Emerging Threats

Work in tech? Get a fast weekly briefing on cyber security, government and business in your inbox every Wednesday morning.

Featuring:
- Cyber security news, features and analysis
- Special briefings on major attacks
- Job opportunities and government contracts

tech.newstatesman.com
Bridging the great pandemic divide

An estimated 11.9 million people in the UK lack “essential digital skills” and some four million are offline, research by Lloyds Bank has found. Yet six weeks into Britain’s lockdown, it is clear that much of the key to the coronavirus puzzle lies online. From contact-tracing apps to online school resources or simply passing the time, the pandemic and responses to it have been decidedly digital. This reliance on technology highlights the importance of internet access. Among households that have it, contract costs expose additional divisions, with those on pay-as-you-go deals spending far more on data.

The Labour Party under Jeremy Corbyn was mocked for proposing to provide free broadband. But in a world remade by coronavirus, the government and private sector are taking steps to widen access.

In March, major internet providers agreed to remove data caps on fixed-line broadband. The Department for Education has pledged to provide laptops and tablets to disadvantaged children, as well as 4G routers for those with no mobile internet or broadband.

Not being online increasingly affects access to services and opportunities, exacerbating inequalities. Those not online share certain demographics, according to the Good Things Foundation. They tend to be older and have lower educational attainment and income levels. But policymakers must make sure that digital skills catch up as digital transformation continues apace across society. Some 33 per cent of retired people say they lack such skills, but even the more internet savvy could use a boost. A recent survey of UK firms found that more than a third of respondents admitted not knowing what phishing was.

Coronavirus has seen a trend in related online scams, which prey on the vulnerable. Beyond the pandemic, however, cyber safety needs to become an integral part of education and of support for government services. Ensuring people have more confidence online might just get more of us going digital too. According to that same Lloyds Bank poll, of those who said that “nothing” would get them on the internet, 60 per cent were worried about identity theft, 58 per cent about privacy and security, and 55 per cent about use of their data.

6 / Matt Warman MP
The minister for digital on the UK’s cyber security strategy

10 / Jacqui Chard
The NCSC’s deputy director for defence on cyber awareness

14 / Prospering from a pandemic
How hackers are exploiting the coronavirus crisis

18 / Marcus Hutchins
Spotlight profiles the man who stopped WannaCry

22 / Meg Hillier MP
The chair of the Public Accounts Committee on keeping the NHS safe

24 / The future of work
How the virtual office presents evolving online risks

28 / Darren Jones MP
Why technological innovation must be regulated responsibly
Two-thirds of the UK’s remote workers have not received any cyber security training, according to a poll of 2,000 people by Promon, the app security vendor. Promon also found that over three-quarters (77 per cent) of respondents were unconcerned about cyber security, while 60 per cent said they used their own personal devices when working from home.

Last month, the UK National Cyber Security Centre warned that cyber criminals were seeking to exploit the Covid-19 lockdown, revealing a range of attacks that used the public health crisis as a pretext. Phishing emails posing as important company updates have included links that, once clicked, infect computers and professional IT networks. Cyber security experts have uncovered fake email updates posing as senders from the White House, the World Health Organisation and the NHS.

Germany has changed from a centralised to a decentralised approach to its coronavirus contact-tracing app. Reuters reported the main reason for the change was Apple’s refusal to adapt its settings on its iOS mobile operating system to allow centralised apps to run in the foreground. As it stands, only decentralised contact-tracing apps – the likes of which Apple and Google are developing – will be able to run in the background without draining the phone’s battery. By contrast, centralised apps are likely to encounter issues of battery.
A flaw in Apple’s mobile operating system iOS may have left millions of iPhone and iPad users vulnerable to cyber attacks, according to research by ZecOps. The mobile security firm claimed to have found a vulnerability in Apple’s in-built email app, Mail, and alerted the tech giant to the problem in March.

ZecOps said that hackers can embed malicious software into an ostensibly blank message, which when opened in the Mail inbox on an iPhone or iPad would cause the app to crash, forcing the user to reboot. During this lull, ZecOps suggested, hackers are able to access information on the device. ZecOps’s report claimed to have found evidence that the bug has already been used to attack several high-profile targets, including individuals from a Fortune 500 company in the US.

A spokesperson for Apple told Reuters that a fix would be included in the company’s forthcoming iOS software update, but that the company did not consider the risk to be as extensive as ZecOps has suggested. “We have thoroughly investigated the researcher’s report and, based on the information provided, have concluded these issues do not pose an immediate risk to our users.”

The Department for Education has launched “The Skills Toolkit”, offering “free digital and numeracy courses to build [users’] skills” during the coronavirus lockdown. A range of courses are being offered, from basic computer literacy and social media best practice, to more advanced areas of study such as coding and cyber security.

The Skills Toolkit website describes digital and numeracy skills as among those “most sought after by employers”. In 2016, a government report cited evidence that 47 per cent of employers said poor numeracy skills would stop them hiring young candidates. The Department for Digital, Culture, Media and Sport last year produced another report, No Longer Optional, on employer demand for digital skills. Professional roles that require digital skills pay, on average, 29 per cent more per annum than those that do not.

Zoom and Microsoft launch security updates

Rohan Banerjee

Zoom and Microsoft have acted to improve the cyber security of their home-working tools during the coronavirus pandemic.

Conferencing app Zoom, which was downloaded over 50 million times from the Google Play Store in the first quarter of 2020, allows users to host live meetings with audio, video and text messaging capabilities for up to 1,000 people on a single URL weblink. But a trend of “Zoom-bombing”, where uninvited guests had accessed people’s calls after acquiring the meeting link, led the company to take action.

The latest version of the app, Zoom 5.0, has worked in AES 256-bit GCM encryption, as well several new user features such as a report and block system, while also requiring password protection on all calls by default.

Microsoft, meanwhile, has launched a patch to address a vulnerability in its shared working app, Microsoft Teams. CyberArk, an information security firm, identified a problem with how GIF images could be corrupted and exploited by hackers on the platform, which Microsoft has now fixed.
From Alan Turing and the Bletchley Park codebreakers to the battle against climate change, technologists in the UK have been pivotal in taking on global challenges. Now, as we continue to tackle the coronavirus pandemic, the UK’s cyber security sector is stepping up to play an important role in combating the fallout from the spread of the disease. It is doing this in a number of ways.

A recent report from UK and US intelligence services showed cyber criminals are exploiting the crisis to target people and organisations. In response the government’s Cyber Aware campaign has set out ways we can protect ourselves by using strong and different passwords for online accounts, and by turning on two-factor authentication where possible.

The National Cyber Security Centre has issued guidance for home-working and dealing with suspicious emails, and it is giving organisations in the voluntary sector free access to online training. The recently relaunched Cyber Essentials Scheme helps businesses reduce the risk of falling victim to cyber attacks through targeted advice.

More broadly, cyber security specialists are helping protect our national digital infrastructure to keep people and businesses connected and ensure our NHS systems are resilient.

The Department for Digital Culture Media and Sport (DCMS) is working with the tech sector and other government departments to lead the fight against fake news. When we see dangerous or misleading content getting traction or being shared unchecked, we are acting quickly with the major social media platforms to combat it.

With the boom in digital technology, the need for cyber security professionals has never been greater. It is no surprise the number of cyber security firms in the country has grown by 40 per cent since 2017. This sector is a fast-growing...
asset for the UK. Data from a recent study for DCMS shows new cyber security tech hubs are thriving in north-west England, Scotland, Wales and Northern Ireland. They have collectively secured 20 per cent of industry investment deals over the past four years.

This government is committed to supporting firms through these challenging times and has announced an unprecedented package to help businesses, workers and organisations. While our top priority is rightly to combat the spread of coronavirus, protect the NHS and save lives, our ambition to level up the country remains unchanged.

As the minister charged with overseeing the country’s digital infrastructure and cyber security, I want everyone with the talent and aptitude to have the opportunity to succeed regardless of where they live. Through the Cyber 101 programme we are delivering boot-camps to train the next generation of professionals, most recently in Newcastle, Edinburgh, Birmingham and Newport. We have invested £2m in helping academics commercialise research and set up companies through the Cyber Security Academic Start-Up Accelerator Programme.

We must also inspire the next generation and attract talent from all backgrounds. I attended the grand final of our CyberFirst Girls Competition in Cardiff in March and watched talented students get a taste of what those in cyber jobs face every day. The nationwide CyberFirst programme has to date helped inspire more than 80,000 young people to consider a career in cyber security. We want to make sure the UK has world-leading cyber security standards to give consumers the confidence to trust organisations with their data. This is especially important as our daily lives become more connected to the internet, from fridges to security cameras and children’s toys.

The current security standards of many of these devices are low, putting the security and privacy of consumers at risk. I recently announced new legislation to hold firms that are manufacturing and stocking internet-connected devices to account.

Manufacturers will now need to make sure pre-programmed passwords in internet-connected devices are unique and not resettable to universal factory settings. At the point of sale, either in store or online, they will have to state the minimum length of time for which the device will receive security updates.

Companies making smart devices will also need to maintain a public point of contact so any security vulnerabilities found can be reported and addressed quickly. The vulnerability of such devices is a global issue and my department has been leading a cross-border initiative to create a world-standard of security.

This strategic approach to cyber security will ensure we are resilient during this crisis, and will allow us to seize new opportunities in the future.
The difference that a decade makes

Cyber security has evolved from an afterthought into a key consideration for businesses and individuals alike, says Kevin Brown, managing director of BT Security.

Over the past ten years cyber security has transitioned from a jargon-filled topic considered the preserve of IT departments to one of the key pillars of an increasingly digitised society. For where technology has enhanced plenty of products and services, it has also brought with it new risks. As more and more organisations make the move online, so too do the criminals looking to exploit them.

Cloud-based software has catalysed a culture that craves speed and flexibility, but has also created new attack surfaces, that can be made even larger by people’s oversights.

Cyber security can no longer be treated as an afterthought; it is one of the first and most important decisions any modern organisation worth its salt should make. And it is now far from an IT-only issue. Effective cyber security and resilience – that is to say a company’s capacity to cope with a breach – hinges on having a good blend of technical provision and human understanding. The latter extends from the boardroom to even the most junior member of staff.

At the start of the decade, cyber security was regarded as an optional extra. It was better to be safe than sorry was the widely accepted wisdom, but the chances of actually being made sorry were slim. Essentially, security was considered as a more defined set of defensive items – such as anti-virus programs or firewalls – that protected core services and deliverables. Most data breaches before the 2010s were unintentional or accidental. Many were focused around customer access platforms where databases of credentials or accounts were lost.

Over the past decade, it has become almost impossible for businesses to maintain the traditional outer perimeter they had so carefully built up. That security perimeter has moved from static to completely elastic as systems and individuals became more connected than ever. Cybercrime, meanwhile, has become increasingly organised along industrial lines, with groups increasingly using automated tools to speed up their attacks and make them even more targeted. Protection of data (driven by a hugely increased...
understanding of the monetary value of personal data, and the introduction of regulation such as GDPR) is now seen as absolutely key. This has meant that various layers of protection, alongside active threat monitoring and engagement, have become not just recommended but required.

The decline of physical, on-site IT infrastructure and a shift to cloud-based storage is particularly significant. Companies are looking to consolidate data in ever larger storage areas with major providers, as this allows them to move more quickly and cheaply into new ways of working. The old “self-contained” data centre model has now largely been broken as a result. The resulting need to connect the enterprise and all branch networks, data centres and international offices places increasing pressure on not just network technologies, but also security departments, which have to assess, monitor and protect their company’s data across all those locations.

As important as organisational shifts towards new technology is the rise in and evolution of personal devices. As we all got used to using app stores over the past ten years, we have also come to appreciate the risks around them – from unverified apps that may display harmful content, to app access and permissions that allow the harvesting of personal data. At a business level, security has also had to evolve to manage employees using their own devices to access company systems.

Similarly, businesses have also adapted to the massive use of social media for professional purposes, including the potential to unwillingly share confidential information. Indeed, social networks have evolved over the past decade from a tool that people used to connect with friends and family, through to being the major way that many people interact as profound implications for personal security through to misinformation and the impact of algorithms on our personal lives and nations as a whole.

Moving forward, into the 2020s and beyond, security can no longer be focused on the defence and detection picture. Rather, it must be more attuned to response and enablement. The coronavirus pandemic, which has brought about the world’s largest working from home experiment, has underscored the need for cyber security strategy to be implemented throughout organisations. Everyone has a part to play. As remote working reaches a new level of normality, businesses must consider not only how to keep their connections as secure as possible, but also engage with their staff, and inculcate good cyber hygiene.

In the future, cyber security strategy needs to be responsive and flexible. That means accepting that you can’t always control the devices people use to access information or the public networks they use, but you can control the gateways and the policy. Policy, in turn, drives exactly what you can access and how, and what you can do once you have information on your device. Businesses need to ensure that policy is applied from the centre out to their entire organisation – so that information security isn’t just considered as a traditional network or data centre issue, but applies across all business processes.

Organisations increasingly need to prioritise different security protections for specific elements of their systems, based on each element’s respective risk to the business. And the same is true for individuals and households. We all have to think about the data and assets we couldn’t afford to lose, and ensure that we have the necessary protections and “defence in depth” to protect them.

For more information, please visit: www.bt.com/security

Remote working is becoming the new normal
How are hackers seeking to exploit people’s fears over coronavirus, including employees of critical infrastructure organisations?

Life in the UK has fundamentally changed and people are relying more on technology for day-to-day services, for work, and to stay in touch with loved ones. However, with more use of this technology comes more exposure to online harms.

We know that cyber criminals are preying on people’s fears around the current pandemic. Techniques include sending phishing emails containing malware, which appear to come from trusted health organisations offering advice, and others which aim to “sell” face masks and thermometers to fight the disease. Criminals have also been scanning for vulnerabilities in remote working software as more people are working from home.

While we haven’t seen a major increase in the activity of cyber criminals, we have seen growth in coronavirus-themed attacks. We’ve highlighted this activity recently in a joint advisory with the US Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency. And this is why we’ve done a significant amount of work in recent weeks to help protect the public and businesses from those seeking to exploit the crisis.

What steps is the NCSC taking to protect citizens and businesses from coronavirus-themed scams?

The NCSC has ramped up its Active Cyber Defence programme, which looks to automatically reduce the number of cyber attacks by, for example, blocking phishing attacks and taking down fraudulent websites. In one month we took down more than 2,000 online scams related to coronavirus, including hundreds of fake online shops selling fraudulent coronavirus-related items.

We’ve also launched our pioneering Suspicious Email Reporting Service, the first of its kind anywhere in the world. This tool allows people to flag possible scams to our experts by forwarding suspect emails to report@phishing.gov.uk. In its first three days, the service received more than 12,000 reports from the public, which resulted in the removal...
Online criminals are always evolving their techniques

of more than 220 phishing campaigns. There is a plethora of advice and guidance for individuals and businesses on the NCSC website, including advice on working from home and using video conferencing apps. We’ve also recently published six actionable steps people can take to protect themselves from the vast majority of threats as part of our Cyber Aware campaign. The most important of these is to have a separate password for your email account, because that is the gateway to everything. Enable two-factor authentication to reduce the risk of attack, update your software and apps and back up important information that could be lost if your phone, tablet, or laptop gets hacked.

We’ve seen a recent resurgence in ransomware attacks on healthcare organisations around the world. What practical measures has the NCSC put in place to protect NHS trusts?

We’re fully focused on helping the UK’s health services defend themselves from cyber attacks, particularly during the unprecedented demand placed on them by the coronavirus outbreak.

We are working closely with the NHS to ensure online services can cope with demand, and prioritising any requests for support from health organisations. Our close contact with the sector means that we can inform them of any malicious activity and take the necessary steps to help them defend against it.

In light of the pandemic, what is the biggest cyber threat facing the UK today?

The overall levels of cyber crime have remained stable, but there is an increased proportion of that overall level which is related to the coronavirus outbreak. Online scams have moved away from the “traditional” tax rebate or unclaimed lottery win to selling fake PPE, providing fake cures, and looking to take advantage of emergency relief schemes. Online criminals are always evolving their techniques, and I’d encourage everyone to familiarise themselves with NCSC guidance to help keep them safe online.

This year the NCSC launched an annual diversity survey. Why is diversity in the cyber security sector critical to keeping the UK safe?

Talent from all backgrounds and perspectives is vital to the sustained innovation in cyber security. Digital skills are increasingly valuable, and these along with other skills (such as communications, engagement and critical thinking) are needed in order to stay ahead of the threat and help people stay safe online.

It is vital that cyber security is seen as a sector where people can join at all points in their career, from school and university right through to returning to work after a childcare break or changing track mid-career. Threats come from so many different sources and motivations, the ability to defeat them relies on “all ideas” coming to the table and “all voices” being heard.

Our annual diversity and inclusion survey with KPMG will help us understand the make-up of the current cyber security workforce. From this, we will then develop strategies that improve opportunities on offer to all.
It is well accepted that the UK, and indeed the world, is short of cyber security skills. This shortage applies to everyone, ranging from the everyday understanding and practice of cyber security by the general public through to the more sophisticated degree of cyber security awareness necessary for policymakers and business leaders. I hope the pandemic has reminded us that society cannot function without experts, and also that we are short of them.

This was recognised early by the UK government, which included among the many initiatives it launched off the back of the 2011 National Cyber Security Strategy, funding for two Centres for Doctoral Training (CDTs) in cyber security, one of which we have been hosting at Royal Holloway, University of London, since 2013. So what are CDTs, and how do they help to train new cyber security experts for the UK?

CDTs are four-year PhD programmes. Our CDT funds an annual cohort of around ten new starters. Royal Holloway’s CDT has thus far recruited seven cohorts, two of which have now graduated. That’s 20 new experts, 50 on the way, and we currently have funds to train another 40 over the next four years. Each cohort engages in a year of multidisciplinary training before each researcher selects an individual project topic, which they pursue in depth for the remaining three years. Each researcher is also expected to undertake an internship with one of our CDT partner organisations. There are four defining keywords worth expanding on.
There are three significant benefits of the CDTs’ cohort-based approach. Firstly, a PhD can be a long and lonely journey if studied in isolation. Pursuing a PhD within a cohort can be much more nurturing, with lifelong friendships likely to emerge. Secondly, developing a distinctive training programme for a cohort is more effective, and scalable, than bespoke individual training. And thirdly, and perhaps most importantly, a cohort brings together individuals with diverse backgrounds and life experience. We firmly believe that cohorts establish collectives of researchers who are much more creative than the sum of their parts. As an example, one team of four CDT researchers won the inaugural Cyber 9/12 UK security policy competition in 2018.

Our CDT training programme is inherently multidisciplinary. This recognises that cyber security is not solely an issue of technology. It also requires an understanding of how individuals, groups and society more broadly engage with digital technology. Our CDT recruits not just computer scientists, engineers and mathematicians, but also sociologists, psychologists, economists and geographers. The training programme exposes them to the likes of firewalls and encryption, but also to securitisation theory, geopolitics, and human and social factors. They attend taught courses on Royal Holloway’s pioneering Information Security masters programme, but also undertake group exercises such as critiquing national cyber security strategies, designing campus cyber security awareness campaigns and conducting boardroom simulation exercises. We want every cyber security expert we train, regardless of specialism, to appreciate the bigger cyber security picture, and how their expertise contributes to this picture.

Of course, a PhD is ultimately about research. Our CDT’s official title is the Engineering and Physical Sciences Research Council’s CDT in Cyber Security for the Everyday. That “everyday” is multifaceted. Firstly, the research addresses challenges concerning the technologies deployed in digital systems that people use, sometimes inadvertently, daily. Researchers in the CDT have been investigating security of software, data protection in cloud environments, existing security technologies and those that will become mainstream in the future, such as post-quantum cryptography. However, the research also addresses the everyday societal experience and practice of security. Our researchers have been investigating cyber security in the workplace, the privacy and security implications of health and transport apps, maritime cyber security, and the establishment of national data embassies.

Finally, the CDT is all about partnerships. One goal of our CDT is to embed all our CDT researchers within the wider cyber security community. This begins during the first-year training, especially through a series of events that we call Cyber Security in the Wild. Each of these involves an engagement with cyber security practitioners to explore both what their day job looks like, but also their own professional journeys. We do this through field trips to different types of cyber security organisation, as well as by welcoming visitors to our own campus. Our CDT partners also act as hosts for internships.

These have taken students all around the world to experience different cyber security cultures, including Amazon Web Services, HP Labs, Cabinet Office and Nato’s Shape (supreme headquarters allied powers Europe). We are always seeking new CDT partners, so please do get in touch if you would like to consider becoming involved in our training programme or hosting CDT researchers on internships.

Our first CDT cohorts are now fully fledged. CDT graduates have found employment as cyber security experts in a range of established security technology companies, government roles and start-ups, while a couple of others have continued in academia. Providing all the cyber security skills for the UK’s future needs will require many different interventions, at different levels. By training tomorrow’s cyber security leaders, we are confident that the Royal Holloway CDT is playing a very important part of delivering this.
How cyber criminals and nation-state actors are exploiting the Covid-19 crisis. By Oscar Williams

Prospering from a pandemic

In early April, British and American cyber officials took the rare step of issuing a joint security advisory. Such interventions are reserved for the most significant cyber incidents, from Russian hacking to major criminal campaigns. But this particular advisory was unlike those that preceded it. Rather than highlighting a specific software vulnerability or nation-state campaign, it covered a broad range of attacks that shared just one trait: coronavirus.

Attackers, security officials revealed, were seeking to exploit people’s fears of the pandemic for a variety of malicious purposes, including data theft, fraud and espionage. Although analysts working at the National Cyber Security Centre (NCSC), a division of GCHQ, noted that the total number of security attacks had not risen, they witnessed a sharp rise in the number of attacks using the outbreak as bait. In one week alone in March, 6,000 coronavirus-related domains were registered, with security experts warning that many of them were malicious.

It is perhaps no surprise that cyber criminals, characterised by cynical opportunism, would attempt to exploit a global health crisis. But it is not just fraudsters who are deploying such tactics. The NCSC’s advisory noted that “advanced persistent threat” actors (APTs) were also exploiting the pandemic to launch campaigns. APTs are better known outside of security circles as state-sponsored hackers.

“[APT and cyber criminal] activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised,” the NCSC stated. “Their goals and targets are consistent with long-standing priorities such as espionage and information operations.”

Speaking to Spotlight, Paul Chichester, the director of operations at NCSC, said: “We’ve seen that cyber criminals are changing tactics to take advantage of the pandemic and coronavirus is ideal bait to phish for sensitive information and infect devices with malware. This is a fast-moving situation and our priority, alongside international partners, is to ensure that the public and organisations can take action to protect themselves.”

In mid-April, an email with the subject line, “Covid-19: Emergency advice from the NHS”, was sent to 21,000 people in the UK. After opening the email, recipients were advised to click a link to see a list of up-to-date coronavirus cases in their area. The link opened a fake Microsoft Outlook page that invited people to resubmit their email address and password, which could subsequently be sold on through dark web forums.

“This particular campaign illustrates the tailoring of threat actors’ messaging to reflect what is happening in the media,” Carl Wearn, head of e-crime at Mimecast, which uncovered the campaign, told NS Tech at the time. “With the NHS currently working on a contact tracing app, this scam looks to take advantage of this by offering people the opportunity to see the number of coronavirus cases in their local area. This is obviously very tempting to people wanting to keep themselves as safe as possible.”

While hackers have targeted a range of businesses since the start of the outbreak,
Hospitals have faced a surge in ransomware attacks

arguably the most exposed organisations are those operating in the healthcare sector, and there have already been some high-profile targets.

On Sunday 15 March, as the size of the coronavirus crisis was becoming apparent in the United States, the US Health and Human Services Department (HHS) was hit by a distributed denial of service (DDoS) attack. The attack, which leveraged servers around the world, hit the department’s systems millions of times in an apparent effort to thwart the agency’s response to the outbreak. Speaking to Bloomberg anonymously at the time, an official said that a nation-state actor may have been responsible.

Since the coronavirus crisis began to unfold, security experts have warned that such provocations could be considered acts of war during a global pandemic. But the HHS is not the only organisation to have been hit. According to Reuters, hackers believed to be working for Iranian interests reportedly targeted the personal email accounts of officials working for the World Health Organisation in order to get information about the global spread of the virus.

Hostile nation states are not the only threat actors targeting healthcare organisations. Despite several high-profile ransomware groups having promised to avoid the sector, Interpol warned last month that hospitals around the world were facing a surge in ransomware attacks, with hackers calculating that organisations which might normally refuse to pay out would be more willing to do so.

Brno University Hospital, one of the Czech Republic’s major Covid-19 testing centres, was held to ransom over the course of a weekend in mid-March, prompting staff to relocate some patients as IT staff scrambled to get systems back online. While the NHS is considered to be relatively well prepared for ransomware strikes, having bolstered its defences in light of the 2017 WannaCry attack (See: Interview with Marcus Hutchins, p.18-20), other healthcare organisations around the world are less well prepared.

Nevertheless, while healthcare organisations are particularly exposed, the NCSC’s latest guidance suggests they are by no means alone in weathering a storm of Covid-19-themed attacks.

“As the Covid-19 outbreak continues to evolve, bad actors are using these difficult times to exploit and take advantage of the public and business,” said Bryan Ware, assistant director for cyber security at the US Cybersecurity and Infrastructure Agency, in the joint alert it issued with the NCSC in April.

“We urge everyone to remain vigilant to these threats, be on the lookout for suspicious emails and look to trusted sources for information and updates regarding Covid-19,” he continued. “We are all in this together and collectively we can help defend against these threats.”

The UK has been in a nationwide lockdown since 23 March, with most shops and services closed or severely limited
Staying safe in cyber space

Cyber attacks against Industrial Control Systems are rapidly increasing, and our response needs to adapt to keep up, says Dr Richard Smith, associate professor in cyber security and deputy director of the Cyber Technology Institute at De Montfort University.

The Cyber Technology Institute at De Montfort University (DMU), Leicester, is a recognised centre of excellence in cyber security research with strong industry links, and security for Industrial Control Systems as its flagship specialisation area.

The Industrial Control Systems security challenge
Industrial Control Systems (ICS) are ubiquitous to modern life yet they remain unknown to many who rely on them. These systems control our critical national infrastructure, such as electricity generation, chemical processing, water treatment and nuclear power, and the manufacturing systems of organisations everywhere.

These systems are often focused on creating a product, ranging from fully formed cars to individual units of electricity. To improve the efficiency of the process to create these products, more and more systems are becoming connected to the internet, either directly or through links within the organisation’s enterprise network.

ICS are, along with many Internet of Things devices, often referred to as cyber-physical systems. This means that cyber attacks no longer only impact the cyber domain but can have a physical impact in the real world, as evidenced by the Stuxnet and Triton attacks.

Unfortunately, many of these systems have been in place for many of years which, when coupled with regulatory or safety requirements of the systems themselves, means securing them presents a unique challenge at both a technical and human level.

Technical constraints
ICS previously relied on security through obscurity; with an extremely high entry barrier to understanding the systems and their protocols, the chances of a major cyber attack were low. In recent times, this barrier has come down significantly. Information on the protocols is widely available, services acting as “Google for ICS and IoT devices” allow for quick discovery, and past exploits are incorporated into open source penetration testing toolkits, making it easier than ever for malicious actors to attack a system.

Security vulnerabilities have been reported in control systems and there has been an observable increase in cyber threats in recent years. Unlike IT systems, where patches to mitigate vulnerabilities can be installed within short timescales, patching is often only possible by halting activity on operational devices and therefore is
further time-constrained in many cases. These changes to an ICS must also be rigorously tested before deployment to ensure the risk of unintended consequences is contained, as the impact can extend to physical damage, denial of national infrastructure, and environmental as well as financial loss. Changes also need to be certified with the relevant regulatory body, adding cost and often significant delays.

Human Factors
The challenge is not limited purely to the technical aspects of ICS. Often the people responsible for the security of these systems lack the resources required to keep them safe. Many IT cyber security professionals do not understand the requirements of ICS, where continuity of process is key. Even with everyone on board, the lack of a shared technical language can lead to confusion and delay, with team members talking at cross-purposes or unsure of what is being proposed.

How can DMU help?
DMU’s Cyber Technology Institute (CTI) provides world-leading research by delivering practical solutions for industrial issues to develop a smart, safe and secure cyberspace. This work has led to DMU being recognised as an Academic Centre of Excellence in Cyber Security Research by the National Cyber Security Centre (NCSC); one of only two Academic Centres of Excellence in Industrial Control System Cyber Security in Europe by Airbus; and being admitted to the Research Institute for Trustworthy InterConnected Cyber Physical Systems (RITICS), funded by NCSC and the Engineering and Physical Sciences Research Council (EPSRC). The CTI offers an MSc in cyber security closely aligned with our research, with its modules taught in blocks that are frequently taken by our industry partners as continuous professional development modules.

Industry requirements are at the centre of our cyber security research, which focuses on organisational relevance, supported through the centre’s exceptionally strong industrial advisory group consisting of Airbus, BT, Deloitte UK and Rolls-Royce.

One example is the Agile Incident Response 4 Industrial Control Systems, an NCSC/EPSRC-funded project. Rigid, procedural incident response processes are increasing the predictability of the defence efforts and make it more difficult to protect the remaining infrastructure and business functions in the context of fast-pivoting and multi-pronged cyber attacks. This is exacerbated when incident response crosses IT/operational technology (OT) boundaries and communication between stakeholders, often from different disciplines and organisational hierarchies, is frequently impeded and situational awareness is decreased.

Agile approaches, on the other hand, welcome changing requirements and are driven by value and the understanding of the system by a cross-functional team that can manage conflicting stakeholder requirements. This approach is therefore geared to environments where change is constant and the environment and objectives are not clearly identified or defined. This work is producing a framework that advocates the integration and evaluation of agile methods and practices, used in, eg SCRUM and KANBAN, to provide a security incident response team with the ability to respond quickly to changes while maintaining the focus on the business and its value-chains. By its very nature incident response needs to be adaptive to a highly dynamic nature of cyber attack and anticipate further exploitation paths of the adversary, and requires a cross-disciplinary team effort to respond more effectively.

To validate the framework, the team have run a series of cyber warfare training exercises involving a professional OT red team and a blue team of industry professionals from cyber security and from engineering, media and psychology. Utilising our new state-of-the-art Research Security Operations Centre, these live, real-time events have allowed us to tailor the tools and techniques to work with existing practices to increase team situational awareness and reduce response times. The framework is being developed in a modular fashion, allowing organisations to tailor their approach to meet their own needs and Agile maturity level.

For more information, please visit: www.dmu.ac.uk/research/centres-institutes/cti

Cyber attacks will have real-world impacts
Marcus Hutchins thwarted the 2017 cyber attack that hit the health service. He talks to Samir Jeraj about the latest emerging threats.

The man who stopped WannaCry

In August 2017, tired and in a haze from a week of parties at the annual Def-Con hacker conference, Marcus Hutchins was arrested at a Las Vegas airport. Only a few months earlier, the British cyber security researcher had been named as the hero who foiled a major ransomware attack. WannaCry infected 200,000 computer systems in more than 150 countries. Its most high-profile victim was the NHS. But in Vegas, the heroic story of the man who stopped WannaCry took an extraordinary turn.

“I was waiting for my flight home, someone in CBP [Customs and Border Protection] uniform approached me and asked my name,” Hutchins recounted in a documentary about his story released last year. “They led me to an interrogation room built into the airport – and it turned out that the guy was actually an FBI agent.”

Then 22, Hutchins was charged with developing and selling malicious code that was incorporated into malware between 2012 and 2015. According to a Sunday Times report in 2017, GCHQ knew that Hutchins would be arrested in the US. Although Hutchins had previously worked with the National Cyber Security Centre, part of GCHQ, it did not warn him.

During the ensuing two-year legal battle, Hutchins was unable to work or to leave the US, staying in Milwaukee and then Los Angeles. Eventually he agreed a plea deal that could have resulted in a ten-year prison sentence, but was released for time served with one year under supervision. At the sentencing the judge placed great emphasis on the work Hutchins had done since creating the malware for which he was arrested, particularly his role in combating WannaCry. In the past, Hutchins has spoken about being a “different person” when he was writing malware as a teenager.

Hutchins, 25, emerged from this cinematic series of events less than a year ago. He is used, he told me via Skype, “to this kind of life”. He is reticent to relive what happened; the attention that WannaCry brought still feels strange. “I really don’t think about it much. It seems like a Black Swan event… I think: that is a thing that happened and something like that may never happen again.”

Its most high-profile victim was the NHS
The 2017 attack affected computer systems in one in three NHS trusts and just under one in ten GP clinics. The disruption led to around 19,000 appointments being cancelled in one week, and a total cost of £92m. WannaCry tore through systems running Microsoft Windows, encrypting the contents and demanding payments in bitcoin to unlock them.

At the time, Hutchins was working out of a bedroom at his parents’ house in Devon for Kryptos Logic, a Los Angeles-based cyber security company. In the first few hours of the attack, he noticed that the malware’s code sent a signal to an unregistered website every time it infected a new system. He registered the site and the attacks slowed. Then they stopped.

Hutchins had discovered a “kill-switch”, possibly created so that the hackers could bring the attacks to an end if necessary, or just a flaw that was accidentally included in the code. The attackers were not looking to stop, however. They launched a “distributed denial-of-service” attack to try to crash the servers of the newly registered website, starting up the WannaCry attacks again. But they ultimately failed. Hutchins had protected the site by using the cache to handle the higher traffic rather than a live site, which would have been overwhelmed.

Hutchins is due to return to the UK this year, but, ultimately, he plans on finding a way to go back to the US. “I wish I could stay,” he says. “It was definitely a change for the better, despite the mess that brought me here.”

The cyber security researcher comes across as understated and methodical. He is impressively self-taught. He completed a computer course at school, but never went to university. On a gap year – brought about by “bad luck and bad decisions”, as he has written on his blog, Malware Tech – he further developed his skills. It was his blog, which is still active, that first brought him to the attention of firms looking for people with his particular skillset.

WannaCry, Hutchins said, did not really target the NHS: “It went after everything and it just kind of happened.” The way it attacked was unusual. “That was pretty much the first and last time we ever saw a ransomware worm,” he said. A worm is a form of malware that spreads copies of itself from computer to computer without needing to latch on to a piece of software. “If you had the capacity to make a worm, going for ransomware would probably not be your first call. It’s a very crude way to make money.”

The WannaCry attack crossed a line, he said, and is unlikely to inspire
No one looked at WannaCry and thought, ‘Hey, that’s a good idea, let’s simultaneously piss off every intelligence agency in the world.’” It was a state actor that did it [the UK and US governments have said that North Korea was responsible for the attack] and they still got found out, so I can’t imagine there are criminals out there thinking, ‘This is something we should do’... I think it was someone [who] found a nuclear weapon and decided they were going to rob the convenience store with it.”

The attacks have been attributed to hackers, backed by the North Korean state, who used cyber weapons stolen from the NSA by hackers believed to have connections to Russia. State-backed attacks are a core element of geopolitical power struggles and non-actor maneuvering. Hutchins describes such attacks as “essentially state-sponsored terrorism, but with cyber crime”.

Coronavirus has ushered in new threats. Virtual private networks (VPNs) have been hit in the past few months by more “opportunistic attackers going for whatever is available”, Hutchins said. “[This is] a big risk now because a lot of companies are usingVPNs to get people on to their networks from home.” The other kind of attackers are more targeted, using “very typical spam” such as “your payment has been denied”.

“The other kind of attackers are more targeted, using ‘very typical spam’ such as ‘your payment has been denied’.”

With “semi-targeted ransomware attacks”, hackers mass-infect systems, go through them and pick out businesses to hit – “high-profile targets who would pay more than your average ransomware victim,” Hutchins explained. “A lot of the big financial crime actors have pivoted to that instead of their normal bank fraud.” The targets of such attacks include “pretty much everything you wouldn’t want them to hit: police departments, hospitals, state governments. They’ve even hit a couple of utility providers,” he said. “They’re going after stuff that actually matters.”

How prepared is the average organisation or individual for emerging cyber threats? “Things have definitely got better recently with high-profile attacks making people realise they need to take security seriously, but I still think that everyone is hugely underprepared.”
Beyond passwords: the future of web authentication

The University of Surrey’s Mark Manulis, Helen Treharne and Chris Newton, and Matthew Casey from Pervasive Intelligence, discuss the new mechanisms being developed for keeping data secure.

What are the main issues with password insecurity?
Much has been said about password insecurity. Users are known for making poor password choices, with passwords often being written down, reused across multiple websites, or revealed through phishing attacks. Deployed policies requiring users to frequently change and memorise new passwords are unusable and magnify the problem. The need to adhere to legacy systems in password management and provide for alternative reset mechanisms introduce further risks and high costs. The UK’s NCSC has issued numerous guidelines on how to improve password authentication. But in the coming years passwords will no longer be used as a main authentication factor. This is foreseeable, given new regulations such as the revised EU Directive on Payment Services (PSD2) on stronger customer authentication and recommendations by the World Economic Forum on adopting passwordless authentication.

What does the future of authentication look like?
The need to strengthen user authentication has already been recognised and many competing solutions are currently being deployed. Collectively known as 2FA/MFA, they still widely rely on passwords, strengthened by additional measures such as one-time passcodes. There are less secure solutions with short time-limited codes sent through out-of-band channels, eg email or SMS, and solutions requiring additional software/hardware authenticators on the user side to locally generate and verify the codes. They must be securely configured for each web service and cannot be reused, limiting portability and requiring complicated, often manual reset mechanisms. As with passwords, using passcodes bears the risks of guessing and phishing attacks.

The game changer is the open FIDO Alliance specifications for completely passwordless user authentication. On track to become a new standard, WebAuthn, developed by the W3C Web Authentication Group, relies on public-key cryptography to improve the security and privacy of web users. While commodity smartphones and various USB/NFC/Bluetooth tokens will serve as WebAuthn authenticators, there are still usability limitations with regards to their portability, back-up and reset mechanisms.

How is the University of Surrey involved in shaping that future?
The Surrey Centre for Cyber Security (SCCS) is working with leading WebAuthn industries on back-up/recovery mechanisms for future web authenticators and is also exploring new cloud-based architectures with hardware-based roots of trust to support delegation of WebAuthn credentials. SCCS has experience in the design and analysis of (multi-factor) authentication and identity management protocols, grounded in modern cryptography and formal protocol analysis. In our recent projects we developed privacy-preserving authentication and attestation protocols for users and machine-to-machine communications, with applications for future transport and rail systems. SCCS is also working on authentication protocols for distributed systems involving IoT and blockchain technologies.

For more information, please visit: www.surrey.ac.uk/surrey-centre-cyber-security
The coronavirus outbreak has forced many of us to adopt new ways of communicating, both at work and in our personal lives. Technology can help us with this. But, as many people have found out the hard way, the platforms that allow us to connect with one another are not always secure. Unwanted participants can join and record conference calls. Data could be stored inappropriately. And cyber criminals are always looking for new vulnerabilities they can exploit to steal or extort.

The NHS faces unique cyber security challenges at the best of times. There are more than 200 trusts in England alone, each with computer networks that need to be protected, while NHS England’s core infrastructure connects 28,000 healthcare systems across 21,000 organisations. Coronavirus has meant many frontline staff are currently working in new roles in hospitals, using unfamiliar systems. Elsewhere, GPs are being asked to provide care remotely wherever possible, so that patients don’t need to visit surgeries.

To provide the best possible care, health professionals need to access and share sensitive data about patients – but they also need to ensure that this data is protected appropriately. There are new tools available that do this; NHS Digital has recently confirmed that the Hospify app meets its standards. This makes it the first messaging app certified for use by both patients and professionals. Staff previously communicated via personal, insecure apps.

The WannaCry cyber attack in 2017 forced the NHS to cancel more than 19,000 appointments and divert ambulances away from five hospitals. Nevertheless, when the Public Accounts Committee reviewed the response to the attack, we concluded that the NHS had got off lightly. The attack had been

Coronavirus must be the health service’s top priority, but its response should not leave it open to cyber attacks, says Meg Hillier MP, chair of the Public Accounts Committee
How to keep the NHS cyber secure

Personal devices can compromise security

relatively unsophisticated, and was not specifically targeted at the NHS. It also took place on a Friday, which meant that services that don’t operate at the weekend were less affected than they could have been. And a cyber security researcher found a “kill-switch” to stop the virus spreading later that same day. (See interview with Marcus Hutchins on p.18-20)

The potential harm that a comparable attack could cause right now does not bear thinking about. We told the government then that it needed to urgently put in place plans to implement the lessons learned from WannaCry, since cyber security is essential for patient safety. While some such changes have been made, work on others is still ongoing. Responding to Covid-19 must be the NHS’s top priority, but it is important that cyber security is not overlooked, and that the response to coronavirus does not leave the health service open to cyber attacks.

There are other lessons learned from WannaCry that are particularly relevant across the public and private sectors at the moment. For instance, NHS trusts could have protected themselves against the attack if they had applied the latest security patches and maintained strong firewalls. Many employers are currently rolling out new remote working tools to allow their staff to connect to corporate networks from home, or are making much greater use of existing tools. Some versions of these tools are known to have vulnerabilities. If not fixed, these can leave an organisation open to attack, just as a failure to patch systems left some NHS trusts vulnerable to WannaCry.

Employers need to make sure that they do not overlook security in their haste to get staff back online. They also need to recognise that products originally designed for personal use may not offer the security protections that corporate users require. In many cases, products that were designed to be secure from the outset will be more appropriate.

The British economy is highly dependent on the internet. However the Public Accounts Committee last year warned that the government has not done enough to enhance cyber security across the economy. We have also been concerned for some time that British citizens do not have the cyber security awareness they need. In 2017, we reported that British workers are less confident in their ability to protect data and devices than their counterparts in Brazil, South Africa and China.

More recently, a government survey found that almost a third of people don’t feel they know how to protect themselves online. It is essential that everyone is able to take care of themselves online. Cyber criminals will exploit any gaps they can identify. They have been quick to take advantage of the coronavirus epidemic, adapting existing scams designed to steal money and collect sensitive personal information.

It is also clear that the country does not have enough cyber security specialists. We raised this first when we examined how government protects its own information, then when we evaluated how successful the first National Cyber Security Strategy had been, and again when we investigated the response to the WannaCry attack. Yet such skills gaps persist; government research indicates that 48 per cent of businesses do not have enough people with the skills to carry out basic cyber security tasks such as setting up firewalls. Firms, including specialist cyber firms, also face a shortage of people with more advanced skills.

The government told us in 2019 that it would be some time before it could evaluate whether its efforts to increase the number of people with cyber skills were working. It is vitally important that these efforts do succeed. The unprecedented disruption to our way of life in recent weeks shows just how important it is to have people who can respond with speed and flexibility to meet unforeseen challenges.

It seems inevitable that the coronavirus pandemic will normalise remote working. High-level and personal cyber security must be at the heart of this new normal.
Is the global pandemic forcing firms to become more cyber aware? By Rohan Banerjee

How to work from home safely during a crisis

The coronavirus pandemic has catalysed a global home-working experiment. With social distancing measures in place worldwide, the traditional office nine to five has for many been replaced by emails, video conferencing, and remote access to shared computer servers. While there are some positive aspects to the new status quo – does anyone really miss the morning commute? – moving out of the office has placed organisations at greater cyber risk.

In the dim, distant past of water coolers and office banter, some members of staff may have viewed cyber security as the remit of their colleagues in IT, but working in quarantine demands more individual awareness. “Extra vigilance is required, especially regarding what you are clicking,” says Adenike Cosgrove, international strategist at Proofpoint, a cyber security services firm. “Remote working often means you aren’t protected by the same safeguards your office has in place… and the risk of email fraud naturally becomes greater. For example, it becomes more difficult to verify whether the person behind the email is actually who they say they are; you can’t just head over to their desk to check.”

The technological expertise of hackers should be seen as secondary to human error. “The person at the screen or keyboard is always the weakest point in a system,” Aaron Mauro, assistant professor of digital media at Brock University in Ontario, Canada, wrote in The Conversation last month. “Attackers will use a set of techniques...to trick us into divulging sensitive information.”

Indeed, Proofpoint’s most recent annual Human Factor report, published last September, found that 99 per cent of cyber attacks require some level of human interaction, such as following a hyperlink, entering password credentials, or downloading an email attachment. Hackers tend not to target executive or management-level employees, but rather those in more junior positions, the report said.

The threat of phishing – fraudulent emails that involve some kind of impersonation or misdirection to convince the recipient to do something...
How to work from home safely during a crisis

Covid-19 is amplifying people’s anxieties – has increased alongside the spread of Covid-19. Chaminda Thushara Hewage of Cardiff Metropolitan University’s computer science department, explains that while the “format of phishing is largely the same”, the context of coronavirus and people’s more susceptible emotional states because of it, are being exploited.

“There is a lot of panic due to Covid-19… and people are anxious about what is happening. The World Health Organisation has referred to this [situation] as an ‘infodemic’. This means people are searching for health information online. Many attackers, therefore, are creating phishing campaigns to pretend that they are providing health guidelines or services relating to the virus,” he explains.

Action Fraud, the UK’s reporting centre for fraud and cyber crime, found that over £2m had been lost to scams using coronavirus as a pretext in this country since the first quarter of 2020. And in a recent survey of UK businesses by Gauntlet Risk Management, more than a third of respondents admitted to not knowing what phishing was.

What lessons can companies learn from the sudden shift to home working? How will the world of work adapt to cope with similar situations in the future? Business strategies need to strike a balance between technical provision and human resources. Norton, which produces a popular anti-virus software, has published guidelines urging good cyber hygiene. These include strong and regularly changed passwords, timely software updates, a clear distinction between personal and work-related devices, and secure virtual private network (VPN) arrangements.

A VPN is a piece of software that creates a secure link between a person’s internet access, whether using a public or private connection, and that of their organisation. In other words, it is like a passageway, protected by encryption, that only someone with specifically granted access can use. Access is usually granted by a two-step verification process. This could involve a password and a code texted to someone’s mobile phone.

But while VPNs are widely recommended in the cyber security industry, they still come with caveats. For one thing, as Phil Chapman, a cyber security instructor at Firebrand Training told Computer Weekly in a recent interview, they rely on the security of the originating network. If that is questionable, then there is cause for concern. Chapman advised companies to urge staff against using their home Wi-Fi, but to connect their computer to the router with an ethernet cable instead for added security.

Johannes Ulrich, fellow and dean of research at the Sans Institute, says that using devices exclusively for...
work is a good habit to get into when not in the office. In their haste to get people working from home during the pandemic, Ulrich says, many companies have taken costly “shortcuts”, with some allowing employees to use shared home computers, rather than supplying them with company kit. “Using the same computer for confidential company data that the kids use for online gaming can expose that data to malicious content introduced by other users,” he explains.

Home assistant devices such as Alexa or Siri are a risk factor that many companies are currently overlooking, Ulrich adds. “They may pick up phone calls or video conference discussions and exfiltrate them,” so people should be mindful about having them in the room that they are working in.

The video calling platform Zoom saw its user base grow by 67 per cent in the first quarter of 2020. At the time of writing, it had been downloaded more than 50 million times on Google Play Store. The software, which allows anyone to join a call by clicking a weblink, has helped to substitute for office meetings. As convenient as this is, the platform does present vulnerabilities. Its open nature has given rise to the trend of “Zoom-bombing” – where people who are not meant to be on a call somehow manage to access the link.

The firm’s CEO Eric Yuan has confirmed Zoom is working on a newer version of its software with stronger encryption technology built in. This is due to be launched in May. In the meantime, users can take steps to guard against breaches, including using the right settings and following good cyber hygiene. According to guidelines published by PC Mag, users should avoid sharing their link or meeting ID on other platforms, such as social media or public forums. As well as setting a meeting password, users should set screen sharing to “host only” where possible.

As for the human side of cyber security, communication is key. Without being able to wander over to someone’s desk to check something, in instances of doubt, a simple query can go a long way. Did you send that? Can you confirm X or Y? Norton’s guidelines suggest that a phone call to clarify something in an email is a low-tech solution to what could potentially be a huge problem.

The coronavirus crisis, Adenike Cosgrove hopes, will be the impetus that companies need to start viewing cyber security as an “ongoing” risk, affected by “new realities that are reshaping the workforce”. Occasional phishing tests and training “once or twice a year” are “simply not enough”. Awareness “throughout” organisations will dictate whether or not they are equipped to cope. If working from home is to be the new normal, Cosgrove says, then employees should be guided on how to do so safely. The basic principles of cyber security – user vigilance, timely updates of hardware and software, and regularly changing passwords – have not changed. But Covid-19 has certainly underscored their importance.
The worries of working remotely

UK-based firms have a long way to go when it comes to safe cyber hygiene, two recent surveys indicate.

- **77%**
  More than three-quarters of UK businesses have suggested that they are “unconcerned” by the threat of a cyber attack.

- **14%**
  More than a tenth of firms’ employees admit to having access to sensitive company data without their employer having carried out any checks on the cyber security of their device.

- **80%**
  Four in five firms have admitted to not having any detailed cyber security policy in place.

- **10%**
  One in ten UK employees say their company’s wi-fi password was common knowledge and readily shared, prior to social distancing measures.

- **33%**
  More than a third of UK employees say they do not know what phishing is.

A cross the world, Covid-19 is accelerating the pace of technological change. We are using technologies to adapt to the world in ways many thought unimaginable just a few months ago. Previously niche ideas, such as virtual classrooms and GP surgeries, have now become the mainstream. Last year, just 5.1 per cent of people worked from home. Now most of us are doing it. And did anyone predict the establishment of a virtual parliament in 2020?

For as long as I can remember, I have advocated for the technological transformation of our private and public sectors. Britain has suffered a productivity problem for more than a decade: high employment rates and high number of working hours, but stagnant output and pay. The solution to wealth creation and wage growth, in my view, is the rapid technological transformation of how we do business. In the public sector, too, with increasing demand and increasing costs, the route to improved service delivery and better cost efficiencies lies in the digitisation and personalisation of how services are delivered to service users.

We have started to see some of those benefits during the coronavirus lockdown. For workers without the dreaded commute, the start of the day is a more positive experience, no doubt helping increase the quality and speed of output. GPs are able to reach more patients per day using online or telephone appointments than at the local surgery. Replacing international travel with video conferencing brings savings to our carbon output and travel budgets.

These things are never perfect, however, which is why the state has an important role to play. Whether it’s the inequality that comes from lower-income families or rural communities not having adequate online access, or ill health not getting picked up by GPs due to a lack of patients self-referring. For workers who are unable to work from home, and for those of us concerned about the accumulation of wealth and power at the top of the technology market, it is vital...
that the state understands the gaps and fills them with the public policy measures that deliver the values-based outcomes the British people expect.

But what is “the state”? Yes, central and local government plays a crucial role in delivery. But parliament, the courts and civil society have a crucial role to play too. It is important not just to recognise the limitations of executive power in delivering everything that we want, but also to recognise the constitutional importance of institutional oversight, debate and accountability, which secures the best possible outcomes.

During this pandemic, it has been great to see technology adoption increase so quickly. But with parliament not at full speed (albeit in digital hybrid), our courts in a jam and civil society facing new challenges in adverse circumstances, it’s all too easy for new technology-enabled ways of working to become mainstream without proper thought.

Let’s take two examples: Covid-19 tracing apps, and the use of facial recognition technologies. At the Institute of AI – a global, not-for-profit network for legislators interested in the regulation of artificial intelligence, which I chair – we have been tracking how different countries have approached the use of tracing apps. In China, Alipay and WeChat have been integrated into the government’s tracing app, giving access to contacts, financial transaction data and device location. Access to certain areas is only permitted with the immunity passport provided by the state. In South Korea, Singapore and Hong Kong, age, gender, location and financial data is tracked by the minute using emergency legislation implemented during previous pandemics. We cannot simply copy-and-paste this approach in Europe.

That is why we are looking at this issue on the Science and Technology Select Committee. The development, roll-out and retirement of these apps must take place within an appropriate legal and ethical framework. For this technology to work for us, appropriate checkpoints and sunset clauses are needed to prevent wider-spread use in the future.

In facial recognition technology – a tool that can, in theory, increase the efficiency and effectiveness of policing by scanning large crowds and matching individuals with target lists held by the police – the role of the wider state is vital once again.

Yes, the technology is remarkable and developing at a significant pace. But some of the images held by the police are stored unlawfully, according to a 2012 High Court ruling, due to the Home Office’s technical inability to delete the images of unconvicted citizens automatically. While new technologies develop at speed, old technology – in this instance legacy servers – cause wider policy problems. One solution, to build new facial image databases by scraping social media images, is clearly not a solution acceptable to the public or to parliament. These issues, as well as the equality issues that arise from discriminatory training data-sets due to higher arrest rates amongst the black, Asian and minority ethnic community, require an active state and benefit from an empowered civil society.

However, it is unsustainable to rely on parliament or the courts to set and enforce these rules alone. While technology moves fast, primary legislation does not. That is why regulators are crucial in updating the rules and avoiding an overloaded court system. But forensics and biometric data regulators are not, in my view, given sufficient powers or resources to do their increasingly important work properly.

And that is why, in my private member’s bill on forensics and biometrics, I am calling on the government to strengthen the regulation of these policy areas.

These challenges are not just related to the pandemic, and it is positive that we are seeing citizens, businesses and organisations embrace the benefits of technology. But in moving fast, we must remember that we do not want to break things on the way. All of us, whether we are in government, the courts, regulatory bodies or civil society, have a role to play.
Over the past decade, the discussion of cyber security and privacy protection has moved from technical papers to the front pages as more people ask how to keep networks secure. This is hardly surprising. Cloud computing, big data, 5G, the Internet of Things, and artificial intelligence have created more complex, open systems that use more diverse technology. Innovation is redefining traditional network boundaries, dissolving the borders between the digital and physical worlds. New services are being rolled out quickly. And geopolitical tensions have made the debate fractious.

The challenge is immense but not insurmountable. The basic principles of cyber security have not changed. Transparency and common international standards can facilitate verification. A sense of shared responsibility can mobilise the action we need.

These are the firm beliefs of Huawei, which has worked closely with our telecoms network customers for more than 30 years to build over 1,500 networks in more than 170 countries and regions. Together, we have connected more than three billion people worldwide, and maintained a strong track record in security and reliability throughout.

Huawei is a private company owned by its employees. This has given our people a stronger stake in our success and supported our global growth. It is also why our founder, Ren Zhengfei, has said he would never agree to a request from the Chinese or any other government to provide access to our technology or network data. He would rather sell the company or shut it down, than breach customer trust and destroy the enterprise he and other employees have spent the past three decades building.

As the world goes digital at a faster rate, we have made cyber security and privacy protection a crucial part of Huawei’s strategy. We are committed to improving our software engineering capabilities and business continuity management systems, while enhancing the resilience of networks. We are establishing an end-to-end cyber security assurance system across the business. And we are committed to openness and transparency so our performance can be verified.

Our commitment is to do everything in our power to help our customers build resilient networks. As a provider of smart devices, we embed privacy protection into the entire product lifecycle, giving consumers full transparency and control. Beyond our own business we champion the development of shared standards and independent, objective verification mechanisms so that customers can choose products with the confidence that they meet the right standard.

No company is an island. In the digital age the challenges we face are universal. The demand for trustworthy digital infrastructure keeps growing as the cloud, digitisation and software become the norm. Huawei shares the same objectives as all telecoms operators and governments, namely secure, stable and resilient networks. We must work together to build them.

For more information, please visit:
www.huawei.com/uk
A crucial element of the UK’s fledgeling lockdown-easing plan is a digital contact-tracing app developed by NHSX, the innovation arm of the health service. It will be ready to launch in a matter of weeks, and will reportedly be used in combination with manual contact tracing and increased testing to help prevent a second spike in Covid-19. The app will work by pinging – via Bluetooth – other phones in the near vicinity, and storing a record of who we’ve been in close contact with over an epidemiologically relevant time frame.

Contact tracing, the key to easing lockdown, comes with a cyber security price tag, says Laurie Clarke

If someone receives a coronavirus diagnosis, everyone who was within their infection range will be notified of the need to self-isolate. But what sounds fairly intuitive has opened up a deeply divisive debate over the best way to design such an app.

An argument that has recently been raging in Europe is whether centralised or decentralised apps are preferable when it comes to privacy. The former means that in the event that the user alerts the app of a positive coronavirus test result, data is sent from the phone of the app user to a centralised database (run by a nation’s health service or government). The central database would then unlock the pseudonymised identities of the infected person and everyone with whom they had been in contact. In a decentralised model, the data is processed on the phone; the government never receives identifying information about app users.

Privacy and security experts have strongly rejected centralised apps, claiming that they are ripe for function creep and could be co-opted for mass or targeted surveillance purposes. A group of more than 300 academics signed a letter arguing this in April. In Europe, Germany flipped from a centralised to decentralised app. Other countries including Switzerland, Austria, Finland and the Czech Republic have also stumped for decentralised versions. France and the UK are still gunning for a centralised approach.

Meanwhile Apple and Google are developing their own decentralised system that will run in the background of their handsets. Together, the two companies control the operating systems of the vast majority of phones in the world. Both have said that they will not allow centralised contact-tracing apps to run in the background on their handsets, due to the greater number of privacy issues associated with this type of app. It’s partly for this reason that Germany decided to switch to a decentralised design.

If developers can’t find a way around for this issue, people would need to keep their phones constantly unlocked in their pockets in order for the app to run continuously. This would not only rapidly drain the battery, but would also leave all of the data on the phone insecure if the handset was stolen. Australia – which opted for a centralised approach – said it had found a solution, but officials have since admitted that problems have arisen. The UK also claims to have found a successful workaround, but since the source code is not yet published, it’s unclear what this “hack” is, and how effective it will be.
Read more in-depth interviews and features and download full policy reports at: newstatesman.com/spotlight