Lindy Cameron at Cyber 2021, Chatham House

Lindy Cameron reflects on her first year as the NCSC CEO with a fresh ransomware warning

In a Chatham House speech today (Monday, October 11), Lindy Cameron marked her first year as NCSC CEO by looking back on key learnings from the past year and warning that ransomware is the most immediate cyber security threat to UK business.

The speech also covers major international cyber incidents over the last year and the actionable steps that would have avoided many of these threats.

The full speech is available below.

Lindy Cameron's speech in full

Good afternoon.

It is a pleasure to be opening Cyber 2021 and I am delighted to be speaking alongside such an array of experts.

As the CEO of the National Cyber Security Centre, it is great to see an organisation with such a strong track record as Chatham House focus so keenly on cyber security.

As Patricia said, I'm joining you today just over a year into my tenure at the NCSC. It was a huge honour to take over leadership of such a pioneering organisation. The creation of the NCSC within GCHQ five years ago showed real foresight and recognition that improved cyber security was central to the UK's future prosperity.

Since our creation we have delivered significant benefits to the UK. I would encourage you to look out for our Annual Review, which will be published next month and will showcase some of the positive real-world impact we have had over the last year.

But in a world where emerging technology is developing at a rapid pace – and a six-hour outage at Facebook and WhatsApp makes global news headlines – we can't rest on our laurels. The NCSC has always been firmly focused on how the UK can safely take advantage of the opportunities that technological developments create. And to ensure we do that we must continually understand the ever-changing challenges that we face.

So, a year into the role, I am going to review some of the major events we have seen, discuss the current threat picture we face and – most importantly – consider the future challenges that we are anticipating and how we intend to manage them.

Central to keeping the UK at the forefront of cyber security will be a new National Cyber Strategy, due to be launched before the end of the year. And a refreshed NCSC mandate to scale the impact my organisation delivers to build the UK's cyber security.

Looking back over the last year

But looking back on the last year we have had some major cyber incidents to manage and indeed major successes achieved.

Probably the most significant – and one that received attention across the world – was what became known as the SolarWinds attack which involved one of the world's most popular IT system management platforms being compromised by the Russian Foreign Intelligence Service.

Supply chain attacks – where an actor can find a route into a victim's system by targeting a vulnerability in their software or service supplier – aren't new and we've published guidance about how to manage those risks. But the large-scale nature of the attack and the privileged position the software had was different in this case. Thousands of installations were affected, even though it appears that the end targets were predominantly focused on the US Government.

We have also seen in the last year real-world impact from a spate of ransomware attacks. There has been significant damage caused to the public sector. Ireland's Health Service Executive suffered a massive ransomware attack, leading to months of disrupted appointments and services.

Hackney Borough Council announced significant disruption to services – leading to IT systems being down for months and property purchases within the borough delayed. And of course the attack on the Colonial Pipeline Company led to fuel shortages across the East Coast of America.

We have also seen a vulnerability in Microsoft Exchange exploited – initially by Chinese state-backed actors known as HAFNIUM. When Microsoft identified the issue and planned to patch, the exploitation became much more widespread and damaging. What was particularly challenging about responding to this incident was how easy it was for attackers to work out which servers were vulnerable.

Perhaps one of the key things I have learnt in my time as NCSC CEO is that many – in fact actually the vast majority - of these high-profile cyber incidents can be prevented by following actionable steps that dramatically improve an organisation's cyber resilience. This advice is freely available on the NCSC website and I would encourage you to visit. Because responsibility for understanding cyber security risks does not start and end with the IT department. Chief executives and boards also have a crucial role – and we have advice for them too. I don't think any chief exec would get away with saying they don't need to understand legal risk because they have a General Counsel. I think the same should be true of cyber risk. This is a board-level issue.

In the last year we also saw NSO Group's Pegasus suite, which was a separate issue with far-reaching consequences. Reportedly, customers of NSO Group had marked tens of thousands of global telephone numbers as potential targets which demonstrated something we have raised a red flag about before – the commercial market for sophisticated cyber exploitation products was an issue.

Those with lower capabilities are able to simply purchase techniques and tradecraft – and obviously those unregulated products can easily be put to use by those who don't have a history of responsible use of these techniques.

So we need to avoid a marketplace for vulnerabilities and exploits developing that makes us all less safe.

But we haven't just spent the last year simply defending against attacks – the UK Government has also taken steps that will make our country a safer place to live and work in the decades to come. Again, I will say much more about NCSC's role in this at the launch of our Annual Report in November, but to give you some key highlights:

We made significant progress on the Telecommunications Security Bill, which will protect the UK from cyber threats to and through the telecoms network that underpins our digital society. Once enshrined in law, this will change the incentives within the sector – mandating good, objective security in operators and vendors and providing Government with the ability to restrict vendors we judge pose a national security risk. But the Bill is only part of the solution to the challenges we have seen in the telecoms supply chain and DCMS's diversification strategy will also play a crucial role in addressing market failure.

We've also seen the National Security and Investment Act which is now on the statute books – enabling the government to intervene in takeovers and other business transactions to protect national security, including for cyber security reasons.

We have also continued to roll out the NCSC's Active Cyber Defence Services to protect our country at scale from cyber threats.

And we have worked with sectors – from education to farming, sport to CNI – to provide bespoke advice on becoming more resilient.

And we have continued to drive increases in cyber security skills and diversity in the industry, including through our flagship CyberFirst Girls Competition.

The challenges we face today

So let me say a little bit about the challenges. Looking back at the last year illustrates the diverse nature and significance of the threats and cyber issues we face and will continue to face in the coming years.

A year into my time at the NCSC, what are the key challenges today?

This is obviously something we discuss a lot internally, but as the world slowly opens up again, it's been really great to share our thinking on these challenges with our international partners face-to-face – or in reality mask-to-mask.

You are probably expecting me to list several countries – and it would be remiss of me to give a speech to Chatham House without doing that.

But first I want to discuss four key themes that we are seeing today in cyber security – some of which I have already touched on. These four are: the ongoing impact of the pandemic; the ongoing threat posed by ransomware; the growth of supply chain attacks, and the strategic technological challenges we face.

Firstly, the Coronavirus pandemic continues to cast a significant shadow on cyber security and is likely to do so for many years to come. Malicious actors continue to try and access COVID related information, whether that is data on new variants or vaccine procurement plans. Some groups may also seek to use this information to undermine public trust in government responses to the pandemic. And criminals are now regularly using COVID-themed attacks as a way of scamming the public.

Secondly, ransomware presents the most immediate danger to the UK, UK businesses and most other organisations – from FTSE 100 companies, to schools; from critical national infrastructure to local councils. Many organisations – but not enough – routinely plan and prepare for this threat, and have confidence their cyber security and contingency planning could withstand a major incident. But many have no incident response plans, or ever test their cyber defences.

And the law enforcement challenge these groups pose is acute: the criminals responsible often operate beyond our borders, are increasingly successful in their endeavours, and pose a global challenge we must fight together to ensure no place becomes a safe haven.

But while ransomware continues to pose a threat, the methodology of ransomware criminals is evolving as they seek more effective ways to make money: in addition to shutting down an organisation's ability to function, many now also threaten to publish exfiltrated data on the dark web. And their intention is clear: to increase pressure on victims to pay.

We expect ransomware will continue to be an attractive route for criminals as long as organisations remain vulnerable and continue to pay. We have been clear that paying ransoms emboldens these criminal groups – and it also does not guarantee your data will be returned intact, or indeed returned at all.

But we should not view ransomware as a risk we have to live with and can't do anything about. We've seen this issue become a leader-level G7 topic of conversation this year. Governments have a role, and we are playing our part. We are redoubling our efforts to clamp down and deter this pernicious and spreading crime, standing firm with our global counterparts and doing our best to turn this into a crime that does not pay.

But victims also have agency here too. So I'm going to ask: do you know what you would do if it happened to you? Have you rehearsed this? Have you taken steps to ensure your systems are the hardest target in your market or sector to compromise? And if you'd even contemplate paying a ransom, are you comfortable that you are investing enough to stop that conversation ever happening in the first place.

Thirdly then, supply chain attacks which continue to be an attractive vector at the hand of sophisticated actors and I think the threat from these attacks is likely to grow. This is particularly the case as we anticipate technology supply chains will become increasingly complicated in the coming years.

SolarWinds was a stark reminder of the need for governments and enterprises to make themselves more resilient should one of their key technology suppliers be compromised. But I think that incident illustrates two key principles we need to follow in how we manage these risks.

First, organisations need to establish a clear security direction with their suppliers, asking for and incentivising good security through their supply chains – often relatively straight forward security practices, such as controlling how privileged access is managed.

Secondly, organisations should take an approach where their design is resilient if a technology supplier is compromised. The SolarWinds incident is a good example. To be blunt, if your SolarWinds installation couldn't talk directly to the internet – which it shouldn't have been able to do – then the whole attack was irrelevant to your network.

I completely understand this is getting harder, especially for small businesses with less capability. But it is crucial to build layered defences that are resilient to this and the NCSC has advice and guidance that can help.

My fourth theme then is one of the biggest and most significant challenges we are grappling with today, the development of strategically important technology. Technology continues to advance and develop at pace and has become ever more integrated into our everyday lives, our businesses and our infrastructure. We are all increasingly dependent on that technology and it is now fundamental to both our safety and the functioning of society, which gives us two challenges.

First, where the UK leads in an emerging technology, our adversaries may seek to steal that technology, traditionally through cyber espionage and IP theft. But increasingly seeing this threat is evolving to include strategic foreign investment into those companies – enabling our adversaries to effectively buy emerging technology rather than steal it.

And secondly, there is a very present risk that, as technology and supply chains globalise, our adversaries and competitors will seek to influence the standards of emerging technology in a way that undermines our security. Think about smart cities in the future. Our democratic values enshrine security and privacy, and our development of the standards and technology will be guided by those values.

Authoritarian states like China consider surveillance to be more important and therefore its standards and technologies are more likely to be driven by those values. So what values will drive international standards? What does that mean for our long-term security and privacy? At the NCSC, we are already planning for these challenges as our recently published security principles for smart cities show.

So, if those are the four big themes or challenges, what about the threats? I doubt anything I'm about to say will come as a surprise to a well-informed audience like you because the Government's Integrated Review published earlier this year makes clear that "*Russia remains the most acute threat to our security.*" And we have been clear and consistent in calling out Russian cyber aggression. In addition to the direct cyber security threats that the Russian state poses, we – along with the NCA – assess that cyber criminals based in Russia and neighbouring countries are responsible for most of the devastating ransomware attacks against UK targets.

China is clearly a highly sophisticated actor in cyberspace with increasing ambition to project its influence beyond its borders and a proven interest in our commercial secrets. How China evolves in the next decade will probably be the biggest single driver of our future cyber security. This is a country with an internal market of over 1.4billion people that sits behind a heavily protected Great Firewall. Demand from a market that size will be a huge driver of international future technology. But competition in that market is carefully controlled. What the Chinese government sees as its role in technology – and how it chooses to project that internationally, while protecting it domestically – will be really key. We must be clear eyed about this, and – in particular – protect ourselves against Chinese practices that have an adverse effect on our own prosperity and security.

While less sophisticated than Russia and China, both Iran and North Korea regularly use digital intrusions to achieve their objectives – including through theft and sabotage.

I know of course an audience at Chatham House will be interested in nation-state cyber activity, but it is important to remember that the vast majority of hostile cyber activity that most people and organisations in the UK will experience will come from criminals, not from nation states.

And therefore absolutely central to the UK's response to these threats is resilience.

We need the UK's public sector to be the best defended in the world.

We need the UK's businesses and organisations to understand the threats they face.

And we need the Great British public to have the skills to help them stay safe and to have technology to hand that removes the security burden on their daily lives, making them safer by default.

Often it is as simple as following straightforward steps that will dramatically improve cyber resilience. And of course the best place to start - as you'd expect me to say - is at NCSC.gov.uk.

The challenge of tomorrow

So if these are the challenges of today, what are the challenges of tomorrow? Given the rapid development of emerging technologies we must think ahead. We need to anticipate how the threat will change, so we are ready to respond to it.

In the coming years, society will benefit hugely from developments that make our lives more efficient and greener – such as smart cities. But it is inevitable that our adversaries – whether they are nation-state or cyber criminals – will seek to exploit the opportunities that these changes bring. And when they are successful, the potential impacts are much greater than the attacks we see today. So, we must ensure we are in a strong position to safely take advantage of these emerging technologies.

Unless we design them properly, changes like smart cities will bring with them an ever-increasing attack surface and proliferation of vulnerabilities for our adversaries to exploit. and that combined with the wider availability – often on commercial terms – of cyber exploitation tools, means that hostile actors will be able to deploy malware with greater frequency and less predictability.

Alongside this change, we are likely to see the balkanization of technology. I spoke already about how states are using technical standards and technology to promulgate their values and their political agendas. No great state will ever again be reliant on its adversaries for core technologies and know-how: I think the US action against Huawei shows the impact of that dependency. But we probably therefore will end up with multiple competing tech stacks, each with very different security properties. Long-term cyber security in that future world will look very different.

It's an issue that Chatham House are already doing valuable work on – only last week GCHQ Director Jeremy Fleming took part in a fantastic discussion here with Dame Wendy Hall on "who controls the internet."

Meeting tomorrow's challenges

So the challenges that we face both today and in the future are clearly significant. But at the NCSC and across Government we are ready to meet them.

The Government's Integrated Review provides an excellent framework for our response – setting the ambition for the UK to be a world-leading democratic and responsible cyber power, able to protect and promote our interests in, and through, cyberspace.

Cyber security is absolutely critical to delivering key Government strategies from boosting national resilience to making the UK a science and technology superpower. And to ensure the ambition is delivered on, the Government as I said will be publishing a new national cyber strategy later this year.

To meet the challenge of the future, we must not only build on our successes to date, but take our cyber security to the next level of scale and automation to meet the threats that we will face in the next decade.

National cyber resilience is the foundation of cyber power and our first priority must be to recalibrate our approach to it. I mentioned, the Facebook and WhatsApp outage last week which was not a cyber incident is an example of the impact when key services are not available – essential communications systems stop working and businesses lose money.

To date, we have made great progress building UK resilience. Our Active Cyber Defence programme has delivered transformative services that remove malicious content at scale. A lot of that is down to many of our citizens – the suspicious email reporting service has received 7.7 million reports from the public and taken down 119,000 malicious URLs as a direct result of these reports. By protecting themselves better, citizens are also keeping each other safer and their country safer.

But the systemic risk to many of our critical networks and data is too high and we cannot tolerate this risk into the future. So we need to combine tougher regulation in some sectors, with targeted, increased support in others, and better protection across the board for citizens, including enhanced and automated defences.

We in Government must lead the way in improving our own cyber security – protecting critical national infrastructure, critical government services and data we hold in trust for everyone. And Government investing in its own cyber security will also mean the public sector's buying power will help ensure the market provides good, secure technology by default. This will be essential to realise the benefits of the UK's long-term transition to a fully digitized economy.

We also need to ensure that technology is "secure by default" – and at the NCSC we are continuing to change how we work and challenging the orthodoxy using science and evidence. So last month for example we published our plans to move away from our past, prescriptive approach to assuring technology – such as encryption products and routers – which was based on point in time certificates. In the future we will take a principles-based approach to security functionality and put much more emphasis on proportionality and on the engineering practices of the developer, rather than running through a check-list of criteria that need to be met. This approach will be repeatable, evidence-based and, crucially, scalable, to ensure it delivers a real national level impact by creating a market that rewards those developers who invest in their security engineering.

Improving our resilience also plays a key role in deterring cyber attacks; our adversaries will see that an attack against the UK is likely to be less effective and the perceived benefits will be reduced.

To quote my colleague Ian Levy – who I'm sure many of you know well – "*we need to ensure that the dumb stuff doesn't work anymore and attackers need to try much, much harder, in a much more targeted way.*"

From this position of defensive strength, we will aim to deliver a more sustained, proactive and integrated campaign for disrupting and imposing costs on malicious actors, recognising the reality that cyberspace is now a domain of systemic competition and widespread criminal activity - including urgent threats such as ransomware. We are working to better integrate and deploy a wider range of levers, including our legal tools and powers, our diplomatic network, intelligence law enforcement, technical expertise, economic measures and of course our military capabilities. And, working, with the newly established National Cyber Force.

As well as being prepared to tackle the risks and threats as they emerge, we also need to actively shape the cyber environment of the future to avoid repeats of the situation the world found itself in on 5G, for example. This will require a more interventionist approach to technology, from Semiconductors to AI, from quantum computers to connected places. We need to foster and protect competitive advantage in the technologies critical to cyberspace and mitigate cyber risk at an earlier stage by ensuring security is designed into the digital economy of the future. And we need to do more to ensure that debates about technology and internet standards support our future security and prosperity.

We also need to take a more activist leadership role internationally, in line with the Integrated Review's objective of shaping the international order. So we at NCSC will work with the FCDO to put cyber power at the heart of the UK's foreign policy agenda, strengthening our collective security, ensuring our international commercial competitive advantage and shaping the debate on the future of cyberspace and the internet.

To underpin these efforts, we need to actively level up cyber capacity across the UK. We need to address the skills shortage across the cyber profession and our own workforce, increasing the diversity of talent we are able to draw on, and raising cyber and digital literacy across the general population.

Working with UK Research and Innovation, we have helped build a strong academic base in cyber security across the UK, we have seen the number of Academic Centres of Excellence in Cyber Security Research grow from nine to nineteen, and we have established four Research Institutes building capacity and research in critical areas of the field . We can capitalise on the foundation by building the regional ecosystem of cyber businesses, jobs, exports and innovation beyond London, capitalising on the existing strengths we have in the South West, Manchester and Belfast and stimulating new clusters of activity. Our ambition is that every organisation and household across the UK should derive some benefit from the UK's cyber power, empowering them to take advantage of the opportunities of new technology confidently and securely.

Conclusion

So, one year into my role at the NCSC, I am proud of the organisation I lead – the way we respond to incidents to reduce national harm, the deep technical expertise that we have and the dedication of every person within our mission to make the UK the safest place to live and work online.

I am also clear-eyed about the scale of the challenge we face. To simultaneously respond to incidents on a day-to-day basis while also building a model of improved security in the context of the dramatic growth in emerging technology. It will be difficult.

But I am also excited about meeting that challenge. The Integrated Review and the upcoming National Cyber Strategy gives us the framework we need to build a UK...

That is planning ahead.

That is building resilience.

That is growing the skills base.

That is engaged with our international partners.

And that is – ultimately – much more cyber secure.

Thank you.

PUBLISHED

11 October 2021

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals

DATE OF SPEECH

11 October 2021

LOCATION

Chatham House, London (virtual)