CYBERUK 2024: Anne Keast-Butler keynote speech

Anne Keast-Butler, Director GCHQ delivers the keynote speech at CYBERUK 2024, ICC, Birmingham.

Good morning and welcome to CYBERUK 2024.

I'm Anne, Director GCHQ, and I'm delighted to be here with you here in Birmingham, a hub for future tech in the UK.

This is my first CYBERUK as Director GCHQ and I want to start with a huge thank you to this community for making me so welcome.

It's been quite a year. And as the Prime Minister said yesterday, the next few years will be some of the most dangerous and transformational.

Putin continues to pursue his senseless and brutal invasion of Ukraine, Iran stokes instability and insecurity in the Middle East, and China is an ever more assertive power. And this all comes at a time of unprecedented acceleration of technology.

So, this morning, I will share with you the future threats that I see and how GCHQ and our partners can counter them.

I will start to explore how we can reap the benefits and manage the risks of future tech like generative AI.

And I will focus on why resilience and partnering better and faster than ever are crucial for us to be future ready.

Some great speakers, panels and events will then help us all get further into this over the next two days.

My starting point is cyber crime. Ransomware continues to be the most acute and pervasive cyber threat for UK businesses and organisations.

We're doing everything we can to counter it. Working with partners to detect criminal activities and degrade the Ransom as a Service ecosystem and produce intelligence that means those involved in ransomware are held to account.

Last week, the National Crime Agency unmasked the leader of the LockBit ransomware group, Russian national Dmitry Khoroshev.

A significant disruption, showing that there is no hiding place for cyber criminals, and a brilliant example of international partnerships.

Turning next to Russia. We are increasingly concerned about growing links between the Russian intelligence services and proxy groups to conduct cyber attacks – as well as suspected physical surveillance and sabotage operations.

Before, Russia simply created the right environments for these groups to operate but now they are nurturing and inspiring these non-state cyber actors and, in some cases, seemingly co-ordinating physical attacks against the West.

The Russia threat is acute and globally pervasive. It requires constant vigilance and collaboration to defeat it. We can see that Putin has not given up his maximalist goal of subjugating the population of Ukraine.

Which is why the UK's support will remain steadfast, for as long as it takes, because only through strength and partnership will Putin be deterred.

At GCHQ, we continue to strengthen Ukraine's cyber capabilities to share vital intelligence and expose Putin's malign plans and his increasing reliance on state – such as China and North Korea, and, of course, Iran, who continue to supply drones to Russia in return for money and military assistance.

On Iran, while we see little in the media about their online capabilities, they remain aggressive in cyberspace. Actors associated with the state have been implicated in attacks against victims in many countries.

And Iran is continuing to grow its cyber espionage expertise alongside a range of disruptive and destructive capabilities. Whilst they might not always use the most advanced capabilities to conduct their operations, they should not be underestimated.

Russia and Iran pose immediate threats, but China is the epoch-defining challenge.

The people of China and the Chinese community overseas have contributed greatly to life here in the UK. But recent events remind us that our country and democratic institutions remain of interest to the Chinese authorities.

We want to engage with China where it's mutually beneficial. Like tackling climate change, engaging in safe trade, and AI safety. It matters that China joined in signing the declaration on AI last November at Bletchley Park, the wartime home of GCHQ.

But as the Prime Minister said recently, the leadership of the People's Republic of China, the PRC, is increasingly working with others to try and reshape the world.

Responding to the scale and complexity of this challenge is GCHQ's top priority and we now devote more resource to China than any other single mission. Through their coercive and destabilising actions, the PRC poses a significant risk to international norms and values.

In cyberspace, we believe that the PRC's irresponsible actions weaken the security of the internet for all. China has built an advanced set of cyber capabilities and is taking advantage of a growing commercial ecosystem of hacking outfits and data brokers at its disposal.

China poses a genuine and increasing cyber risk to the UK.

The PRC is looking to shape global technology standards in its own favour, seeking to assert its dominance within the next 10 to 15 years.

Which is why the UK's intelligence community is working alongside our Five Eyes allies – and beyond – and also in partnership with industry and academic colleagues to deter and combat cyber threats from nation states and hostile actors.

We have repeatedly called out Chinese cyber adversaries for activities that threaten the security of the UK or target the institutions important to our society, such as the compromise of the UK Electoral Commission.

We do this on the basis of GCHQ's cyber security expertise within the NCSC and also our unique intelligence-based insights, which help to contextualise the threat so that you – every citizen, every business – can take action to protect your sensitive data, your systems, and your IP.

As the head of a world-leading tech organisation and as a mathematician, it's clear that technology and security are more tightly coupled than ever before. Collaboration across academia, the private and public sectors is crucial for developing cutting edge science and technology solutions for national security.

To quote the Foreign Secretary, who spoke at NCSC's headquarters in London last week: we need to forge partnerships to out-cooperate and out-innovate our adversaries. Because the world of communications is at a pivot point.

Quantum engineering is reshaping the future of computing, the next generation of advanced telecoms will make the world a global cloud of interconnectivity, and, right now, there are almost 10,000 satellites orbiting above us – which places new demands on the UK intelligence community for security and resilience.

This was unimaginable a decade ago. And it's clear that the technological transformations of the next decade will far exceed those of the last.
This is most evident with generative AI. These powerful systems are advancing at an exponential rate, outpacing the expectations of even those who lead their development.

When it comes to AI at GCHQ, we're focused on three things: using our unique expertise to help ensure security and safety are hardwired into AI development; understanding how our adversaries are using, or plan to use, AI to cause harm, and exploring how AI can help enhance our capabilities, make us better at keeping the country safe.

We're using AI across all parts of the intelligence and security cycle in support of our people – and in responsible and ethical ways.

We're leveraging AI advancements to bolster our protection against cyber threats.

And we're doing all of that as child sexual offenders are exploiting AI to create increasingly severe material, fraudsters are using AI to draft convincing phishing

emails, and others are using AI to enhance ransomware, infiltrate systems, spread disinformation, and erode trust in democratic institutions.

Which is why we're working with partners to identify and disrupt criminals abroad: using our intelligence to prevent many millions of pounds of fraud here in the UK and deploying cyber operations to remove child sexual abuse material.

Together, we stand as a robust line of defence against the misuse of AI.

And all of this comes in the year of elections, with 64 countries taking to the polls. I am proud that GCHQ is playing its part in the UK's Defending Democracy Taskforce and working with partners to ensure safe and secure elections.

Of course, none of our successes are possible without the best people, empowered and equipped with technology to help solve seemingly impossible challenges.

This needs the right mix of minds. I am the 17th Director of GCHQ but I'm also the first woman to hold this role in our 105-year history. You don't need to be a mathematician to be surprised by those numbers.

And all of us in the cyber industry, everyone in this room, has a part to play in building a diverse workforce. We need to attract more talent from ethnic minority backgrounds, and we need more women in science, technology, engineering, and maths.

So that we are better at solving the seemingly impossible. So that cyber security can work for everyone. And so that we are ready for the future. Looking round the room today how are we doing?

Alongside creating the right mix of minds, what else can we do to manage evolving threats in the face of technological change?

I see three key ingredients: resilience, partnerships, and speed.

Firstly: resilience. The complex set of infrastructure that support our communications, our utilities, our supply chains is fragile and vulnerable to disruption. From war in Ukraine to destabilising action in the Red Sea, we have all felt the economic shockwaves of conflict.

We need to work together to make our systems more resilient to threats – criminal or nation-state; we need to protect our sensitive data from falling into the wrong hands. True resilience is something in which we all have a stake and good cyber security matters more than ever.

The NCSC plays a leading role in improving this resilience, but we cannot do it alone. It must be a CEO and a boardroom priority: a collaborative effort between government and the private sector, especially where UK critical infrastructure is privately owned.

And that brings me onto partnerships. We need to work together – faster and ever more effectively.

In a moment you'll hear from Harry Coker, US Cyber Director, and Heather Adkins, Head of Google's Office of Cybersecurity Resilience – just two fantastic speakers that showcase the importance of collaboration with business and the strength of our international partnerships.

Our partnerships are our competitive edge. They are longstanding, steadfast, built on liberal values, freedom, and innovation. But we now need to increase our speed in matching problems with technological solutions and for engaging with all of you on tech development and scaling innovation effectively.

This has never been so important. Our future tech advantage rests on what we as a community do next. Thank you for playing your part.

PUBLISHED

14 May 2024

WRITTEN FOR

Small & medium sized organisations

Public sector

Large organisations

Cyber security professionals

DATE OF SPEECH

14 May 2024

LOCATION

ICC, Birmingham