time, what the impact of this emerging threat would be on an organisation's goals and processes if it were to materialise. This could help businesses plan how they allocate resources for cyber security.

Where do you see this technology being most useful?

As in many other areas, AI is most likely to be useful where it supports human decision-making, and in cyber security that's likely to be in front-line defences. People always need to be in the loop as the context changes so much, and we're quite a way off fully automating cyber defences using AI. However, the threats to cyber systems are ever-changing, and increasing at such a rate that AI technology can offer a lot in support of scaling the analysis of network traffic and software for new and unseen threats – informing analysts that action needs to be taken. Our mission is to continue innovating with AI and to integrate our research into systems that are subject to a wide range of cyber attacks, improving cyber-situational awareness and preparedness.

Does China need spy chips, when it builds so much of our infrastructure?

China's tech manufacturing dominance gives it an edge in the trade war, writes Oscar Williams

Earlier this month, *Bloomberg Businessweek* published an explosive report which alleged that tiny microchips, designed to allow undetected access, had been installed in Chinese factories on equipment sold to almost 30 US companies, including Apple and Amazon. The report sent shockwaves through the technology industry, and prompted sharp rebuttals.

Apple said there was "no truth" to the allegations, while Amazon claimed the article contained "so many inaccuracies... they're hard to count". Unusually, GCHQ and the US Department for Homeland Security also commented on Bloomberg's assertion that the FBI was investigating the alleged attack; both organisations issued statements saying they had "no reason to doubt" Apple and Amazon.

Security researchers, meanwhile, pondered how such a hack might have worked. Bloomberg suggested Chinese spies had planted microchips the size of pencil tips in servers assembled in China and sold to US firms and government organisations. But its technical explanation was short on detail, and some researchers questioned whether a chip so small was really capable of carrying out the hack. One expert quoted in Bloomberg's story later said he was "uncomfortable" with the article's conclusions.

Most people in the tech industry have taken one of three positions. Some believe the hack was real, and that the units investigating it within Apple, Amazon and the FBI were acting independently, which would explain why the security services were not aware of the findings. Others believe that in the race to deliver a market-moving scoop, Bloomberg's journalists drew hasty conclusions. A third contingent believes that Bloomberg accurately reported what it had been told – but that their sources had fallen for a misinformation campaign.

Whatever the truth, espionage is a key issue in China's trade war with America. Earlier this year, a US government commission found that "Chinese theft of American IP" cost the US up to $600bn a year. The findings are said to have been instrumental in Donald Trump's decision, in March, to impose tariffs on $50bn's worth of Chinese goods.

On 9 October, tensions between the two countries escalated further when a Chinese intelligence official was extradited from Belgium with the intention that he will face espionage charges in an open court.

Whatever you make of Bloomberg's story, it demonstrates an inescapable truth: supply chain insecurity is the price Western governments and businesses pay for global trade and digital economies. Trump can carry on increasing tariffs on Chinese goods, but that alone won't change the West's addiction to technology built (and increasingly, developed) in China.

In a number of key sectors, it is already difficult to keep up. Chinese companies already supply critical components to the UK's telecoms infrastructure, and China's share of the international market is likely to grow with the advent of 5G. This presents a still more unsettling possibility: when China stops hacking Western tech companies, it'll be because, having replaced them, it no longer needs to.