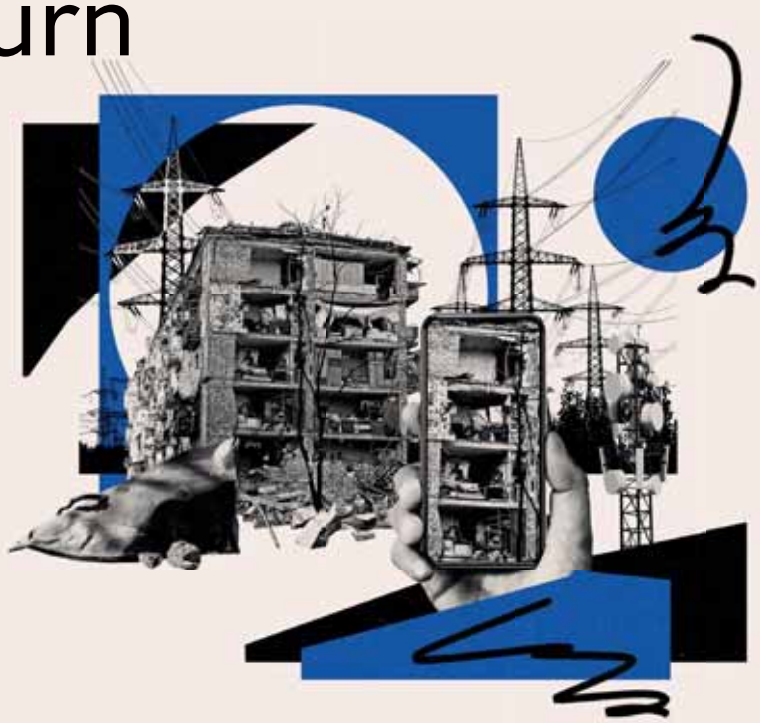
THE NEW STATESMAN

Spotlight

Thought leadership and policy

Cyber Security: The global threat landscape

Angela Eagle MP
Paul Maddinson
Simon Hepburn



Fortinet Security Fabric

Broad

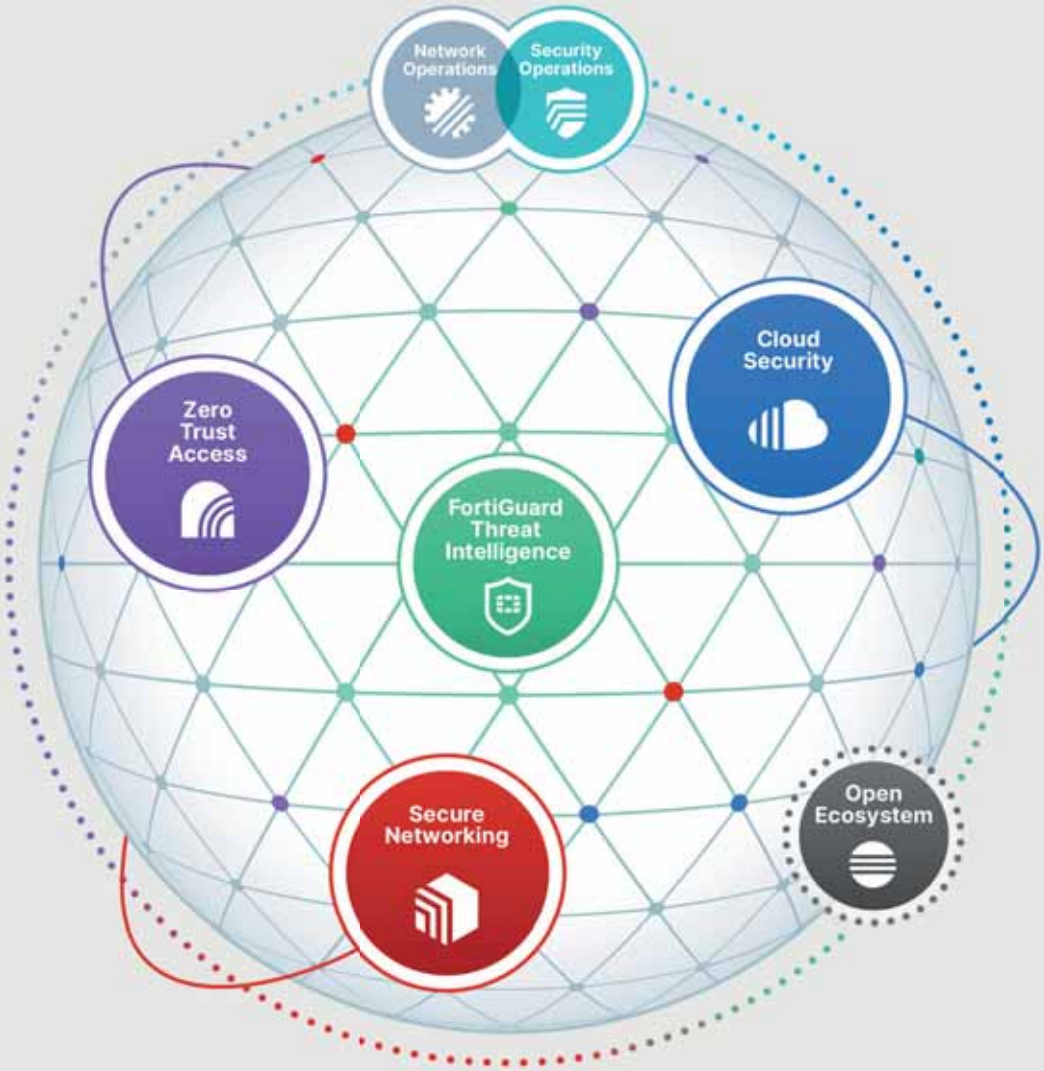
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



FORTINET

www.fortinet.com

A new era of hybrid war

Russia remains "the most acute threat to our security," the government stated in its Integrated Review of Security, Defence, Development and Foreign Policy, published last year.

And yet, back then few would have predicted Russia's invasion of Ukraine, which less than a year later has sparked long weeks of bloody warfare.

In advance of the invasion, experts expected the Kremlin to make more use of the cyber sphere in its "special military operation". While there were significant cyber attacks ahead of the conflict and as it began, the offensive quickly turned "into a military invasion and an attempt to seize territory and ground in Ukraine", as the National Cyber Security Centre's director of national resilience and strategy, Paul Maddinson, tells *Spotlight* (see pages 6-7).

A core thrust of the Integrated Review was that, to remain competitive, "Global Britain" must maintain its strategic advantage "through science and technology" and being a "responsible, democratic cyber power".

In the Ministry of Defence's similarly obtusely named Integrated Operating Concept 2025, also published last year, Chief of the Defence Staff Nick Carter hailed a "significant shift in military philosophy". This new approach, echoed in the Integrated Review, would equip the UK to counter threats in the "grey zone" between conflict and peace.

In this murky no-man's land, disinformation and cyber attacks are weaponised to undermine liberal democracies, as Carter said in an interview last year. The result, he observed, is that "our opponents will have found a way to unravel our democracy from inside...and we won't have noticed it."

Given this new philosophy, the reality of the Ukraine war has been illuminating. As Jonny Ball and Zoë Grünewald note (see pages 8-12), cyber threats have played a part in this war, but they have not replaced older military traditions.

At the time of going to press, the conflict has continued in the vein of past wars, with bombs and bullets more of a focus than online attacks. This is a reminder that, while security strategies must embrace the shiny tech of tomorrow, they must not be complacent about yesterday's threats. ●

Contents

Spotlight

40-42 Hatton Garden
London
EC1N 8EB

THE NEW STATESMAN
Subscription inquiries:
digital.subscriptions@newstatesman.co.uk

Director of Client Solutions
Dominic Rae

Account Managers
Katy Pieris
Jugal Lalsodagar

Special Projects Editors
Alona Ferber
Oscar Williams

Deputy Head of Production
Tony Rock

Design/Production
Rebecca Cunningham

Special Projects Writers
Jonny Ball
Harry Clarke-Ezzidio
Sarah Dawood
Zoë Grünewald
Samir Jeraj

Cover Illustration
Klawe Rzeczy

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017 WINNER

First published as a supplement to the New Statesman of 29 April 2022.

Registered as a newspaper in the UK and US.
The paper in this magazine is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.

Spotlight is the official media partner of CyberUK.

This supplement can be downloaded from: newstatesman.com/spotlight/reports

Pegasus malware hits Downing Street and Foreign Office

Back in mid-April, the Prime Minister was informed that both No 10 and the Foreign Commonwealth and Development Office (FCDO) had been targeted by the hacking software Pegasus – a piece of spyware that can turn a phone into a remote listening device.

Pegasus is developed and licensed to governments around the world by the Israeli firm NSO Group. It infects mobiles with malicious software that can control phones, carry out surveillance and extract data.

Citizen Lab, a research group based at the University of Toronto, recently released a report that said the UAE had potentially orchestrated a number of spyware attacks on the Prime Minister's Downing Street office in 2020 and 2021, and the suspected infections relating to the FCDO were linked with Pegasus operators in the UAE, India, Cyprus and Jordan.

The report suggested that these attacks could have been orchestrated by staff serving abroad and using international sim cards, though NSO Group denies this.

In November 2021, the Biden administration placed NSO Group on a blacklist, after allegations that the company had sold its spyware to governments that were using it for "transnational repression".

NSO Group has denied the allegations, and maintained that it only sells to governments for legitimate law enforcement and intelligence purposes.

A spokesperson for NSO Group said: "NSO continues to be targeted by a number of politically motivated advocacy organisations like Citizen Lab and Amnesty to produce inaccurate and unsubstantiated reports based on vague and incomplete information.

"We have repeatedly co-operated with governmental investigations, where credible allegations [have] merit."

ADAM BERRY / GETTY IMAGES

Russia is the most hacked country in the world

Russia received the most cyber security breaches globally in the first quarter of 2022, affecting 3.5 million people, virtual private network (VPN) provider Surfshark has revealed.

Cyber attacks, linked to the hactivist group Anonymous, have been on the rise in Russia following the invasion of Ukraine. The group has claimed responsibility for attacks on Russian TV networks, websites and government datasets.

The US is the second-most attacked country, followed by Poland, France and India. The UK comes in at 11th place with nearly 296,000 data breach victims.

The data shows that 18 million email accounts were breached globally between January and March 2022, a 58 per cent drop on the last quarter of 2021.

The 2022 Cyber Security Breaches Survey from the Department for Digital, Culture, Media and Sport (DCMS) also reveals that two in five UK businesses reported cyber attacks or breaches in the past year, and a third of these are hit with one every week.

Phishing is the most common threat, experienced by four in five of these businesses, while one in five identified a more sophisticated attack such as malware or ransomware.

The average cost to an organisation of an attack resulting in data or money loss is £4,200, which rises to £19,400 for medium and large businesses.

NSA chief to address CyberUK conference

Experts from across the cyber security industry are set to meet in Newport, Wales, on 10-11 May for the National Cyber Security Centre's (NCSC) annual event for the sector.

The theme of the CyberUK conference is a "whole-of-society approach to cyber security", building on the publication of the government's National Cyber Strategy earlier this year. The event will also look at the challenges and developments in ransomware, future technologies, defending the UK at scale and building a diverse workforce.

Over 1,500 attendees are expected to attend in person to hear speakers including Rob Joyce, director of cyber security at the US National Security Agency (NSA); Jen Easterly, director of the US Cybersecurity & Infrastructure Security Agency (CISA); and Jeremy Fleming, director of GCHQ. The event will also hear from Lindy Cameron, CEO of the NCSC.

Cameron said: "Our programme offers something for everyone in the cyber security community – from hearing about how other organisations dealt with incidents to the latest international perspectives on future technologies."

Spotlight is the official media partner for CyberUK. Visit cyberuk.uk

US government confirms infiltration of energy infrastructure

A joint statement by several US government agencies has confirmed the discovery of malware tools intended to disrupt and shut down industrial systems, including liquefied natural gas infrastructure and electricity grids in the country.

Although the government agencies did not name likely culprits or give specific details, cyber security specialists from the private sector have speculated that a state actor was almost certainly responsible, and said that there were similarities between this malware and other cyber attacks launched by Russian government-affiliated groups against physical and critical national infrastructure.

Malware traced back to hackers linked with Russian military intelligence has previously successfully attacked the Ukrainian energy grid and Saudi oil refineries.

The US government and its "Five Eyes" intelligence-sharing allies – including the UK, Canada, Australia and New Zealand – have warned that Russian state actors and pro-Russian cybercriminals are likely to step up attacks against countries that have imposed sanctions on the Kremlin and provided Kyiv with military aid.

£19,400

Average cost of a cyber attack to medium and large businesses that experienced loss of money or data

39%

Four in ten businesses have reported a cyber breach or attack in the last 12 months

83%

Of businesses that did experience cyber breaches, four in five reported phishing attacks

DAVID A LITMAN / SHUTTERSTOCK. SOURCE: DCMS

The view from the front line

"We need to raise the UK's resilience"

Paul Maddinson of the National Cyber Security Centre says the war in Ukraine has redrawn the threat landscape

By Oscar Williams

On 28 January, nearly a month before the invasion of Ukraine, British security officials issued a threat warning to UK organisations. In the advisory, published on the website of the UK government's National Cyber Security Centre (NCSC), the officials said they had observed cyber activity in and around Ukraine that "fits with [a] pattern of Russian behaviour".

In modern warfare, hostile cyber activity is often a precursor to military conflict. The war in Ukraine is no exception. In the days leading up to the invasion, the Kremlin launched a series of distributed denial of service (DDoS) attacks on Ukrainian institutions, while also deploying sophisticated "wiper" malware that targeted government systems, destroying files and software as it spread.

The NCSC's officials had anticipated the risk. "We identified the possibility of conflict and therefore an increasing cyber threat before the end of last year," says Paul Maddinson, the agency's director of national resilience and strategy. "We've taken some time to try and explain quite carefully what we mean by that increased threat."

A career civil servant who has worked for the NCSC since its formation, Maddinson says that despite the organisation's best efforts, the threat has been "portrayed in extremes" in the media. "It's either 'There's going to be a cyber Armageddon tomorrow', or, 'Actually, there's been no cyber incidents or attacks at all'."

The reality, says Maddinson, is somewhere in between. There have been "quite a lot of cyber attacks against Ukraine and Ukrainian infrastructure", he says. "And some of those have been [at a] low level of sophistication, like DDoS, but some of them have been quite sophisticated, like the wiper malware and the attack on the satellite provider."

The Viasat broadband satellite network was hacked on the day of the invasion. It is widely regarded as the most significant cyber attack of the early part of the conflict. Although the UK was not affected, it disrupted broadband connections around Europe. The incident validated NCSC's warnings of the risk of "spillover attacks" that would spread beyond their targets and ensnare Western organisations.

Nevertheless, Ukrainian government infrastructure is generally believed to

Ransomware is an enduring threat because it's a successful model, says Maddinson

have held up well during the war. The NCSC and other Western security agencies have provided cyber support to Kyiv. Maddinson says that while "it's really important to know that we don't have particularly good insights necessarily into what's going on in Ukraine", the country has made a "fantastic effort, as they have in other fields, to defend themselves against this aggression".

Once the invasion was under way, Russia's focus largely shifted from cyber to conventional warfare. "It clearly turned very quickly into a military invasion and an attempt to seize territory and ground in Ukraine," says Maddinson. "The cyber incidents have been in support of that strategic objective. So I think that would explain why you saw quite a lot of significant activity [from Russia] ahead of the invasion and during the invasion."

While cyber activity has played a smaller role in the conflict than some expected, the Kremlin has sought to carry out further disruptive attacks as the war has gone on.

On 12 April, a spokesperson for the Ukrainian government revealed officials had foiled an attack on the energy grid that could have plunged two million people into darkness. "It looks like we have been extremely lucky to respond to this in a timely manner," said Viktor Zhora, deputy chairman of Ukraine's State Service of Special Communications.

As the conflict has progressed, so too has the risk to Western organisations. Maddinson says the increased cyber threat to the UK and its allies is now "less to do with the military conflict on the ground" and the risk of spill over attacks and "more to do with the geopolitical tensions with Russia, whether they escalate and whether Russia decides to take measures against us". At present, Maddinson adds, it remains a "low likelihood", but he "wants organisations to be prepared".

However, the primary threat to British organisations from Russia remains organised cybercrime. After an attack on a major US oil pipeline last year, leading Russian ransomware operators announced they were retreating from dark web forums. Some security experts speculated that the statements may have followed an intervention by the Kremlin, but they appear to have been purely symbolic.

In early February, the UK, US and Australia published joint research on ransomware. It revealed that the threat has continued to grow over the past year and that operators have only become more sophisticated in their approach. "It's a really successful criminal model and therefore it's an enduring threat," says Maddinson.

However, hackers have begun to refine their focus. There has been "a bit of a move in places like the US away from what the criminals call the 'big-game hunting' of going after the really large companies", he adds. The trend is spreading across the Atlantic too, with small and medium-sized businesses in the UK increasingly finding themselves in hackers' sights.

Given the rising ransomware rates and the risk of Russian escalation, Maddinson could be forgiven for feeling pessimistic about the evolving threat landscape, but he remains undeterred. The war, he notes, has "proven what we were saying in the National Cyber Strategy", published in December. "We need to raise our cyber resilience against this kind of heightened threat. If anything, it's prompted us to try and accelerate some of the measures that we were intending to take anyway."

Maddinson clarifies that the NCSC is not focusing on specific sectors. "We're trying to raise the overall bar of resilience." By doing so, he says, government and industry will be better protected "against whatever threat may manifest itself as a result of the Russian invasion of Ukraine. But actually, we're also raising the bar against the other threats such as ransomware and cybercrime, which continue to be a major problem too."

THE NCSC

Why Ukraine has stayed online

Conventional forces are still the primary factor in warfare

By Jonny Ball

In November last year, as Russian troops gathered on Ukraine's border, Prime Minister Boris Johnson told MPs on the commons liaison committee that "the old concepts of fighting big tank battles on the European landmass are over".

"There are other, better things we should be investing in" besides tanks, said Johnson: "...in the future, combat air systems, cyber, this is how warfare in the future is going to be."

The Prime Minister faced a heated grilling from sceptical members of his own party, including the committee chair, Tobias Ellwood. He asked Johnson to "reconsider" cuts to conventional forces on land, sea and air. "What's amassing right now on the Ukrainian border?" asked the former soldier, before immediately answering his own question: "It's tanks."

The Integrated Review published by the government in March last year promised a "modernisation programme that embraces the newer domains of cyber and space". The number of British Army troops was to be cut to 10,000 below its conventional "established strength" of 82,000, alongside reductions in previously planned fighter jets and Royal Navy ships. A National Cyber Force was announced, with headquarters in the north of England. Cyber was, said Johnson, "revolutionising the way we live our lives and fight our wars, just as air power did 100 years ago".

Not even a year later, Russia is conducting a decidedly old-fashioned invasion of Ukraine on a scale not seen in Europe since the end of the Second World War, involving tens of thousands of ground troops and heavy artillery.

At the outset of the invasion, some predicted an unprecedented conflict in cyberspace. Russia's capacities for cyber warfare were known to be extremely sophisticated. The Kremlin had already proved itself an aggressive actor, particularly against its neighbour in Kyiv after the 2014 "Maidan" protests toppled the pro-Russian government of Viktor Yanukovych. In 2015, in western Ukraine, unidentified hackers became the first to successfully conduct a confirmed shutdown of a power grid by hacking. Ukraine's government immediately pointed the finger at Moscow.

Just a year later, a malware attack took down power in the Ukrainian capital – again, blame was quickly apportioned to shady groups affiliated with the Russian security services. The Kremlin issued strenuous denials. In 2017, the "NotPetya" ransomware attack targeted the National Bank of Ukraine and several other companies internationally (although 80 per cent of those affected were in Ukraine). Immediately prior to Russia's invasion, Ukrainian government websites were defaced with crossed-out yellow-and-blue flags, and a warning for visitors to "be afraid and expect worse".

But despite the history of cyber operations conducted against Ukraine after it moved to exit Moscow's post-Soviet sphere of influence, the country has remained online throughout the current conflict. Energy grids are functioning well. Communications have not broken down (at least in the parts of Ukraine that have remained unoccupied). And critical infrastructure such as public transport has remained functioning in many parts of the country.

"This is a bit of a dose of realism about the reality of cyber operations," says Jamie MacColl, a research fellow in cyber threats and cyber security at the Royal United Services Institute, a defence think tank. "They do have effects, they do have a place. But they're not a decisive capability. They are hard to use, they take a lot of planning and

they require a lot of resources."

All has not been completely quiet on the cyber front, however. Several attacks against companies and organisations in Ukraine have been reported since the conflict began – including one malware assault, coinciding with the start of the invasion, against Ukrainian customers of Viasat, a US provider of satellite broadband services. Other attacks have reportedly been thwarted with the help of the US and its allies. Since 2020, the US Agency for International Development has pledged investment worth $38m for building Ukraine's cyber operations.

Ukraine also boasts its own sizeable tech sector, which has pitched in with the war effort. According to *Radio Free Europe*, various hacktivist groups act as the Ukrainian counterparts of infamous Russian-linked hackers such as Fancy Bear. Ukrainian groups RUH8, Falcons Flame and CyberHunta (together known as the Ukrainian Cyber Alliance) use data leaks and website-defacement campaigns to undermine the Kremlin and its military operations.

"I think in some quarters it was severely overestimated what kind of things you can do with offensive cyber operations," MacColl tells *Spotlight*. "It is extremely difficult to shut off a national power grid. The cyber attacks that Russia conducted against a very small part of Ukraine's electricity system in 2015 and 2016 required something like 30 months of planning, and they were only able to turn the power off for a few hours. So the assumptions about those kinds of capabilities have always been slightly exaggerated."

Another area in which Russia has struggled to make an impact is in the information war. Prior to the invasion, as well as using cyber attacks and leaks against those opposed to their agenda, Russian bot and troll farms were engaged in promoting pro-Kremlin content online. The extent of the influence of such operations is hotly debated, but Russia's sway over public opinion in the West on the Ukraine invasion is virtually nil.

"I'd say that's because of the nature of the war," says Joanna Szostek, a lecturer in political communication at the University of Glasgow and an expert in Russian disinformation in digital and social media. "I was surprised [when they invaded Ukraine] because in the past it looked like Russia valued plausible deniability. Even if many of us considered it implausible deniability, there was at least some space for them to plausibly deny what they were up to, whereas [in this war] there's just no space for deniability at all."

SEAN GALLUP / GETTY IMAGES

Russian disinformation efforts about Ukraine have been unsuccessful in the West

This is a far cry from the time when the "little green men" who appeared on the Crimean peninsula in 2014 could be waved away and characterised as local separatists. Or when referenda could be held ex post facto to ratify the secession of breakaway republics within Ukrainian territory, as occurred in Crimea that year.

"All wars have their own unique dynamics," MacColl says. "The dynamic of this war has very much been set by the complete absence of planning and preparation on the Russian side." With better planning and preparation, he adds, things could have been different.

But this war has served as an ugly reminder to many that conventional military threats have not disappeared. Boosting cyber capabilities to the detriment of conventional forces is, as Tobias Ellwood told MPs last year, "a bit like saying, fine, I've managed to get my computer with all the software on it, I'm completely protected. But I forgot to lock the front door."

JOE RAEDLE / GETTY IMAGES

A refugee from eastern Ukraine arrives at the central station in Lviv

How the Ukraine conflict is reshaping the dark web

As the war drags on, cracks are forming in the digital underworld

By Zoë Grünewald

Before Adam Darrah spent his days scouring the internet for security breaches, the director of dark ops at ZeroFox, a cyber firm specialising in the dark web, was a US government employee. The work, he explains, involved a fair amount of speaking Russian and conducting "Russian analysis".

His move to dark web surveillance made sense, then, because the "kings and queens" of the dark web are Russian speakers, according to Darrah. "Nobody rules the dark web like the Russian-speaking world," he says.

The dark web – a group of websites only accessible via special routing software, usually Tor – has a bad reputation. The phrase has long been synonymous with a brisk illegal trade in pornography, weapons and drugs, and an ecosystem of hackers and illegal data dumps. The reality is far more nuanced, however. For each nefarious use "we can find beneficial" ones, says Robert W Gehl, an academic from Louisiana Tech University. "The *New York Times* set up anonymous whistle-blowing systems for people to point out government and corporate malfeasance. The *Times* also mirrors its content as a Tor hidden service, as does the non-profit news organisation ProPublica."

As Darrah explains, the potential user should think of the dark web as a "big city".

"You know where you belong and don't belong... If you stay in the places where you belong, you're fine," he says.

Since the outbreak of the Russia-Ukraine conflict this year, Darrah tells *Spotlight* he has not seen anything quite like it: the geopolitical tensions that have changed the world are also changing the dark web.

Russian-speaking dark web forums for hackers might often be accessible through criminal means, but they have always had what Darrah calls a "code of criminality". Under that unofficial code "you're not allowed to develop tools, or sell embarrassing information, that could hurt any nation in the CIS [Commonwealth of Independent States, a group made up of former Soviet republics]", he says.

But after Russia invaded Ukraine that code was broken when the Conti ransomware group posted on the dark web announcing their "full support of Russian government". ▸

"If anybody will decide to organise a cyber attack or any war activities against Russia, we are going to use all our possible resources to strike back at the critical infrastructures of an enemy," said the group, which has in the past carried out attacks on organisations including the Scottish Environment Protection Agency and clothing retailer FatFace.

According to Darrah, the move was unprecedentedly provocative – running counter to what he calls the "gentleman's agreement" of the dark web. This led to retaliation from Ukraine-aligned actors both on the dark and clear web. In what cyber security news site *The Record* has dubbed the "Panama Papers of ransomware", leaks of Conti's private chat logs were publicly dumped on the internet, with the Twitter handle @ContiLeaks laying bare "everything from the mundane details of how Conti is organised to new anecdotes about the group's possible links to the Kremlin".

This shows "cracks appearing in the order", says Darrah. "The rate at which data is being dumped by both sides is something I've never seen before. It's constant."

The conflict is playing out on the dark web in other ways, too. In March, a blog from Trustwave, a cyber security provider, reported that it had noticed a "wide variety of attempts by dark web forum members to influence the conflict from the cyber side". Groups have been set up on both sides specifically for cyber warfare, such as the "IT Army of Ukraine", which rallies hackers together to launch cyber attacks against Russian businesses and institutions.

These calls to action have changed since the Russian invasion of Crimea in 2014. At that time, for instance, Russian hackers disrupted Ukrainian telecoms, including the personal phones of Ukrainian MPs. But, as *Politico* has noted, those attacks were "nothing compared to what a full-blown physical invasion coupled with cyber warfare would look like". And experts say we are starting to see what that might look like. Trustwave said that cyber activity has become "more destructive and organised", with Ukrainian government officials calling for individuals to come and "fight on the cyber front" as part of the war effort.

"The dark web is a mirror of above-ground geopolitics"

The reason for the shift, Darrah believes, is the shock of the "unprovoked carnage", as well as the deep cultural and emotional ties between Russia and Ukraine.

"We all know how deep those ties are, historically, culturally, linguistically, everything," he says. In February, even the hacker collective Anonymous declared it was "officially in cyber war against the Russian government". On 26 February the group announced that it had hacked a number of streaming services and live TV channels in Russia to broadcast war footage from Ukraine. The footage showed a message reading "Ordinary Russians are against the war".

Could the dark web exacerbate the conflict, drawing more actors in and paving the way for increasingly destructive cyber attacks? Arguably, the dark web is amplifying some of the "background malicious cyber activity", says Eric Jardine, an assistant professor in political science at Virginia Tech, specialising in the dark web. He explains that this is because it allows the spread of tools and training. It also allows actors to "communicate with less risk of detection".

But both Jardine and Darrah believe that this activity is a direct result of the Russia-Ukraine conflict, rather than the inevitable evolution of technology and warfare.

"Understanding the political antagonisms that exist independent of the dark web helps you understand the way in which the dark web might get used in that nexus. Because if it can amplify, say, cyber attacks or cybercrime between countries, and you have pre-existing tensions, then it makes sense that it would," says Jardine.

But it was the "shock value" of this invasion that shook the foundations of the dark web, according to Darrah. The dark web does not always represent and amplify all that is bad in the world; it would be far more accurate to see the dark web as a reflection of the world outside, he says. "The dark web is a mirror of the clear web, and now the dark web is a mirror of the above-ground geopolitics."

SHUTTERSTOCK / GIOVANNI CANCEMI

Groups on both sides of the conflict have been set up specifically for cyber warfare

Comment

"For fraudsters, the rewards are colossal and the risks are far too low"

By Angela Eagle

An elderly constituent defrauded out of her life savings; a couple paying a deposit to their "solicitor" – who turned out not to be – and losing the lot; unauthorised loans taken out using a constituent's stolen identity – these are just some of the issues in my casework that are part of the tsunami of fraud sweeping the country.

Even prior to the Covid-19 pandemic, the growth of fraud and cybercrime was alarming and unacceptable. After two years of lockdowns, many of us have changed the way we shop and access services, and the scourge is growing exponentially. So far, the response of the government and law enforcers has been wholly inadequate. For the fraudsters, the rewards are colossal and the risk of being caught is unacceptably low.

The scale of the problem is staggering. Prior to the lockdowns, fraud was estimated to cost £130bn to the UK economy. The coronavirus support schemes run by the Treasury were so open to fraud that a department minister, the peer Theodore Agnew, resigned in protest, calling it a "great time to be a crook". He complained in evidence to the Treasury Select Committee that even very basic checks were not done before Bounce Back Loans were paid out. Despite the government's protestations, we know that little of the billions lost in the Eat Out to Help Out scheme and the Bounce Back Loans will ever be recovered.

The Treasury Select Committee, of which I am a member, recently held an inquiry into the increasing problem. We discovered a situation rapidly worsening, with each part of a fragmented law enforcement hoping someone else would take the lead in attempting to bring fraudsters to justice. The reality is that no one is taking the lead on enforcement effectively.

Ministers giving evidence professed themselves "frustrated" at the lack of progress and the seemingly inexorable march of the fraudsters and scam merchants. But they resorted to process-heavy explanations of action rather than focusing on outcomes. Clearly, despite various anti-fraud processes being successfully undertaken by the government, actual outcomes only worsen. Cybercrime and fraud are soaring even as the chances of catching and prosecuting the criminals diminishes.

The ONS recorded 4.6 million incidents of fraud in England and Wales at the end of March 2021, making it the most common type of crime. Action Fraud, the UK's national reporting centre for fraud and cybercrime, reported a 36 per increase in cybercrime during 2020, recording nearly half a million offences. Almost none are ever prosecuted. Authorised push payment fraud (where the victim is conned into paying money into the criminals' bank account) is the second-largest type of scam, with £207.8m being stolen in this way in 2017. Only a quarter of the victims of this fraud ever get their money back. Credit card fraud, copycat websites, clone sites, and investment and pension scams all flourish with impunity online. Even Covid-19 scams now proliferate, rising by 44 per cent to 95,531 incidents in the past year, according to Action Fraud. These are not victimless crimes. Many people are tricked out of substantial amounts of money and have their trust in people and the society they live in shattered.

We need more effective and co-ordinated anti-fraud enforcement as well as modern legislation. The Online Safety Bill, which is currently making its way through parliament, has thankfully been amended to include paid-for adverts rather than simply applying to user-generated content. This is a tiny step in the right direction given that it will introduce a duty on social media platforms and search engines to prevent fraudulent paid-for ads appearing on their services.

There is currently a government review under way of the regulatory framework for online advertising that has the potential to regulate more effectively the current "online Wild West". But none of this will make any difference if enforcement does not become more effective than it is currently. As the Financial Conduct Authority recently noted, there are promotions online for firms that do not exist, for companies that claim to be based in the UK but are not, and for clones of legitimate businesses. This must stop, and only the government can ensure that it does. ●

Angela Eagle is the Labour MP for Wallasey

The expanding threat landscape

Fortinet is building cyber resilience across industries

In association with FORTINET

Forty years ago, nobody envisioned that the internet – built to connect networks and devices – would become one of the most concerning landscapes of the 21st century.

In recent decades we have had significant cyber attacks in media, financial organisations, governments, oil and gas, and so on. These breaches coincide with a concerning rise in ransomware as part of the range of increasingly sophisticated attacks. These events became more prevalent as organisations started to expose their networks, data and processes to adapt to a new digital era. The same trends led Fortinet back in 2000 to identify the need for comprehensive security and to develop state-of-the-art solutions that provide broad, integrated and automated protection against security threats.

Data, the new radioactive element

As the digital field evolved, organisations realised data allowed them to make better business decisions. Data-driven business decisions became mainstream, but the methods to secure them stayed the same until the old and outdated 1995 Data Protection Directive was replaced by the General Data Protection Regulation (GDPR) in 2018.

GDPR mandated that organisations must protect user data by default. While GDPR did not slow down the number of attacks – nor was that its purpose – it enacted a shift in how securing personal data was done, from being an afterthought to being required by law.

GDPR also showed that data isn't oil, and is more like a radioactive source – extremely useful and powerful when contained in data warehouses where predictions and advanced analytics are extracted, but destructive when breached and out in the open, with a long half-life like nuclear waste. Think about the implications of exposing medical records, public political preferences in a regime, and so on: once it leaks, there is no turning back.

Regulations for a new digital age

Data will play a significant role as currency for artificial intelligence systems. As such, data regulations that don't stifle innovation will be one of the critical aspects that will drive substantial adoption.

The economic powers want to lead the regulatory data space. Europe did it once with GDPR, and it also signalled that it intends to lead the way with recent proposals such as the Data Act, the AI Act, and other digital policies that are part of its A Europe Fit for the Digital Age strategy.

On the other hand, the UK published its National AI Strategy last year, a ten-year plan signifying its intention to build the most pro-innovation regulatory environment in the world.

Besides the necessity of a regulatory framework around data, there is also a requirement for increased cyber resilience – an organisation's ability to prepare for, respond to and recover from cyber attacks.

The National Cyber Strategy 2022 plan highlights how the UK is focused on resilience as part of its strategy. The EU is implementing a similar approach with its A Europe Fit for the Digital Age strategy, which proposes a regulation to increase resilience in critical sectors and a new set of rules for sharing, processing and storing data.

The revision of the Network and Information Systems regulations (NIS2), and industry-specific regulation such as the Digital Operational Resilience Act (DORA) or the UK equivalent PS21/3 for financial organisations, steps forward to increase resilience in critical sectors.

Enabling resilience in critical sectors

DORA and PS21/3 are significant milestones for financial services organisations (FSOs). They will accelerate innovation by harmonising risk management across member states, identifying critical business services, setting thresholds for critical services, and requiring regular cyber resilience testing.

A key difference between DORA and PS21/3 is that the latter focuses on the financial institution's own scoped business services, whereas DORA focuses on ICT risks.

Another key provisioning in DORA is how to address third-party risk – as cloud service providers (CSPs) are a big part of the modernisation effort by FSOs, it can lead to concentration risk. DORA has specific provisions for third-party risk management that bring CSPs and other third-party providers into scope for risk management.

In that regard, Fortinet has been at the forefront of risk management, working with customers to support many areas from current and upcoming resilience regulations, such as:

- **Operational resilience**: Fortinet Security Fabric is the industry's highest-performing cyber security platform, with a rich open ecosystem spanning over 480 security partners. It covers the extended digital attack surface and cycle, enabling self-healing security and networking to secure people, devices and data everywhere.
- **Security monitoring**: Fortinet provides platforms and solutions to allow customers to monitor and track risk. FortiManager supports network operations use cases for centralised management, compliance best practices, and workflow automation to protect against advanced threat actors. The threat intelligence provided by FortiGuard Labs helps organisations stay ahead of new and existing threats.
- **Digital resilience testing**: Fortinet customers benefit from a long-standing commitment to meet the requirements of the most security-minded organisations. With a broad portfolio, comprehensive service offering, and a strong network of partners, Fortinet can help customers test their systems and networks to meet regulatory needs.

MICHAEL M SANTIAGO / GETTY IMAGES

Colonial Pipeline suffered a major ransomware attack in May 2021

A cyber-aware workforce

While technology is key in cyber security, people are the most critical sources for data compromises. Organisations must be prepared for a loss of control if their workforce is not taught cyber awareness.

The World Economic Forum states the current cyber professionals' gap sits at three million people, which will significantly impact the ability of organisations to respond to threats, and cause delays in digital transformation programmes. In response, the EU and the UK have focused on building digital skills and inclusion via CyberGirls, European cyber security education, the UK Cyber Security Council, and many more programmes in the past years.

Fortinet, as a cyber security leader, has provided both free training through the Fortinet Network Security Expert (NSE) Training Institute and resources on cyber awareness to help build a resilient workforce. It is also committed to helping address the cyber security professional gap by training one million cyber professionals by 2025. Partnerships with active associations such as Women in Cybersecurity (WiCys) or Latin American Women in Cybersecurity (WOMCY) are working to promote the Fortinet NSE certification among those communities and organisations. ●

Follow Ricardo Ferreira, field CISO at Fortinet, on LinkedIn: linkedin.com/in/securecyber

How ransomware shut down an English council

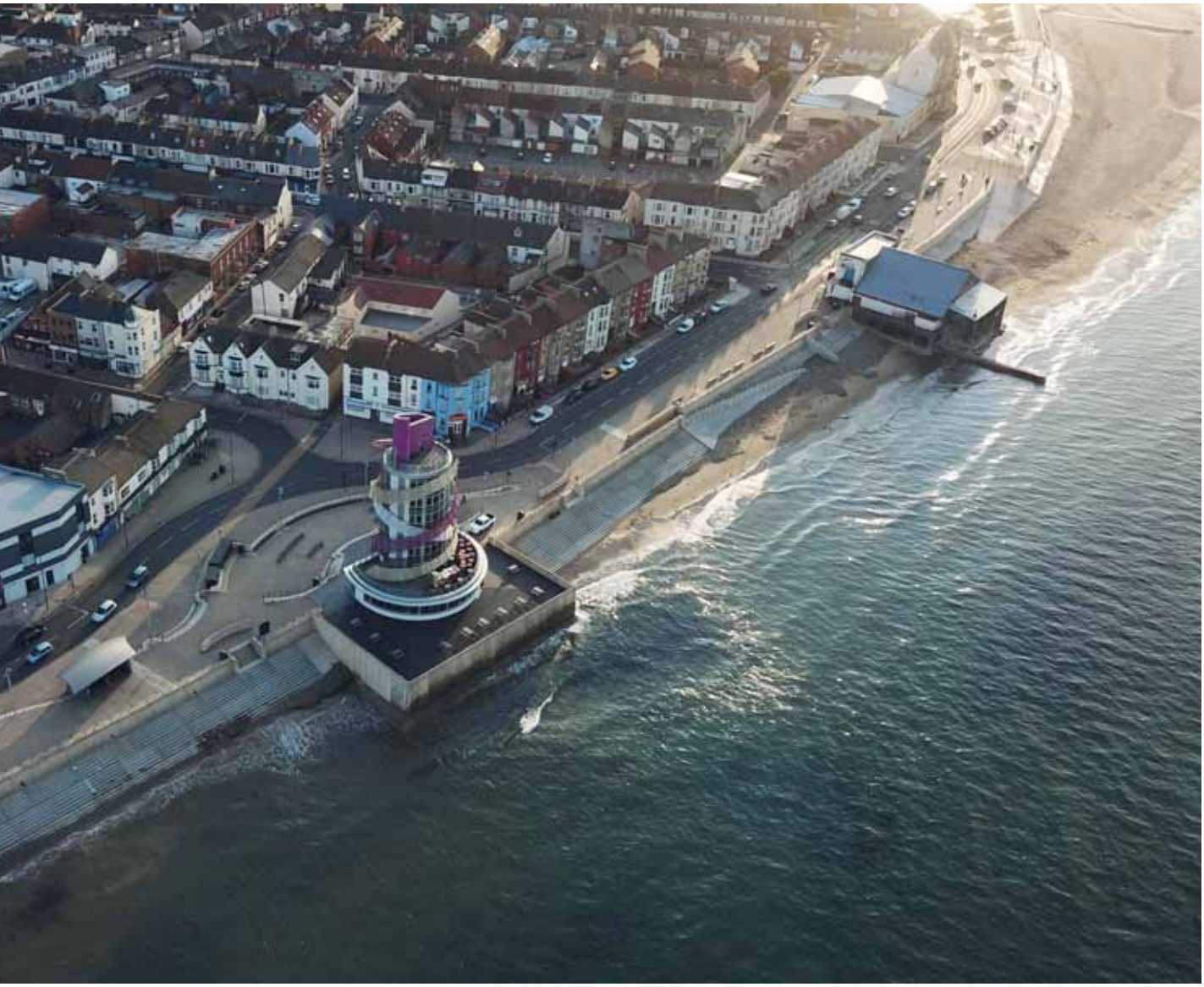
The attack that sent Redcar and Cleveland back to pen and paper

By Samir Jeraj

It was 8 February 2020 and the Covid-19 outbreak was yet to be declared a pandemic. In Yokohama, Japan, 61 of the passengers on a quarantined cruise ship were suspected of having caught the novel coronavirus. Meanwhile, in north-eastern England, a very different type of virus had struck.

At around 11am that February morning, cybercriminals unleashed a "catastrophic" cyber attack on Redcar and Cleveland Council, overcoming its defences and taking down the entire computer system in a matter of minutes. *Spotlight* has pieced together the events from public documents, reports and information as the council declined to participate in this story.

A single email with an attachment



The coastal town of Redcar, with its iconic Beacon

SHUTTERSTOCK / NIGEL RUSBY

was the source of the attack. Council IT staff noticed immediately, recognised what was going on, powered down the servers and called in the National Cyber Security Centre (NCSC). A subsequent external investigation by the council's auditor would conclude the council had "proper arrangements and controls in place to reduce the likelihood of a cyber security breach" given the resources available.

But it was already too late: almost every computer, laptop and phone connected to the system was rendered unusable, visitors to the council website were greeted by an error message to "please try later", and partner organisations cut off contact to avoid the contagion spreading. As a unitary council, Redcar and Cleveland runs local services ranging from bin collection and street cleaning to housing, social services and schools. All were affected.

"Councils, like many organisations and individuals globally, frequently face attempted cyber attacks," councillor Peter Fleming, leader of Sevenoaks District Council and chair of the Local Government Association's (LGA) Improvement and Innovation Board, tells *Spotlight* via email. "[But] in most cases, these are untargeted attacks, where malicious actors indiscriminately target devices and users regardless of the victim."

As the world went remote, the staff went analogue

Redcar and Cleveland Council was initially cagey about releasing all the details about the "cyber attack" to the press and public, and took 19 days to confirm what everyone already suspected – that it had suffered a ransomware attack. Throughout this time, its IT system remained unusable, and it would take the council around eight weeks to restore a majority of services, and a further five to restore ▸

◂ the "low-priority" data that it held. Some services did continue, however: on Facebook, one resident noted that council tax payments were still being taken online by a third-party organisation.

Following the attack, senior council officers quickly set up a command centre to coordinate their response, establishing new systems and governance mechanisms to cope with the lack of IT, telephones and printers. Confidential information was kept in that room and that room alone for the first few weeks.

As well as encrypting all operational data, rendering it useless, the cybercriminals encrypted the back-ups too. The only data to avoid this fate was held on antiquated tape storage that was too obsolete to be affected by the ransomware. It contained "significant" amounts of children's services data.

Business continuity documents that were saved digitally and not available in hard copy also could not be used. Staff went analogue, putting in new phone lines and reverting to pencil and paper to record information while the online services were rebuilt. As the world began to go remote due to the start of the Covid-19 pandemic, council officers held face-to-face meetings to keep each other informed of what was happening because they could not rely on email. They worked long, stressful hours, council staff later recalled in a video about the attack, and had to accept that years of their work may have been lost in the blink of an eye.

The cybercriminals said they would keep the data encrypted until Redcar and Cleveland paid them £1m. The council refused because there was no guarantee that the data would be released, and because, as noted in the minutes from a November 2021 meeting of the council's Scrutiny and Improvement Committee, central government had requested that it refuse to pay.

"Deciding to pay a ransom demand is a very difficult choice for victims and one that is not taken lightly," says Eleanor Fairford, deputy director for incident management at the NCSC. She adds that "sadly, if you do pay the ransom there is no guarantee that you will regain access to your data, and seeing their scheme work can embolden criminals to try the same thing again".

Redcar and Cleveland was also in no position to pay the ransom. At the time of the attack, the council's total annual spend was £279m and it had just £5.2m in reserves, down from £25m in 2019. The administration, a mix of Liberal Democrats and independents who had taken power from Labour in the May 2019 local elections, was warned by its auditor that summer that it would run out of money by 2021 unless it cut spending (the council has since made cuts, raised council tax and been able to shore up its reserves).

"Responding to a cyber attack can be incredibly challenging," says councillor Fleming. He adds that a "multi-stakeholder response" has been shown to be effective in dealing with cyber attacks on local governing, bringing together support from the NCSC, the LGA, the Department for Levelling Up, Housing and Communities, and the Cabinet Office.

School admissions were an early victory for council officers at Redcar and Cleveland, with around 1,500 anxious families assured on 28 February that secondary school places would be allocated as usual and on time, despite the cyber attack.

Initially, the council costed the damage caused by the cybercriminals at around £16.4m, but by August 2020, it had reduced that to £10.4m, and then down to a final figure of £8.7m following a financial impact assessment completed in June 2021. The government offered to give the council £3.68m in April 2021. This prompted outrage from councillors, who had been led to believe central government would take "full responsibility" for the cost of the attack, according to the minutes of a council meeting. The council administration would later come in for criticism for acceding to demands for confidentiality from central government and keeping backbenchers and opposition councillors in the dark over these developments.

A later investigation led by councillors concluded that the loss of several senior officers for reasons not related to the attack may have affected the ability of the council to negotiate robustly with central government. They also noted, however, that Redcar and Cleveland is the only local authority to date to have received any money from

The attack took place shortly before

the pandemic hit. Pictured: Redcar and Cleveland council piloting Covid-19 lateral flow tests

IAN FORSYTH / GETTY IMAGES

central government (that was not a loan) to deal with the aftermath of a cyber attack.

"It's essential local authorities treat cyber security as a priority and take action to protect their systems, secure sensitive data and practice incident response plans in case the worst happens," says Fairford. She encourages councils to use the NCSC's free Active Cyber Defence services and to follow NCSC guidance to help them run smoothly.

"Ten years ago, cyber security was a niche, technical topic," says Fleming. "The last decade was the first decade since the Second World War that civil institutions in the UK [have come] under regular attack from foreign actors." He adds that this means cyber security requires investment in skills and technology, and a change in "mindset and culture", particularly in local government providing vital services to vulnerable people. He says the LGA is supporting councils to explore and improve their cyber security culture through a new LGA Cyber 360 programme. Fairford, meanwhile, says the NCSC works closely with local authorities to advise on cyber security best practice and offer expert advice on keeping systems secure.

"Following Russia's invasion of Ukraine, cyber risk is heightened globally," says Fleming. There have been multiple Russian attacks against Ukrainian critical infrastructure since the start of the year and the intelligence services have warned that more are likely.

"We in local government remain vigilant to the increased cyber risk," he states. The reality is that Redcar and Cleveland may be an early warning for other councils. The London Borough of Hackney also suffered a catastrophic cyber attack in October of 2020, as did Gloucester City Council in December 2021. It is likely that others will follow.

Cybercriminals are difficult to track and even more difficult to prosecute, and waves of untargeted attacks for money may increasingly be matched by targeted attacks by or on behalf of nation states as geopolitical tensions rise. While local governments can put in the precautions they can afford, they may also need to plan for the worst-case scenario: running a 21st century organisation on analogue alone.

Secure the edge to protect the core

Why software attestation alone is not enough to keep critical infrastructure safe

In association with ULTRA

The first step in any system security design is a risk analysis. This is designed to answer questions about external interfaces and threats. While encrypted communication and user authentication controls are straightforward enough, a system security architecture quickly becomes complex when answering the question "how does a system ensure software is trustworthy?"

Attestation is the process of validating software authenticity during start-up and periodically during operation. The purpose is to detect software tampering and code injection. There are many trade-offs to consider in security design, including public key storage, start-up timing, impact on performance, software updates and private key management. Solutions range anywhere from on-chip secure boot, such as the i.MX processor, to a Trusted Platform Module co-processor, or software-based solution. Each has its own risks, cost and design impact, which is why it's important to engage with cyber security design experts.

Without attestation checks, malicious software can quietly run in the background collecting system and local network data, or even perform a pivot attack by sending malicious commands in an attempt to exploit other devices. Starting with hardware, attestation checks software layer by layer using digital signature algorithms to verify authenticity. This process makes sure none of the operational security controls, such as command authentication and encryption, can be bypassed by the malicious code.

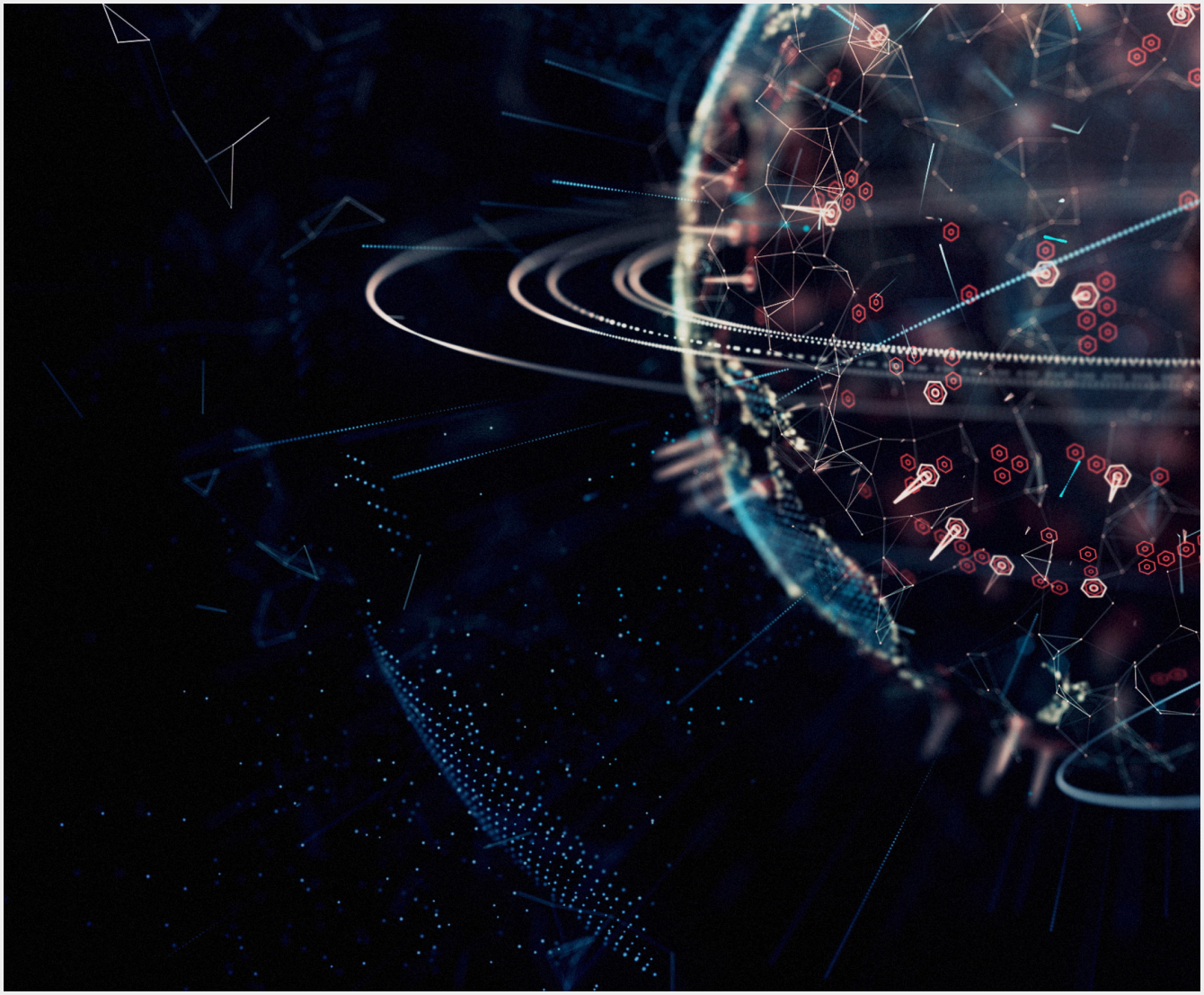
Securing millions of lines of code in the internet of things

Attestation may protect the intended security controls but makes no promises about the quality of the software itself. A zero-day attack is the exploitation of a latent defect within completely authentic software, typically resulting in the injection of malicious code to compromise data or operations. Without attestation, the modified code can be stored to memory and executed every time.

According to the Steve McConnell book *Code Complete*, the industry average of latent defects is about 15-50 errors per 1,000 lines of delivered code (Kloc). With even the most experienced software developers, Microsoft reports 10-20 defects per Kloc during testing, and 0.5 defects per Kloc in production.

According to a 2017 *Visual Capitalist* article, an average iPhone app has 50,000 lines of code, a military drone uses 3.5 million lines of code, the Android operating system includes 12-15 million lines, and a modern car contains 100 million lines of software. Most internet of things (IoT) devices rely on an operating system and third-party libraries, so even at a conservative one million lines of code, this means there's anywhere from 500 latent defects to upwards of 50,000. What's the probability that there's a zero-day attack somewhere in there? Now multiply it by the number of different IoT devices currently on your network. Bottom line: even with the best security design, no IoT device is completely trustworthy.

On a more alarming scale, the supply chain attack against SolarWinds' Orion network monitoring platform in 2020 sent shock waves throughout the world, with suspected state-sponsored hackers gaining access to US government agencies, critical infrastructure entities and private sector organisations. The injection of malicious code into Orion between March and June 2020 allowed the hackers to compromise Microsoft and FireEye, as well as the Defense, State, Treasury, Homeland Security and Commerce departments in the US



Without attestation checks, malicious software can run quietly in the background collecting data

government. The SolarWinds hack was severe because it took place on the build server, injecting malicious code before the digital signing process. As a result, the compromised software became authenticated and undetected by system attestation checks.

Edge network security

Since attestation and security design are unable to address all vulnerabilities, IoT device users need another layer of defence to protect their data and core computing resources. An edge network security solution provides the required reinforcement to detect and contain the impact of a compromised device though the following capabilities:

1. VPN/VLAN Encryption: segmenting devices onto their own network or private cloud protects other computing resources from traffic monitoring and pivot attacks. The combination of a network encryptor with end-point software are the building blocks to FedRAMP and Commercial Solutions for Classified approval.

2. Gateway: monitors and controls the networks, subnets, addresses and ports that a device may communicate with. This minimises incoming network attacks, while controlling outgoing message destination in the event of compromise. Robust event reporting enables administrators to detect and take action.

3. Deep Packet Inspection: monitors and controls the type of messages that are communicated between approved systems to ensure only valid data is exchanged between approved end points.

Ultra CYBER's edge network security solutions combine encryption, gateway and deep packet inspection into wired, wireless and embedded form factors to meet any operating need. Ultra CYBER supports clients with best practice products and services to protect critical infrastructure device operation and data. ●

Gregory Rudy is vice-president, business development at Ultra Intelligence & Communications – CYBER Division

ULTRA

The UK Cyber Security Council

"You don't have to be a programmer to work in cyber"

Simon Hepburn, CEO of the industry's new trade body, on demystifying the sector

By Sarah Dawood

Working in cyber security comes with great responsibility. The same skills that lead someone to be an excellent threat analyst or penetration tester also enable them to be an excellent hacker; there is little separating security professionals from criminals apart from morals, and expertise can be used for nefarious purposes. This is why, explains Simon Hepburn, CEO of the UK Cyber Security Council, the industry needs oversight.

"When you train people in ethical hacking and penetration testing, there is a firm focus on protecting, but [this knowledge] could [be used for] the opposite," he says. "We really want to build in and maintain public confidence in the industry."

The council, which launched last year, was born out of the UK government's National Cyber Security Strategy 2016 to 2021. This concluded that the industry needed a new independent body that could set professional standards and bring together different specialisms.

Cyber security companies join as members on a voluntary basis. The organisation's core aims are to bolster professional development and training through establishing qualifications and curriculums, improve the industry's diversity and inclusion, and regulate cyber firms through a new code of ethics and "chartered status" – an official mark of approval.

Research suggests there is a need for such an overarching body. Less than a quarter of UK cyber roles are filled by women, while there is a significant skills gap – recent reports from the Department for Digital, Culture, Media and Sport found that there is an annual shortfall of 10,000 people in the sector, while half of all businesses say they lack basic cyber skills.

Hepburn, who has a background in social mobility, education policy and career development rather than cyber, admits he is in no way a "technical expert" but was drawn to the organisation due to its onus on "making a difference" through helping to create a more "open and inclusive" profession.

The council is the first all-encompassing cyber industry body and is still in its infancy. A key challenge for Hepburn will be joining up the various organisations, resources and regulations that already exist. Cyber professionals are currently expected to abide by the

Security of Network and Information Systems (NIS) Regulations 2018 and GDPR, while a certification called Crest exists for penetration testers specifically (those who are trained to simulate cyber attacks). Additionally, the Cyber Body of Knowledge (CyBok) is an online archive of learning materials, providing a basis for an official cyber curriculum.

Hepburn says that he "doesn't want to reinvent the wheel" and is borrowing from these resources to develop qualifications and standards. He has also been inspired by more established industries, such as medicine and law, to create a code of ethics and a professional "chartership", which would require cyber businesses working on critical national infrastructure or big government projects to be accredited. These measures will help to ensure individuals are "held to account", he says, with the risk of being struck off the chartered list if not.

Hepburn believes the new official body will help to instil public confidence in the industry, but some worry that the creation of the UK Cyber Security Council causes yet more confusion in an already fragmented technology sector, and risks creating a silo between system design and system security.

"My concern is that separating 'cyber security' as a discipline from computer science or 'computing' is not going to end well," says Ian Batten, a lecturer in computer security at the University of Birmingham. "It implies that we are OK with continuing to make insecure systems, then adding the security afterwards." He likens it to "adding seatbelts to an old car" and says that the existing chartered institute for IT – the British Computer Society (BCS) – would be "far more appropriate" as an overarching regulator.

Hepburn, however, believes that cyber needs to find its own voice. "We're such a new profession – we don't want to get lost in computer science or IT because cyber security is not just that," he says.

"One of the myths of the sector is that you have to be a programmer, and it's all to do with computers and technology," says Hepburn. "This is one of the reasons a lot of people don't join. But the 'ologies' – criminology, psychology, anthropology, sociology – are all really helpful skills to have."

UK CYBER SECURITY COUNCIL

"Cyber attacks are not biased to race, religion or class," says Hepburn

This confusion carries through to higher education, he says, with university students often studying incongruent courses for the jobs they want to do. "Someone will do a course in security architecture when they want to do penetration testing," says Hepburn. "We need to accelerate awareness of the profession." The council has recently employed an outreach and diversity programme manager to help do this and is working on networking events with schools and businesses, where students can learn about different roles and even secure entry-level positions.

The need for sector regulation has never been greater. New rules are coming into force in the EU (the Digital Operational Resilience Act), which place more liability on cyber companies that provide security solutions to financial services firms (such as banks), should a breach happen. This is of particular importance to global cyber companies, and regulation is likely to follow suit in the UK and for other critical sectors.

Only morals separate ethical hackers from criminals

The council's accreditation systems are currently a work in progress, and in the meantime Hepburn's main priority is in public awareness and promoting the work of partners such as the National Cyber Security Centre (NCSC) to highlight the ever-evolving threat of cybercrime and encourage the public to secure their systems.

"Cyber attacks don't have any geographic boundaries," he says. "They're not biased to race, religion or class – criminals will attack absolutely anybody and organisations of any size."

But "this is not about scaring everybody", he adds; it's about consolidating "the basic things we can all do to protect ourselves". ●

Protecting the most critical infrastructures with wired, wireless, and embedded encryption solutions forged by decades of cryptographic engineering accomplishments.

High Grade Cryptographic Capability For The Toughest Missions

Our cryptographic offerings possess the highest certifications, while addressing modularity, multi-purpose use, legacy support, field re-programmability and ruggedisation for deployment in the toughest of military environments. Ultra is uniquely positioned to develop interoperable **National Security** cryptographic solutions for UK, US, and FVEYs partners.

Certified Edge Security To Protect Devices And Their Networks

A suite of flexible certified **Edge Network Security** solutions to segment and protect devices/computing resources. Wired, Wireless, or Embedded – Ultra edge encryption includes tunnels, gateways, and deep packet inspection for any environment; including federal and critical infrastructure use.

Key Lifecycle Management Solutions For End-to-End Security

Offering the highest FIPS 140-2, Level 4 certified hardware security module (HSM) to protect cryptographic key throughout their lifecycle. Ultra's Keyper and CARDS solution suite provides assured Key Management between devices and users.

Visit us at stand C17 or at **www.ultra.group/cyber** to learn more about Ultra's cybersecurity solutions.

ULTRA