NewStatesman

Spotlight

CYBER SECURITY: DANGEROUS GAMES

Robert Hannigan / Liam Fox / Julian King

NOMINET
CYBER
SECURITY

A SAFER, SMARTER NETWORK **FREE FROM THREAT.**

USE YOUR DNS to detect, block and mitigate cyber attacks:

- Malware
- Phishing
- Data Exfiltration
- Spoofing and cache poisoning
- DDoS
- Spam

Find out more about Nominet Cyber Security
www.nominet.uk/cyber

Outlawing security

Last week, Google and Microsoft wrote to the US senator Nathan Deal urging him to veto Senate Bill 315, which would create a new crime of "unauthorised computer access" in the state of Georgia. In a separate letter, 55 cyber security professionals from organisations including Harvard and Georgia Tech universities, Verizon and Dell, wrote to Senator Deal also asking him to oppose the law. Why would the academics and businesses most deeply invested in cyber security oppose a law that made it a crime to access someone else's computer?

The answer is that accessing someone else's computer is not a straightforwardly moral or immoral act. Last year, the 15-year-old Georgia voting system was found to have been left effectively unsecured for months, but the people who uncovered these flaws needed to compromise the system in some way to prove it. The new law, then, is widely believed to be a measure not against official incompetence but against the discovery of official incompetence.

But a change in the law is not necessary for irresponsible people to cover their tracks. In the US, multiple journalists and security researchers currently face defamation lawsuits by companies that disagree with the ways in which their security failings were discovered and reported. Nor is this a new phenomenon; five years ago, academics in the UK were prevented from publishing their research on how luxury cars could be hacked by a lawsuit from the car manufacturer.

No organisation, device or account is unhackable. For governments and industries to pretend otherwise, and to try to silence those who expose their faults, will only aid those who would rather keep those faults secret and use them for their own, less altruistic, ends. Most penetration testers are happy with the bounties they get for responsibly reporting a flaw, but companies must encourage these researchers and act quickly on their expertise. As one white-hat hacker told *Spotlight* in 2016: "If I know about [your security flaw], chances are a lot of other people do, too."

NewStatesman
71-73 Carter Lane
London EC4V 5EQ
Subscription inquiries:
sbrasher@
newstatesman.co.uk

Account Director
Justin Payne

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 4 May 2018.

This supplement can be downloaded from: newstatesman.com/page/supplements

"The data economy is jeopardised by tech firms acting stupidly"

Robert Hannigan created the first UK Cyber Security Strategy and, as director of GCHQ, established the National Cyber Security Centre. He told Oscar Williams why cyber security could be a tool for diplomacy

Just over a year ago, Robert Hannigan stepped down as director of the intelligence agency GCHQ. In the time since, cyber security has dominated the British news agenda in a way it never has before. The WannaCry computer virus paralysed dozens of NHS trusts within weeks of Hannigan's departure. Two months later, NotPetya – an even more virulent strain of malware – forced manufacturers across Europe to shut down their factories for weeks on end.

While the two viruses have since been linked to North Korea and Russia respectively, they shared a common set of code: EternalBlue, a Windows exploit that had been developed and stockpiled by the US National Security Agency. The NSA reportedly only told Microsoft about the vulnerability after it was stolen by hackers. When WannaCry started spreading, Brad Smith, the software giant's president, compared the theft to the US military losing "some of its Tomahawk missiles".

So does the NSA bear responsibility for the attacks? "Not really, given that the vulnerability had been patched," says Hannigan, who now advises the private sector. Microsoft had issued security updates, but thousands of customers, including NHS hospitals, hadn't updated their systems in time. He adds: "There is a bigger policy question around vulnerabilities; about the default position being that anything that compromises public safety should be reported."

Given how many critical infrastructure providers rely on Windows software, doesn't EternalBlue fall into that category? "The problem was organisations not being able to patch XP, as I understand it anyway." Microsoft had stopped supporting the operating system, meaning some organisations were unable to protect their networks. "It's a genuinely difficult ethical question," he adds. "If you want agencies

IP EXPO MANCHESTER

to do difficult things you have to have some tools to do it. But I agree that in most cases they should be reported because certainly for GCHQ, the first responsibility is the safety of the public."

In recent weeks, the Cambridge Analytica scandal has prompted regulatory investigations, wiped billions of pounds off Facebook's share price, and attracted the attention of policymakers on both sides of the Atlantic. But despite the elevated status of cyber security in Whitehall and Westminster, Hannigan, says he doesn't miss working in government: "I miss GCHQ itself; I miss the people and the technology. There's a great buzz about the place. But I did 20 years in government and that's probably enough and I'm very happy there are other competent people doing it – people more competent than me."

"I don't blame politicians – knowledge is generational"

Politicians have recently faced a barrage of criticism for failing to understand the systems they are trying to regulate. During Mark Zuckerberg's first congressional hearing last month, the Facebook CEO was quizzed about the privacy of messages "emailed" over WhatsApp, and how the social network makes money if it doesn't run adverts. "This is a generational issue," says Hannigan. "It's hard to be a politician trying to regulate something that wasn't really around when you were young. It's moving so fast – so I have sympathy with them. Their job is to reflect voters' feelings, not to say there's an easy technical solution or what it is."

One of the most pressing security issues facing the UK government today is how to protect the country's critical systems. While the US has hardened its stance against foreign tech companies over the last few months, Theresa May has signed new deals with companies such as the Chinese telecoms giant Huawei. The firm operates a cell in Oxfordshire to combat Chinese hacking on behalf of the government. Hannigan says it's generally regarded as having been successful in giving "a reasonable level of assurance": "The issue is how do you scale it up for all companies and all national security issues? That's quite a challenge."

Hannigan led GCHQ for just two years before standing down last spring for family reasons, but he is credited with bringing the agency out of the shadows following the Snowden revelations. Having served in No 10, the Cabinet and Foreign Offices and Northern Ireland, he was unusually visible for a spy chief. He gave prominent speeches, launched the public-facing National Cyber Security Centre and attempted to forge closer working relationships with the tech giants, even if it sometimes meant singling them out for criticism.

Hannigan is still on Silicon Valley's case. "There are so many good things that will come out of better use of data, particularly in healthcare. We don't want a data-enabled economy to be jeopardised by tech companies doing stupid things. That's the worrying thing for me about Facebook and Cambridge Analytica." But Hannigan's frustration is not reserved just for industry. "The potential of human progress through the internet is massive," he adds. "It could be jeopardised by a failure of governments to prioritise good security and resilience."

When it comes to cyber security, the UK and US governments have grown more vocal over the last year. Given the difficulties in attributing cyber attacks, officials tend to shy away from naming nation states. But in recent months, both governments have blamed North Korea for WannaCry and Russia for NotPetya.

"Russia may want to do reckless things in cyberspace"

In April, GCHQ and the NSA also joined forces to release a joint technical alert for the first time, detailing Russia's alleged attempts to hijack internet infrastructure. This was, Hannigan suggests, a veiled warning for Moscow: interfere with these systems and we'll know it was you.

Deterring governments from using cyber weapons, Hannigan says, requires a different approach to conventional weaponry: "In a world where everyone denies everything, how do you have an enforceable arms control model in cyberspace?" Cyber weapons are different to conventional weapons in another important respect too: the complexities of predicting collateral damage. This makes it harder for states such as the UK to retaliate. "When you drop a bomb on something, you know what it's going to do," says Hannigan. The same cannot be said of cyber attacks. Once a virus has been released on to the web, it's impossible to know where it will end up. "I can't believe, for example, that the Russians intended to take down half the manufacturing companies in Europe," he adds. "The important point is that they didn't care."

After the former British spy Sergei Skripal and his daughter Yulia were poisoned in Salisbury in March, commentators speculated that the UK government might respond by launching a cyber attack on Russia. Hannigan dismisses the idea: "Trying to find cyber responses that target those individuals who are responsible for bad things is quite difficult. Economic sanctions frankly make more sense to me very often. The impact of what the US has done around economic sanctions on those around Putin is far greater than anything else that has happened, even than the expulsion of diplomats, which was in its own way impressive."

During a keynote speech at IP Expo Manchester last month, Hannigan warned that the Skripal poisoning indicated Russia's intentions have dramatically evolved. "It's not surprising that over the years, we and other countries have found Russian intelligence services on our networks," he said. "What is worrying is the intent has clearly changed. A country that is prepared to use chemical weapons on the streets of a UK town may want to do reckless things in cyberspace."

There is growing support for an international treaty defining and governing cyber warfare. Microsoft's Brad Smith called for the creation of a Digital Geneva Convention last year. At the RSA security conference in San Francisco last month, Microsoft took this idea a step further, bringing together 34 tech companies to sign an accord promising to protect users and customers from cyber attacks regardless of their origin. The UN's general secretary Antonio Guterres has also called for new rules for cyberspace.

Hannigan supports the principle of a treaty, but fears that as a starting point it may be too ambitious. He warns: "If you go immediately for the treaty, you'll end up just endlessly talking." Instead, he suggests the process should be divided into sectors where a consensus is likely to be reached: "Start with health, for example, and say 'we're going to come up with these ways of behaving with technical infrastructure for health'."

The initiative could be industry-led, but would need the support of government: "I think it would be good for governments to engage with the tech accord, to engage with Brad Smith's Geneva Convention idea and to say: 'well, why don't we sit down – government and industry – and see what might this look like?' Make it West and East, make it non-threatening. […] It doesn't need to be legally binding if there's no way of enforcing it."

It's expected that hostilities in cyberspace will intensify in the coming years. But Hannigan is hopeful that cyber security could, ultimately, serve as a way to bring political leaders together: "That might be massively optimistic, but the internet is so obviously a shared resource and so obviously not owned by any particular government. This could be a place where there is common agreement in a geopolitical context that is otherwise pretty stormy."

Secretary of State for International Trade Liam Fox outlines the Cyber Security Export Strategy, designed to complement the government's safeguarding efforts

There is no room for complacency in cyber security

As International Trade Secretary, I meet regularly with business and political leaders across the world. One topic that is regularly raised is the way that technology has changed the way we have traditionally thought about our borders. This technology revolution, however, has been something of a Pandora's Box. While it has allowed information to thrive, it has also been an opportunity for exploitation – changing the nature of crime before our eyes. Threats to cyber security are increasingly organised and transnational with no respect for geographical borders.

That's why it's the responsibility of government, to lead the field in our global cyber security standards and to promote the UK's world-leading expertise and strengthen capabilities in the UK and allied countries.

Over the last year, we have seen a significant increase in the scale and severity of malicious cyber activity globally. In the UK, we have seen the impact of major cyber security incidents, such as the WannaCry attack that affected 48 NHS Trusts.

This was not targeted at the health service or the UK, but does demonstrate the borderless and often indiscriminate nature of the threat. We saw that too in the destructive NotPetya cyber attack in June last year. That was targeted at Ukraine – showing a disregard for their sovereignty – but its reckless release also disrupted organisations across Europe. This cost hundreds of millions of pounds, including here in the UK. The threat is only going to increase, so our resolve to stay ahead must be unrelenting.

The UK has been clear that it will not tolerate such malicious cyber activity and will seek to impose consequences on those who wish to undermine the rules-based international order in this way. Alongside our allies we attributed NotPetya to the Russian military and WannaCry to North Korean actors.

These attacks have real-world impacts – from a patient missing a cancelled hospital appointment to the small business owner losing daily takings. A cyber attack on one of our most well-known Internet Service Providers cost £60m and the loss of 95,000 customers. It is therefore no surprise that CEOs and other leaders are taking

SHUTTERSTOCK/WILLY BARTON

this increasingly seriously.

It is absolutely crucial that the UK is protected against this threat and it is the something the government is determined to get right.

To meet this challenge, the government has put in place our National Cyber Security Strategy 2016-2021, supported by £1.9bn of transformational investment.

Our vision for 2021 is that the UK is secure and resilient to cyber threats, while prosperous and confident in the digital world.

At the heart of the strategy are three core pillars. Defending our people, businesses and assets across the public and private sectors, be they states, criminals or hacktivists – and developing critical capabilities to build skills, support growth and stimulate science and technology. This includes support for UK firms to export to existing and new markets.

Cyber threats do not respect geographical borders

Alongside this we are committed to working with our EU and international allies to tackle these unpredictable global threats effectively and partners to build cybersecurity capabilities; as demonstrated by the recent Commonwealth Cyber Declaration and the Prime Minister's commitment to invest £15m to help Commonwealth countries strengthen their cyber security capabilities.

We have also created the National Cyber Security Centre, the world-class cyber arm of GCHQ – a leading technical authority on cyber security. The NCSC offers unrivalled real-time threat analysis, defence against national cyber-attacks and tailored advice to victims when incidents do happen.

Since its work began in October of 2016, the NCSC has responded to more than 800 incidents and its Active Cyber Defence has prevented more than 54 million malicious emails spoofing government being sent.

Just recently, the Department for International Trade launched a new Cyber Security Export Strategy setting out how the government will support the UK's world-leading cyber security firms to take advantage of opportunities not just in protecting the UK's infrastructure and businesses, but those around the world.

The UK has an established, expert and innovative cyber security sector made up of around 800 companies across a full range of capabilities, with exports of £1.5bn in 2016. As an international economic department we are working to support firms to export their capability to new and existing markets across the globe.

Working with others, the government will do this through a range of activity, including acting as a trusted advisor to support UK companies bidding for major opportunities and having dedicated cyber security representatives at our embassies overseas in priority markets.

We will also promote the financial support for cyber security exports that may be available through UK Export Finance, which works to ensure that no viable UK export fails for lack of finance or insurance.

This is good for our national prosperity through increased exports, but also improves our own national security by ensuring that we have a viable and resilient domestic cyber security industry that is able to help defend the UK from those who would do us harm.

Having good cyber security is a challenge that governments and businesses around the world are becoming increasingly alive to. The pressing need to invest in having the right people, processes and technology with dedicated attention from company boards is crucial for national security and prosperity. My department is at the forefront of showcasing the UK's world-leading expertise in meeting this vital challenge.

Fortifying the castle walls

Simon Edwards, cyber security architect at Trend Micro, explains why a multi-layered approach is crucial if attacks like WannaCry are to be avoided

IN ASSOCIATION WITH

TREND MICRO™

Cyber attacks are happening all over the world all the time, but unless it is your email account receiving strange messages, or your shares that are suddenly plummeting, or indeed if you happen to be a cyber security professional and enthusiast like myself, it's quite easy to switch off from the noise.

This wasn't the case for the WannaCry attack on the NHS. The ransomware attack spread to over 150 countries in May 2017, and infected more than a third of health trusts in England, leading to the cancelling of at least 6,900 NHS appointments as a result.

The scale of this incident, and the real effect it had on people's day-to-day lives and the ability of NHS staff to carry out their crucial work struck at the very heart of British society. Trend Micro staff like me looked on with horror, only too aware of the software failures that had allowed the NHS to become so vulnerable.

Simply put: 80 – 90 per cent of ransomware attacks enter via email. If an organisation has a standard email monitoring system which is using sandboxing technology – opening the email and following the links included or looking at the document attached to make sure it's not malicious – this will stop a lot of attacks, but not all. The WannaCry attack didn't use email – it had a worm component. These types of worms self-replicate and attack across the network through a number of routes. Unfortunately, the breached health trusts were relying on a single protection technology, but that one technology failed.

At school students are taught that castles rely on multiple layers of protection – an outer wall, an inner wall, and a keep. The same principle applies to cyber security, and Trend Micro is committed to following that principle. As such, we have been developing XGen, a new approach to endpoint security by blending multiple layers of threat protection, to provide

SHUTTERSTOCK/VS148

the kind of layered protection that is crucial in today's climate of advanced and unpredictable threats. The layers include signature-based detection to stop breaches via email, as well as behavioural analysis, application control and if these layers don't stop the threat, then it will be stopped by advanced machine learning.

Having been in the cyber security industry for 20 years, I've watched numerous threats and seen attacks like WannaCry evolve and become more sophisticated. At Trend Micro we are continuously keeping an eye on emerging trends. Our threat defence experts and vast global network are constantly collecting data and identifying threats. A growing and complex threat landscape combined with changing compliance regulations are presenting in-house security teams with significant challenges. The introduction of GDPR, for example, – General Data Protection Regulation – is intended to protect people's private data, but I am concerned that it has created an unlikely opportunity for criminals. Under the new rules, if a company is compromised, leading to the loss of personal data, it has just 72 hours to report this or be fined four per cent of turnover. We predict that this may lead to the emergence of attacks that target GDPR-specific data. It raises the question of whether a company would rather pay a million dollar ransom to retrieve its stolen data from the criminals and not report it, or a multi-million fine for losing said data. This may sound like a strange prospect, but nine months ago the taxi giant Uber attempted to cover up a huge data exploit by paying off the hackers in the hope that the problem would disappear. Safe to say, it didn't.

Cyber security requires a human touch

Other developments in the technology landscape have opened up new opportunities for cyber criminals. For example, the exciting emergence of IOT – the Internet of Things – has not only created innovative applications for business and consumers alike, but has created endless routes for infiltration. The National Cyber Security Centre and the FBI recently launched new guidelines, which warned of the possibility of foreign actors gaining access via wireless routers. Similarly, the targeting by foreign and domestic agents of elections and civic bodies is something we are watching closely. We believe these attacks will become more specific, mutating over the years.

I also predict that in the next 12 months, one buzzword will be heard more and more at cyber conferences: MDR – Malware Detection and Response. Security companies are going to start providing services that are more human-based to help with analysis of breaches and potential threats.

Cyber security actors are beginning to realise that, ironically, sometimes what is missing from the technology and cyber systems business is the human touch. The use of big data analytics allows us to see more than ever before, but it still requires human beings to get out of it in-depth analysis, and lessons learnt. However, the massive skills shortage afflicting the wider tech sector is a major barrier to this development.

At Trend Micro we have over 2000 researchers across both threat research and R&D and we pride ourselves on championing the human aspect of cyber security support. We are a family-owned business that is one of the largest independent security companies in the world. This year we will turn 30; looking to the next 30 years, we plan to keep protecting castles big and small, making sure that cyber criminals are challenged at every turn.

Julian King, European commissioner for the Security Union, explains the need to coordinate the continent's cyber defences

How Europe can unite against its common enemy

We are justly proud of the new opportunities of online services and networks – but there's an iceberg that risks holing the digital flagship beneath the waterline, and we're just beginning to see its tip. Last year, the WannaCry malware attack did not just cause computers to freeze, but entire hospitals to close.

It has brought the issue of cyber resilience into the mainstream of public consciousness and political discourse; though in fact, Europe faces an average of 4,000 ransomware attacks per day. Elsewhere, we've seen attacks and other cyber-enabled threats take place for political reasons: hacks targeted at political parties, purposefully orchestrated fake news, and state actors destabilising neighbours with cyber tools and technologies.

The sad truth is that criminals and other malicious actors have never had it so good. Robbing a bank has never been such an un-kinetic activity – what once involved sawn-off shotguns and stocking masks can now be done from the comfort of home; a major attack can cost as little as $5. We now need to show the party is over: making these attacks harder to commit, and easier to trace and punish.

Public policy measures like improving judicial authorities' access to digital evidence would raise the stakes of cybercrime. But much of the answer lies with the private sector, which ultimately owns most of the internet, hence much of the threat surface. To assure our cyber security, the industry needs to make a switch: from being security consumer to security provider, and from seeing security not as a cost, but as a competitive advantage.

In the "gold rush" to be the first to get products to market, security is – unfortunately – not always first on manufacturers' minds. Relatively simple measures – encryption; eliminating redundant code; unique passwords – get forgotten about, even if they are actually vital to our collective security.

The consequences are already apparent: the Mirai botnet, the first significant attack originating from the Internet of Things, recently took control of around 150,000 routers and CCTV cameras; a few years ago, 600,000 homes in Ukraine lost their electricity, after a deliberate cyber attack was used in a Death Star-like demonstration of power. These vulnerabilities need to go. The tech industry has a duty of care to its customers to ensure products are not just secure by design, but kept up to date as new threats or weaknesses emerge.

The private sector has plenty of reasons to start taking this seriously. As people become more aware of the

SHUTTERSTOCK/ALEXANDROS MICHAILIDIS

grave consequences, there will be a growing clamour for secure products. Cyber resilience will become part of what customers value in a brand; companies with lax standards will see reputational damage. Corporate governance will soon start providing a push, too: recent incidents at Equifax and Uber caused public and political outcries aimed at board level.

According to a recent PWC survey, the proportion of CEOs worried about cyber threats as a major concern for growth prospects leapt from 24 per cent to 40 per cent in just one year. Meanwhile, the cyber insurance market, whose value in Europe is likely to treble to nine billion euros by 2020, will start to enforce its own discipline, rewarding those who take the right precautions.

Europe faces 4,000 cyber attacks a day

The public sector can support this market shift. The rules set out in new EU data protection legislation – including fines of up to €20m for breaches – reflect the seriousness with which EU citizens treat their personal privacy, and offer a powerful incentive for businesses to act accordingly. That is sorely needed: over 12 months, two billion personal records were reported as breached, according to the EU police agency Europol.

New EU network and information security laws will also oblige national governments to ensure that critical infrastructure is protected from electronic attacks. Major sectors such as banking and transport will have to assess and take action against cyber risks – and ideally others should too, especially the public sector. Once they start doing so, there will be a large scale market to supply cyber secure products.

These pull factors must be combined with a push. EU economies of scale mean we are working with the private sector in a €1.8bn partnership to develop new cyber technology – a partnership we intend to extend and develop.

We have also just announced we will be supporting a voluntary framework for certification, so suppliers of new connected devices can assure potential customers their wares are cyber secure, across the largest single market in the world. Currently some EU countries have such standards, and others don't; in some cases, businesses must submit to separate tests in each EU country they want to sell in – a cost most can ill afford.

With 95 per cent of cyber incidents

The tech industry has a duty of care to customers

enabled by some kind of human error, this "big picture" security needs to be accompanied with the most basic cyber hygiene – ensuring everyday internet users have the digital savvy to avoid putting themselves at risk, choosing decent passwords, backing up their work and so on.

Ultimately, keeping us all secure will require the market to change its model. Upgrades are expensive – and we end up with a situation where, for example, forces like Greater Manchester Police try to squeeze as much juice as they can from the lemon, and hang on to obsolete systems such as Windows XP.

If they are not sufficiently secure, we all pay the price. Cash-strapped public services, in particular, would benefit from a more flexible approach – for example, where you can get a residual trade-in value for out-of-date software, just as you would for your old car.

Malware and cyber attacks sit alongside a host of other cyber-enabled risks: online terrorist propaganda, election tampering, and "fake news"-style misinformation. Each of these threats needs a different, tailored response, which will in any case have to recognise fundamental rights like free speech. But, here again, the private sector has a major role to play.

The EU is working directly with internet platforms small and large to ensure terrorist material from Da'esh and others gets taken down immediately, or is prevented from upload; we will consider EU legislation if it is needed. On fake news, we want to support a free and quality media, while ensuring people have the digital awareness and critical thinking skills to separate fact from fiction.

Looking to the future, like many of the other security threats we face, cyber risks are not targeted against any one European nation, but against all of us, and the values we share; they travel easily across borders. The products and services we use online are sold in many different countries; so are their vulnerabilities, and the internet value chain is only as strong as its weakest link.

So ongoing cross-border cooperation will continue to be the best way to manage a cross-border threat – something which both sides in the current Brexit negotiations have recognised. None of that is to say it will be easy: there are legal, political, technical and financial issues to resolve.

The coming months give both major parties the opportunity to work out, in detail, how they want the future relationship to look. Security, online and off, should be a major element.

SHUTTERSTOCK/DAFINCHI

Smoke, mirrors and cyber security

It's time to strip cyber criminals of their camouflage, according to Simon McCalla, chief technology officer at Nominet

The Domain Name System (DNS) is a bit like a telephone directory for the internet. It lists, tracks and matches domain names – such as www.nominet.uk – to machine-readable IP addresses to direct web users to a desired site. Given the sheer volume of web traffic, it should come as no surprise, then, that DNS has become one of the most targeted areas of cyber security.

Several key factors make DNS particularly attractive to cyber criminals. Due to its "behind-the-scenes" nature – the IP address is camouflaged by the domain name – it is very often overlooked by system administrators. Most firewalls, in fact, tend to whitelist DNS. For criminals able to manipulate the domain name of a company website, there is an opportunity to carry out clever cyber attacks involving spam, phishing, click fraud or brand-jacking. Brand-jacking means imitating an existing domain name and website's features so the user is tricked into thinking it is a legitimate site.

The DNS racket, though, carries its own flip side. Ipso facto, if DNS is a centralised resource for criminals, it is also a centralised resource for those looking to stop them. Empowering organisations to protect and monitor their own access to DNS is, therefore, at the core of Nominet's cyber security strategy. As DNS is "always on" it is the ideal place to plug in extra defence software to offer protection from threats that traditional security measures, including antivirus programmes or network firewalls, would overlook.

That DNS security relates to a centralised resource as opposed to an individual device means this is more cohesive than an organisation trying to safeguard every single device that it might use. Every desktop, every laptop, every tablet or every smartphone inside an organisation's walls represents a different access point with a potential vulnerability. DNS-centric security, however, sees all bases covered.

It is understandable that as the world becomes more digital companies can be daunted by the rate at which it is happening. Cyber security is no longer a nominal consideration for businesses. It should be factored into every budget and every decision. As much a risk to a company as losing data is the residual reputational damage an attack can incur. A failure to keep cyber security up to date can cause long-term damage to a company's brand.

At Nominet, we have developed DNS-related services to help companies understand what's happening on their network. Our support packages range from one-off incident reporting following a breach, with board-appropriate collateral to help give a clear picture of what happened, through to live monitoring in which our team of experts proactively monitor the network, alerting the company to any issues and supporting them in solving them. We are armed with a deep-dive analytics tool to analyse huge volumes of data and swiftly identify the cause and nature of an attack.

Our active defence platform is already used by the UK government, which we would hope is viewed as a stellar endorsement of our expertise. Looking ahead, we are hopeful that Nominet can realise its international ambitions and do the same for companies and governments worldwide.

For too long DNS has been used by hackers as an easy portent for cyber crime. It is, in essence, ready-made infrastructure. But that is something that Nominet intends to use to its advantage. After all, even highwaymen need to use the highway.

IN ASSOCIATION WITH

NOMINET

Andreas Haggman, PhD researcher in cyber security at Royal Holloway, University of London, has created a board game to help UK military and policymakers better understand the threats of the digital world

Why so serious? Introducing a fun take on cyber war

Games can be more than a jovial pastime. Children playing hide and seek in the playground and the annual family game of Monopoly at Christmas are not only entertainment, but also serve important functions for social and cultural development. Just consider the character enrichment of Uncle Tom flipping the table and storming out after once more landing on Go to Jail. This emotive and evocative power of games has long been recognised and formally studied.

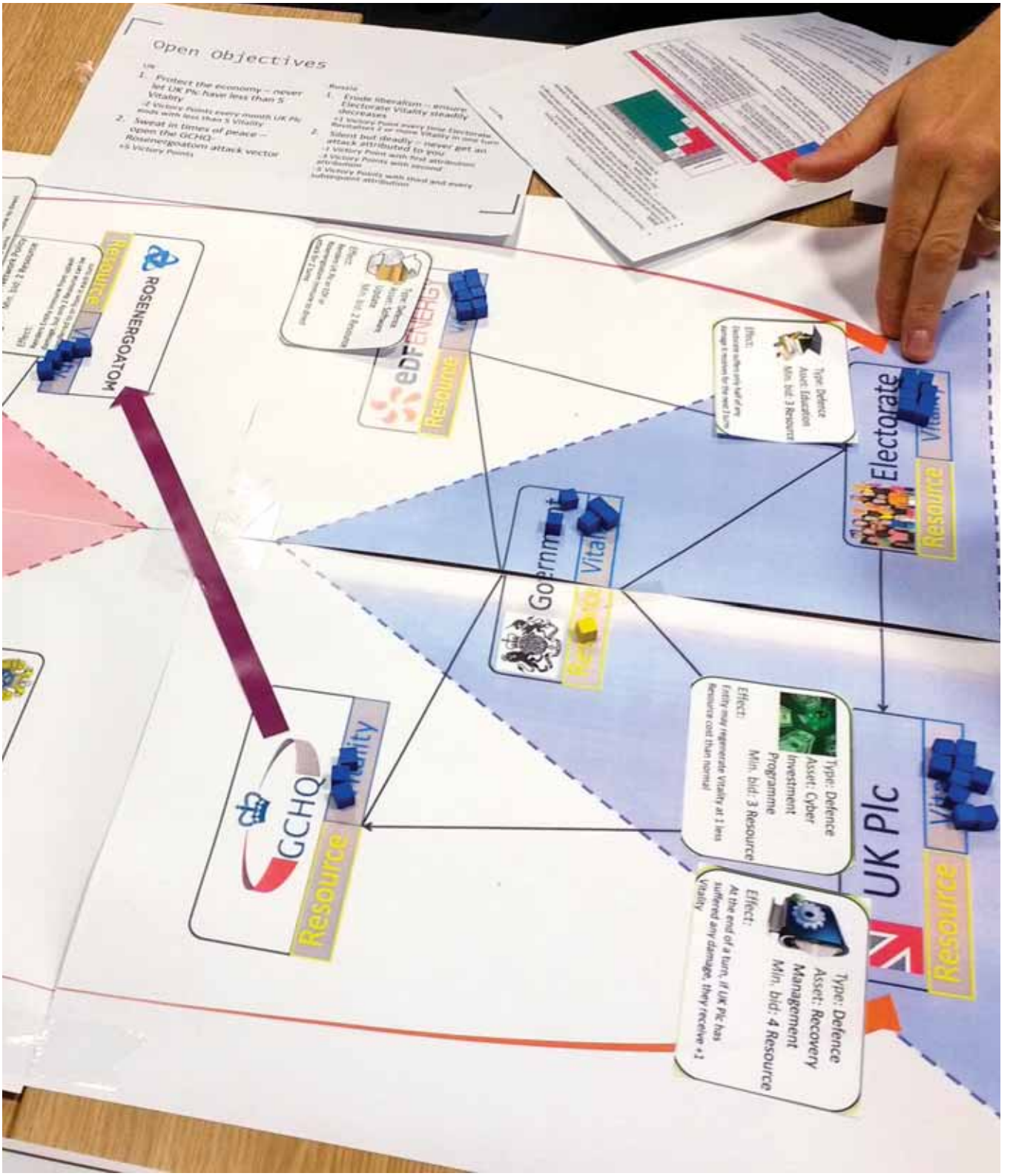
Beyond academia, the power of games has been recognised by a variety of professions. The type of games with the longest history of serious use are wargames, which are used to train military officers in strategy and tactics and their ancestry can be traced back some 5,000 years to Chaturanga in India (a precursor to Chess) and Wei Hai in China (a precursor to Go). Modern wargaming finds its direct roots in 19th century Prussia where Baron von Reiswitz invented Kriegsspiel (literally: "wargame") in 1811.

Kriegsspiel took place on a board with terrain pieces to model geographical features and its playing pieces were representative of real Prussian military units. Dice were incorporated to simulate the unpredictability of conflict and other mechanisms were devised to model difficulties with visibility and communications (later encapsulated in Carl von Clausewitz's famous concepts of "fog and friction"). With further improvements and variation developed over time, Kriegsspiel set the standard for wargaming in a professional context.

The fortunes of wargaming have waxed and waned over the past 200 years, often being cast aside as new methods or technologies were developed. In the 1950s and 1960s, for example, scientific approaches such as game theory and systems analysis took precedence, while in the 1980s and 1990s the rise of the personal computer saw a slump in interest in manual wargaming. At the present time we are experiencing a renaissance in wargaming, with multiple sectors outside the military sphere recognising the utility of games for helping shape how organisations tackle an increasingly entropic world.

One of the most pressing issues today is that of cyber security, which continues to make headlines through ceaseless incidents of compromised systems and data loss, while the spectre of cyber war is carelessly waved around in the media. It also used to be the case that cyber security was seen as a purely technical domain, impenetrable to anyone without a computer science degree. However, this has started to change, with recognition that effective cyber security requires a multidisciplinary approach involving social science and humanities fields such as psychology, law, international relations, ethics, and policy.

Despite recognition of the importance of cyber security and its multifaceted nature, very few wargames exist (in the public domain) that tackle this matter. My own PhD research in the



In the game, the UK has a 50% chance of winning

Centre of Doctoral Training in Cyber Security at Royal Holloway, University of London, has sought to ameliorate this situation.

I have created a table-top wargame based on the UK National Cyber Security Strategy in which two teams of players take control of the UK and Russia. The game is structured around five fundamental constituents of cyber space: government, business, people, military/intelligence, and critical infrastructure, each of which are tasked with attacking, defending, or ensuring prosperity.

Players must manage limited resources to achieve conflicting objectives, while grappling with some of the fog and friction inherent in navigating cyber space, including unforeseen geopolitical events and a black market for offensive and defensive assets.

The game is targeted at senior policy decision-makers, though anyone with an interest in cyber security can play it and gain something. It is intended as a learning exercise, not in the sense that actions taken in the game translate directly to real world policy, but in that the game introduces players to basic and indispensable concepts in cyber security.

The game effectively offers a cyber security 101, without technical jargon or prior knowledge required, and in a setting which is significantly more engaging and rewarding than a PowerPoint presentation or online course. Through the emotive and evocative power of games, my game prompts discussions which enable players to test and share their knowledge and understanding, creating a stimulating learning environment.

Over the course of my PhD research I have conducted over 30 game sessions with more than 250 players across military and civilian organisations in both the UK and internationally, such as the UK Foreign & Commonwealth Office, the NATO Centre of Excellence Defence Against Terrorism, and the German Command and Staff College (thereby bringing the game to its spiritual home). These sessions have yielded a wealth of data about the efficacy of the game and how players engage with it.

So what does the data tell us? Well, if we want to predict the next cyber war by simply crunching the numbers, we find that the UK has a 50 per cent chance of winning, with Russia a 42 per cent chance and 8 per cent chance of a tie, with the war likely to end around 26th October 2020. Looking at average scores (all: 19.08), we also find that we want a good mix of people in charge of the country (mixed groups: 22.25), but not civil servants as they scored the worst (7.50).

However, these numbers are only meaningful if the game model is an accurate depiction of the real world, which it is not. The game model is representative of the real world, but only in a stylistic and in some ways deliberately incorrect way, encouraging players to challenge the game model and thereby derive pedagogical outcomes through discussions. The qualitative data these discussions yield are more meaningful to determine whether the game is an effective learning tool.

Perhaps the most illustrative example of the game fulfilling its purpose came from the play session at the German Command and Staff College. During the post-game discussion, the following exchange was observed between two participants, one of whom was a cyber security expert and one who was not. P1 [expert] said: “I didn’t learn anything about cyber security, but I learned a lot about strategy and how society fits together." P2 [non-expert] said: “I had never heard of things like ransomware before, but now I know I can go ask [P1] about it.”

My game demonstrates that games about cyber security do not require a technical solution, just as cyber security is not only about technology. By creating a social setting where players are encouraged to share their knowledge, the emotive and evocative power of games can be harnessed to exchange and enhance expertise. If you agree that this is a good thing, then heed my advice: go forth and multiplay!

GDPR: dirty words or dirty business?

Business owners are overwhelmed by GDPR. Vince Picton, chief executive of Unity Metrix, explains why, armed with the right knowledge and processes, they shouldn't be

Three things amaze me. Firstly, so many small business owners are so blasé about how they look after other people's data. Secondly, that GDPR is seen as an inconvenience at best to many of them. Finally, that with just days to go so many are still doing absolutely nothing about it.

I want to tell you that the Information Commissioner is not going to run around imposing fines on anyone who doesn't comply by May 25th. I want to reassure you that your business will not suddenly fall off a cliff on that day, or that all your customers will suddenly leave you but, ask yourself this: would you put a Rolex in for repair at a jewellers with no alarm system, or your car at a garage with no CCTV when your keys are just left on the front desk?

Data is money! There are plenty of sources that suggest even personal data for a single individual can have a value of up to £850, so comparing it to a Rolex or a car is not that daft and yet, when it comes to a regulation designed to protect us from those unscrupulous garages and jewellers, who don't take the security of our belongings seriously, we lash out against it.

I personally want to know that my own data is being protected and handled in a way that is deemed to be acceptable, so as business owners you and I both shold be shouting from the rooftops that we welcome this regulation; it reinforces our own values and is an extension of what we already do, which is look after our customers.

The problem lies in the fact that business owners are confused. They know what GDPR is and they know that they are supposed to be building a register of processing activities and data-flows, or are they? And what documentation is required? And what systems need to be in place? And so on.

As the owner of a technology company, the chairman of a parish council and the teacher of a martial arts club that has spent hours deliberating the very same questions, it wasn't until I actually sat down to figure out the logic that things started to fall into place. In short, there is a logic behind the regulation that can be applied to businesses, public

There's logic behind the regulation

authorities, clubs and, in fact, any organisation. I researched what help was available and concluded that most of it relied on the dubious memories of the consultants.

Armed with the 173 recitals and 99 articles of the regulation I spent months trawling through it and automating everything I could, producing a system that we could use internally to help ourselves and other businesses achieve compliance. I developed processes that took the guesswork out of the equation, meaning that I could train others to use the system and pretty much guarantee that as long as our advice is followed closely, our clients will not only be compliant, but they will also have the correct infrastructure and processes in place to protect their client's data properly.

For more information contact us by email: infosec@unitymetrix.com or call 01582 380505

IN ASSOCIATION WITH

Can nuclear weapons be hacked?

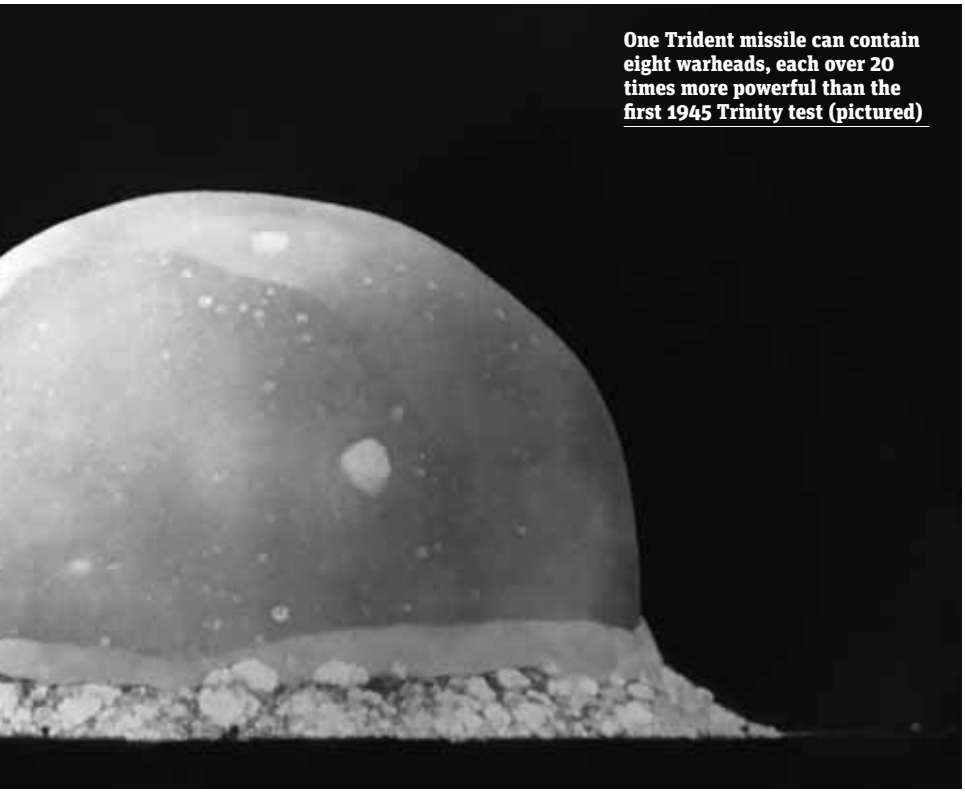
With cyber-enhanced "hybrid warfare" beginning to redefine the battlefield, Will Dunn asks the experts and the MoD whether the world's most dangerous weapons can be compromised

The Trident II D5 missile is powered, in the first moment of its flight, by steam. Inside the launch tube, an explosive charge vaporises a tank of water in a flash. This creates a sudden huge increase in pressure that pushes the missile – which weighs almost 60 tons and is one and a half times the length of a Routemaster bus – out of the submarine, up to the surface and a short distance into the air above the surface of the ocean. As soon as the missile senses that it has begun to fall back towards the waves, the first of its rocket engines ignites and it begins to climb into the air. The power of these engines is phenomenal; in less than two minutes, the missile reaches 24 times the speed of sound, covering five miles a second.

The last publicly known Trident missile test by the UK was in June 2016. HMS Vengeance, then submerged off the coast of Florida, released a missile programmed to head south-east across the Atlantic, crossing thousands of miles of unpopulated ocean to a point below the southern tip of Africa, but this did not happen. According to defence sources, the missile headed instead towards the mainland United States.

Dr Beyza Unal, a senior research fellow in the International Security Department at Chatham House, remembers discussing the malfunction with colleagues at the UN. "There were rumours about it," she recalls. The MoD's explanation was that the missile (which did not contain nuclear warheads) was not faulty, but that it had been supplied with the wrong information; the missile itself quickly recognised the mistake and self-destructed. While Downing Street claimed that the test had therefore been "successful", the pattern of events were of the kind Dr Unal and her colleagues look for. "If a cyberattack happened to a missile system," she explains, "that is

BERLYN BRIXNER



One Trident missile can contain eight warheads, each over 20 times more powerful than the first 1945 Trinity test (pictured)

the kind of consequence that we would see – the ballistic missile or the cruise missile going off from its route."

It is far from the only scenario, however, being discussed in the increasingly pressing field of nuclear cyber security. For more than 70 years, a small group of nations has used the exclusive control of weapons capable of killing vast numbers of civilians to maintain what Winston Churchill described as "the delicate balance of terror". But in recent years, as cyberattacks have become more sophisticated and effective, it has become increasingly likely that they will in some way compromise the world's most dangerous weapons.

Another recent event with all the hallmarks of a hack took place on the morning of the 13 January this year, when every smartphone in the state of Hawaii suddenly displayed the message: "BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL." A second message, sent 38 minutes later, acknowledged that the alert had been a false alarm. While the incident was blamed on an individual pressing the wrong button, Unal says it illustrates that a cyberattack on a nuclear defence system need not directly affect munitions. For Unal the most vulnerable parts of the nuclear weapons complex are "communications, and command and control. The vulnerability relies on the communication channel, and based on misinformation, the decision maker makes a faulty decision. That is, I think, the most worrisome part."

Dr Andrew Futter is the director of research for politics and international relations at the University of Leicester. For his third book on nuclear arms policy, Hacking the Bomb: Cyber Threats and Nuclear Weapons, Futter interviewed people in both the cyber security and nuclear parts of the MoD and the Royal Navy, former officials of the US Defense Science Board and the Obama administration, as well as experts from Russia, China, India and Pakistan. With many of these people he discussed what would happen "if the Cuban Missile Crisis happened today – would JFK have the same amount of time? Would you have tweets coming out all the time, and CNN watching the ships moving in?" The broad consensus is that a modern nuclear crisis would take place, he says, in a "different information environment," one in which "others may interfere with or obscure" the information needed to make the right decision. In a present-day Bay of Pigs scenario, "the time between discovery and decision would be compressed, and that doesn't normally make for good decisions."

Misinformation poses the most serious risk, says Futter, to "those ICBMs in the US and Russia that only need a few minutes to go." Simple interference in communications – Unal points to satellites as a potential weak point – could be enough to stop the most important military decisions being made with a cool head. "Keeping weapons on high alert in a cyber environment," says Futter, "is an enormous risk."

Beyza Unal recalls the story – related memorably in David E. Hoffman's Pulitzer-winning investigation of automatic nuclear systems, Dead Hand – of the most cool-headed decisions of the Cold War. The Russian lieutenant-colonel Stanislav Petrov was in charge of the Serpukhov-15 early warning station on the night in September 1983 when the Soviet Union's satellites, sending data to the country's most powerful supercomputer, registered a nuclear attack by the US. Despite being warned that five ICBMs were on their way to the USSR, Petrov told the decision-makers above him that the signals were a false alarm. "And he was right," says Unal. "But a cyberattack could look like that, a spoofing of the system. Some say that humans are the weakest link in cyber issues. I say humans are both the weakest link and the strongest link. It depends ↵

on how you train them."

Petrov was able to make the right decision because he had spent a decade working on the base, developing its systems. A good sense of what a glitch looked like, paired with his contextual knowledge of how the US would be expected to act, allowed him to read the situation correctly. An automated system – devoid of hunches, experience or wider geopolitical understanding – may not have made the same call.

Despite this, armies around the world are upgrading their nuclear weapons with greater automation and connectivity, potentially at the expense of training. "In the US," says Futter, "there's a real enthusiasm towards moving to, and I quote, 'internet-based or internetted systems' for use in command and control. That sends shivers up my spine."

While misinformation is very dangerous, a hardware vulnerability is more serious still. Both experts, however, agree that these vulnerabilities exist. Unal is concerned by what she describes as "the supply chain vulnerability," because it is "something that states generally can't do much about. The nuclear weapons system is composed of small components. All those components cannot come from the nuclear laboratories. How many computer chips can a lab produce? So, you need to rely on the supply chain for certain components. Do you know that those components are all secure?"

In 2014, a Pentagon investigation found Chinese-made components and materials in Boeing and Lockheed military planes and in Raytheon missiles. But it is the smaller subcontractors used by large defence companies that worry Futter and Unal. "Even if [the component] is made in the UK," says Unal, "how do we know that the company that produces those chips is paying attention to the cyber security risks? It's hard to regulate these things, but there should be a reporting structure on how they are securing components."

Data breaches and other incursions have been reported by defence companies, but smaller subcontractors could be wiped out by the reputational damage of going public. For this reason, Unal says we "probably don't know the vast majority of the vulnerabilities" that exist in the supply chain.

Futter says it's important also to remember that in the case of the US-built Trident system, "we don't write the coding in the missiles". In a world in which a new car comes with over 100 million lines of code, Futter says he doubts that "anyone in the UK could really check through that coding, to see that it is exactly what we think it is. If anybody managed to find a vulnerability in Lockheed or one of their subcontractors in the US and compromised the Trident SLBM, there would be nothing we could do about it."

Futter says the attitude of "a number of British officials" he's spoken to "was that Trident submarines can't be hacked because they're lying on the bottom of the North Atlantic somewhere. But these submarines rely on different systems for the nuclear propulsion plant, navigation, and even for things like the toilets, fresh air and fresh water. All these different computer systems have to be written and built by somebody. The submarines come back into port and have to be updated." Unal agrees: "how do you do maintenance? You infiltrate the system. You do that using a [back]door, and that is an attack vector."

Trident, however, is low on the list of concerns in this field. Both experts point to the India-Pakistan region as an areas in which, says Unal, "there is a high likelihood of nuclear weapons use. The threshold is really low. Any uncertainty created through jamming or spoofing information could create an attack." Between the world's only hostile nuclear neighbours, Futter says the "timelines are so short for decision-making that even something like a denial of service attack, if it happened in the middle of a crisis, could escalate things quickly."

"Russia sees this as an enormous threat"

Futter says the relationship between the US and China could also be compromised due to the nature of their systems. "China has linked in the support systems for conventional and nuclear weapons," he explains, "so an attack to try to shut down a conventional Chinese weapons system could accidentally compromise a nuclear weapon. And then you've got all sorts of escalation."

Of the nine nuclear powers, one state values nuclear cyber security more than any other. "Russia now sees the possibility of this happening – it's even stated in its national security documents – as an enormous threat," says Futter – "one of the biggest threats it faces."

MINISTRY OF DEFENCE

This concern is well informed; Russia is probably the only state to have hacked an adversary's weapons during conflict.

In the spring of 2013, a Ukrainian army officer called Yaroslav Sherstuk developed an app to speed up the targeting process of the Ukrainian army's Soviet-era artillery weapons, using an Android phone. The app reduced the time to fire a howitzer from a few minutes to 15 seconds. Distributed on Ukrainian military forums, the app was installed by over 9,000 military personnel. By late 2014, however, a new version of the app began circulating. The alternate version contained malware known as X-Agent, a remote access toolkit known to be used by Russian military intelligence. The cyber security firm Crowdstrike, which discovered the malware, said that X-Agent gave its users "access to contacts, SMS, call logs and internet data," as well as "gross locational data". In the critical battles in Donetsk and Debaltseve in early 2015, the app could have shown Russian forces where Ukraine's artillery pieces were, who the soldiers operating them were talking to, and some of what they were saying. It may be, then, that Russia's concern – Futter describes it as "panic" – about the risks of hybrid warfare is based on the knowledge that it has been used in battle, and it works.

In the UK, by contrast, there has been little public debate on the cyber security of nuclear weapons. Text searches show that in six years, none of the Updates to Parliament prepared by the MoD on the nuclear deterrent contains a single mention of cyber security. Hansard shows fewer than five mentions of the subject in a decade; no cabinet member has ever spoken publicly on this issue.

This may be partly to do with the fact that nuclear weapons are already hugely expensive and politically divisive. "If they ask for the extra money for cyber security," says Futter "then someone will ask them how secure it really is."

But Beyza Unal underlines why this question must be asked anyway. On the question of why states haven't yet hacked each other's nuclear weapons systems, she says the first point to recognise is that "we don't know if they have or not. Maybe they have already. Even if they haven't done it, probably they will, because there is no system that prevents them hacking each other's weapons systems."

Nuclear weapons are supposed to be political rather than military ordinance: they keep the peace without ever being used. But without open discussion of the risks, without preparation and training at all levels to defend against them, and without international agreement on the boundaries of such actions, the barriers to their use are being silently and invisibly eroded.

THE MINISTRY OF DEFENCE RESPONDS

Asked to comment on the issues raised in this piece, an MoD spokesperson said:

"We have absolute confidence in our robust measures to keep the nuclear deterrent safe and secure. Cyber threats are not new or treated in isolation as we invest significant resources into continually checking the deterrent is completely protected against a wide range of external challenges. The UK takes cyber security very seriously across the board, doubling its investment in the area to £1.9bn and boosting capabilities.

"The annual updates to Parliament focus on the progress of the Dreadnought submarine build programme. To go into detail on every possible system, sub-system or activity we consider for Dreadnought would make the report impracticably long. MoD employs a layered defence against cyber threats across the breadth of systems we operate. It is therefore not a simple matter to detail all of the cyber security measures that protect the nuclear deterrent and other capabilities."

Turning military experience into digital know-how

The new not-for-profit organisation TechVets provides a bridge for veterans into cyber security. Co-founder Mark Milton explains why military personnel are highly qualified to develop the UK's security capabilities

The United Kingdom is facing a critical skills shortage in cyber security. According to a 2017 report by ESG and ISSA, 45 per cent of organisations claim to have a chronic lack of cyber security skills; 70 per cent of cyber security professionals say the skills shortage has had an impact on their organisation; and 22 per cent said that their cyber security team was simply not large enough for the size of their organisation.

Frost & Sullivan predicts the number of unfilled cyber security positions in the UK could hit 1.8m by 2022. The recent increase in the threat posed by state actors to our critical national infrastructure only serves to amplify this situation. It is clear that security leaders need to find a solution to this issue which means finding new sources of untapped talent with relevant, transferable skills.

In the past 12 months, there have been 15,000 military service leavers joining the 908,000 working-age veterans in the UK, of whom 220,000 are unemployed and inactive. Only 4 per cent of veterans work in ICT – a figure that is 20 per cent lower than their civilian counterparts. For female veterans that rises to an astonishing 50 per cent.

Veterans possess unrivalled leadership, crisis management and problem-solving skills. They are adaptable team players, comfortable with working in security environments. In exploring new sources of talent for the industry, the veteran community represents a significant opportunity. When given transitional support, veterans have the potential to make a massive contribution to the UK's cyber security sphere.

We established TechVets as a not-for-profit organisation to help bridge the

SHUTTERSTOCK/KENNY1

Veterans have unrivalled problem-solving skills

gap in cyber security. Our mission is to support service leavers and veterans who would like to build on their transferable skills and develop new ones to work in cyber security.

The government is committed to making the UK a secure and resilient digital nation, and TechVets supports this goal by recognising the unrealised human potential of our veteran community.

General Sir Richard Barrons, KCB, CBE, has recently joined as our ambassador. General Sir Richard served as Commander of Joint Forces Command, one of the six chiefs of staff leading the UK Armed Forces until April 2016. He agrees that "the transferable skills of the veteran community are a national resource and have a vital role to play in supporting the security and prosperity of the nation."

In early March we held a launch event at the Level 39 office complex in Canary Wharf. The event provided an opportunity for the veteran community to hear from their former peers who have succeeded in cyber security, and to network with industry leaders from the National Cyber Security Centre, Amazon, IBM, Google, Oracle, Google Deepmind, the Institute for Cyber Security Innovation, Hut Zero and RAND Europe.

On the 5 April, in collaboration with our industry partner Immersive Labs, we launched the Veteran Cyber Academy (VCA). The VCA provides free cyber security training and employment opportunities for TechVets.

Robert Hannigan, former director of GCHQ, says of the platform: "Identifying, developing and measuring practical cyber security skills is the great challenge for all companies today. The Immersive Labs approach is the most exciting thing I've seen in this space: scalable, agile and appropriate to the way a new generation learns. It has the potential to disrupt and transform this crucial market."

The first cohort of 200 – the programme was oversubscribed five times – students began their training on the platform on the 5 April, and the feedback received so far has been overwhelmingly positive.

Looking forward, TechVets aims to do three things. Firstly, we intend to expand the first cohort of 200, who have access to the Veterans Cyber Academy. We are keen to engage with industry partners who can use the academy as a technical vetting recruitment tool, as well as identify and develop their existing talent.

Secondly, we want to build on the success of the launch and continue to run networking events for the veteran community throughout the year. These events will serve to both inspire and build networks in the industry. We will also be working with our peer organisations in the US, Australia, Canada and New Zealand to hold an annual summit, which will enable us to share knowledge, build relationships, and create international opportunities for our respective veteran communities.

Thirdly, we are going to develop a resource for the veteran community which allows exploration of all the job roles and career paths in cyber security and technology. The site will provide information relating to the latest opportunities, professional development and academic courses to help veterans discover the right career path for them and to make positive steps towards it. We will be working closely with CREST, IET and the BCS in this work.

Core to our principles is the avoidance of duplication, and we will continue to work closely with our supporters in industry (Amazon, Barclays, Deloitte, Google, IBM, Immersive Labs and Oracle); in academia (Information Security Group at Royal Holloway, and the Institute for Cyber Security Innovation); in government (MOD's Career Transition Partnership, Defence Relationship Management, DCMS and the Cabinet Office); and in the military charities and not-for-profits (COBSEO's employability cluster, the Royal British Legion, SSAFA, RFEA, and RBF).

How do you know if you have been breached?

Gayle Kennedy of Countercept explains how a cyber attack nearly brought an international energy company to its knees, and how, with the right support, it was defeated

IN ASSOCIATION WITH

COUNTERCEPT

A false sense of security

On the surface, this energy company appeared to have all the basic security systems in place, including intrusion detection and firewalls. "Many CIOs would deem all the security boxes ticked," said Adam Bateman, managing director of Countercept. "But the reality is that many automated systems are easy for even an amateur hacker to work around."

The attack began as most modern-day attacks do – with the attacker performing reconnaissance on the organisation and its security. By sending a series of emails to the company, the attacker tested the email filters to see what kind of files would go undetected by the company's antivirus software.

Employees are still the weak link

Twenty days later, the attacker sent a phishing email to an employee that contained the Dridex malware, already knowing antivirus controls would not detect it. The malware utilised PsExec – a legitimate Windows process – to run GPG, a similarly legitimate encryption programme used by many organisations. "This kind of attack really pushes the boundaries of attack detection and incident response, as the use of legitimate business tools makes it difficult for an automated detection system to discern what is genuine and what is malicious," said Paul Pratley, head of incident response.

By the time employees noticed that certain files could not be accessed, 70 per cent of the company's data was encrypted and the attacker was moving laterally across multiple locations.

Enter Countercept

It was at this stage that the company contacted us. Our team were on site within a day and were able to gain visibility of the estate within an hour. From that point, we were able to see where the attackers were, where they'd come from, and their access channels. Shortly afterwards, we had nailed down the predominant techniques, tactics, and procedures (TTPs) in use. "We had a master ticket with over 20 tickets in different states," said Alex Davies, TechOps lead at Countercept. "There were many different balls in the air."

Ransom demand withdrawn

Two weeks after our teams first appeared on site, the key assets that had been under the attackers' control were contained – including domain controllers, domain admin logins, and high value assets – and work had commenced to rebuild the infected parts of the IT estate. Meanwhile, we triaged new findings and funnelled them over to the customer for handling, staying on hand to provide guidance and support all the while. In the end, the customer data was secured and the ransom demand made null and void.

"We not only prevented the customer from paying £1m of ransom, but also eliminated the risk of its entire server estate being taken over," said Adam Bateman.

Since then, we have been providing continuous managed detection and response to prevent such attacks from ever happening again. "Countercept provides the capability to defend against targeted attacks, and has already protected us from advanced cyber groups and substantial monetary losses," said the company's CIO. "As a technology leader I believe the Countercept offering to be unique and effective, and that it will improve the state of the attack detection industry."

Find out more: www.countercept.com

CYBER SECURITY: INDUSTRY INSIGHT

The sector's key business deals, jobs and important dates

Contracts and suppliers

Tenders now open
The following public sector tenders are currently open for bids from cyber security suppliers.

East Midlands Strategic Commercial Unit
Contract title: Provision of a Client Side Delivery Partner Service for the Police National Enabling Programme
Bid deadline: 10/07/2018
Tender value: £20.0m
Details: "EMSCU is looking for suppliers to provide a strong cyber security platform to improve collaboration – data handling and intelligence sharing – between UK police forces."
Contact: michael.case16809@emscu.pnn.police.uk

Phoenix Community Housing Association
Contract title: Data Protection Officer Services
Bid deadline: 04/05/2018
Tender value: £45,000
Details: "Phoenix Community Housing Association is seeking GDPR compliance services. The contract is for one year initially with the opportunity to extend after nine months for two more years."
Contact: say.leddington@phoenixch.org.uk

TOTAL VALUE: £20,045,000

Tenders coming up
Public bodies can make their intention of planned procurements known by publishing a **Prior Information Notice (PIN)**. This is not an actual tender but provides potential suppliers with information about what public bodies are planning to buy in the future – products, services etc.

New PINs (last six months):

Cisco Cloud web security licences for the Royal Borough of Kingston upon Thames
Bids to be submitted by: 17/12/2018
PIN value: £79,000

GDPR compliance software for Bedford-based social housing association bpha
Bids to be submitted by: 01/05/2018
PIN value: £60,000

Information risk management for the Frimley Health NHS Foundation Trust
Bids to be submitted by: 13/10/2018
PIN value: £40,000

Digital office supplier engagement for Scotland Excel, the centre of procurement expertise for Scottish local government
Bids to be submitted by: Ongoing
PIN value: Unspecified

TOTAL VALUE £179,000

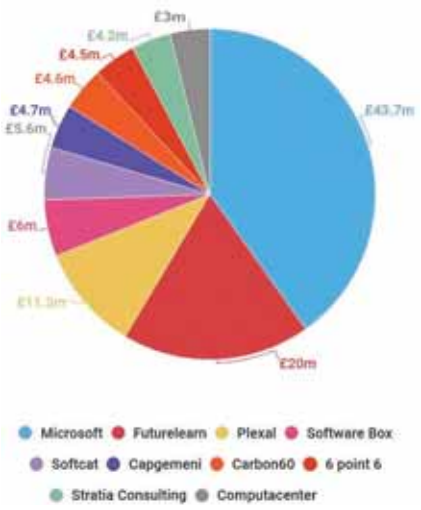


Chart: the biggest public sector suppliers in cyber security, by award value since January 2015

tussell

Tender and framework information supplied by Tussell, a data provider on UK government contracts

Expiring contracts

These are the most valuable awards due to end in the next six months, which may therefore be re-tendered in the near future.

IT Health Check and Penetration Testing
Contracting authority: Department for Work & Pensions
Current supplier: CGI
Contract expires: 09/07/2018
Award value: £2.4m

Security Education & Awareness Programme
Contracting authority: Department for Work & Pensions
Current supplier: Informatica Software
Contract expires: 30/06/2018
Award value: £2.1m

Network Support and ICT Security Managed Service
Contracting authority: London South Bank University
Current supplier: Multiple
Contract expires: 01/09/2018
Award value: £1.5m

Security Operation Centre (SOC) Services
Contracting authority: Driver & Vehicle Licensing Agency
Current supplier: IBM
Contract expires: 01/07/2018
Award value: £1.4m

Cyber Security Taskforce
Contracting Authority: Home Office
Current supplier: Hunter Macdonald
Contract expires: 10/10/2018
Award value: £1.2m

TOTAL VALUE: £8,600,000

The most valuable contracts

These are the most valuable cyber security awards and frameworks issued in the last six months.

Financial Conduct Authority
Supplier: Multiple
Contract title: Skilled Persons Cyber Panel
Date awarded: 23/03/2018
Value: £40.0m

Department for Culture, Media and Sport
Supplier: Plexal
Contract title: London Cyber Innovation Centre
Date awarded: 29/01/2018
Value: £11.3m

Ministry of Defence
Supplier: Carbon60
Contract title: Provision of ICT Support and Security Service for Navy Command
Date awarded: 20/03/2018
Value: £1.1m

NHS Business Services Authority
Supplier: NTA Monitor
Contract title: NHSBSA Penetration Testing
Date awarded: 22/01/2018
Value: £0.9m

Chorley Borough Council
Supplier: Insight Direct
Contract title: Further Competition for Provision of ICT Infrastructure and Disaster Recovery
Date awarded: 15/01/2018
Value: £0.4m

TOTAL VALUE: £53,700,000

IMPORTANT UPCOMING DATES

9 May

The EU's Network and Information Security (NIS) directive is implemented into UK law. All companies identified as either "operators of essential services" or "competent authorities" must comply.

22 to 23 May

The third annual Cyber Senate Nuclear Industrial Control Cyber Security and Resilience Conference will take place in Warrington. This two-day forum will include roundtable discussions and presentations.

JOBS, MOVES AND REWARDS

Vacancies

Cyber Security Architects,
National Cyber Security Centre/GCHQ
Salary: £51,000 to £100,000 per annum DOE
Location: London/Cheltenham
Closing date: Ongoing
Key responsibilities: The NCSC is looking to recruit experienced cyber security architects to consult on the secure design and operation of some of the most important computer systems in the UK. The successful candidates will design and review whether the security controls for a computer system are strong enough across government and the wider public sector. This is based on a thorough understanding of both use and context, and how the system could be attached. Cyber security architects will research and develop new techniques or tools to address systemic security issues.

Vulnerability Remediation Engineer, Apple
Salary: Competitive
Location: London
Closing date: Ongoing
Key responsibilities: Apple is looking for someone to counter any emerging security vulnerabilities amongst its products and services. The successful candidate will have strong communication skills and a calm head under pressure. The role involves vulnerability management for the application and business team, authoring clear and concise responses to security queries. Applicants should have a Bachelor's degree in computer science, with two years' experience in cyber security, or five years' experience without a degree.

Defence Assurance and Information
Security Lead Accreditor, Ministry of Defence
Salary: £37,940 per annum
Location: Huntingdon, Cambridgeshire
Closing date: 5th May
Key responsibilities: The successful candidate will shape the design of secure Ministry of Defence-wide ICT systems and services. The Defence Assurance and Information Security Lead Accreditor will report to the Senior Information Risk Owner (SIRO) and work to improve the Assurance and Cyber Security advisory service to the MoD. Responsibilities include acting as an impartial assessor of the risks that an information system may be exposed to in the course of meeting a business requirement, and confirming that the specific implementation of any system, platform or infrastructure has been adequately secured.

Ethical Hacker, Driver and Vehicle Licensing Agency
Salary: £29,832 to £42,991 per annum DOE
Location: Swansea
Closing date: 31st May
Key responsibilities: This is a hands-on role, carrying out penetration testing activities on applications and infrastructure and helping to define and implement best practice in support of cyber security. The ethical hacker will undertake White Box and Black Box testing services executed both internally and remotely across a number of security domains.

Technical Architect, Government Digital Service
Salary: £50,000 to £80,000 DOE
Location: Multiple – Wales, London & South East, the Midlands
Closing date: Ongoing
Key responsibilities: The role involves being responsible for the design of cyber architecture and undertaking structured analysis of technical issues. The technical architect should be able to be consulted on design, identifying the deeper security issues that need fixing, and explaining them to technical and non-technical stakeholders.

IMPORTANT UPCOMING DATES

25 May
The General Data Protection Regulation (GDPR) will be enforced across all organisations using EU citizens' data.

30 June
This is the deadline for the NHS to update the Public Accounts Committee on what it has done to improve cyber security after the WannaCry ransomware attack.

Appointments

August 2017
Theo Blackwell was appointed as London's first-ever chief digital officer. Theo joined the Mayor of London's team with extensive public and private sector experience. As a cabinet member for finance, technology and growth at Camden Council, he established Camden as London's leading digital borough through its use of public data. Theo's appointment, the Mayor said, is part of a wider strategy to make London the "world's smartest city". Theo has been tasked with making sure that public services are designed and delivered accessibly and efficiently.

January 2018
Colin Lobley was appointed as chief executive of Cyber Security Challenge UK. Lobley joined from DXC Technology's security services division, where he was general manager for the UK. Previously, he spent several years working in the civil service in various roles within the defence, research, technology and national resilience programmes.

March 2018
The Digital Office for Scottish Local Government appointed former Ministry of Defence information systems security professional Andy Grayland as its chief information security officer. Grayland's role sees him focus on helping local authorities deliver against the goals of the Cyber Resilience Strategy for Scotland, the National Cyber Security Strategy, and the recent Scottish Government Action Plan on Cyber Resilience.

April 2018
EY hired Andy Ng as information protection leader responsible for supporting client firms with best practice in data loss prevention, the incoming GDPR and strategic alliances between companies. Previously, Ng worked as Deloitte's director of cyber risk services.

April 2018
McAfee has appointed Nick Viney as regional vice-president for the UK, Ireland and South Africa, with his primary duty to drive business growth. Before being promoted to regional VP, Viney was VP EMEA of the company's consumer sales division.

Bug Bounty programmes

A Bug Bounty programme is a deal offered by many websites and software developers by which individuals can receive a monetary reward for identifying bugs, especially those which cause technical vulnerabilities. This allows the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. Here are some of the most lucrative Bug Bounty programmes around:

Microsoft
Maximum payout: $250,000
Limitations: Microsoft's current Bug Bounty programme was officially launched in 2014 and deals only with online services. A bounty reward is only given for the "critical" and "important" vulnerabilities.

Yahoo
Maximum payout: $15,000
Limitations: The company does not offer any reward for finding bugs in yahoo.net, Yahoo 7, Yahoo Japan, Onwander and Yahoo-operated Word Press blogs.

GitHub
Maximum payout: $10,000
Limitations: The security researcher will receive a bounty only if they respect users' data and don't exploit any issue to produce an attack that could harm the integrity of GitHub's services or information.

Mozilla
Maximum payout: $5,000
Limitations: A reward is only offered for bugs found in Mozilla services, such as Firefox, Thunderbird and other related applications.

2 to 6 July

The annual AppSec Europe conference takes place in London, bringing together the continent's top web developers and security experts for a series of talks, panel sessions and networking events.

9 to 10 October

The fifth annual Industrial Control Cyber Security Europe Conference takes place in London. It involves presentations and debates on the cyber security risks involved in the oil, gas and chemical industries.