Foreign Secretary speech to CYBERUK Conference

It is a pleasure to be here.

As you'll remember on this day, four years ago, computers across the NHS suddenly flashed up a red screen.

With an image of a padlock and the words: "oops, your files have been encrypted."

There was a demand for a bitcoin payment, and two countdown clocks. One for when the ransom demand would be doubled, and another for when the files would be permanently destroyed.

Staff were locked out of the computers they use to access records and book appointments.

They couldn't operate MRI scanners, blood-storage fridges, and even operating theatre equipment were knocked out.

This was the so-called WannaCry attack. A ransomware cryptoworm which targeted a flaw in the Windows operating system.

Now for those not familiar with the scale of the attack.

Computers and data across 48 NHS Trusts were held to ransom.

The assailants were hell bent on extorting money.

With no regard for the human cost.

If these people had actually turned up and mounted a physical attack like this in the real world, there would have been outrage with camera crews and public debate

But because it was online, we react differently.

Maybe it's because we cannot see or visualise those who were attacking the NHS.

But think about it for a moment.

In an age when there are three and half billion people on smartphones around the world.

When we go online to shop, bank and stay in touch with our friends and family.

When MRIs and other hospital equipment is computerised.

When your fridge can tell Asda that you're low on milk.

And when almost everything has a digital dimension.

At what point do we wake up and realise that online is a major part of the real world that we live in.

And that's why it's so vital that we adapt.

Of course, we need to seize the tremendous opportunities that the internet offers.

But we must also ensure that we treat the accompanying threats,

With the seriousness they deserve.

Now according to Harvard's Belfer Centre, the UK is already a top-3 global cyber power, alongside the US and China.

So as well as all the opportunities for economic growth and the wider emancipation if you like of the citizen we see online, I want to talk to you today about how we will continue growing our capabilities to defend the UK's interests online,

And, at the same time, how we will deliver our vision of being a leading responsible cyber power, working with our partners to shape cyberspace according to our values.

Now there is a common misconception that cyber power is all about people like Q in a bunker somewhere, coming up with the gizmos of the future.

The reality is that it is much much broader than that.

Sure, we need coders and computer scientists if we are to succeed.

But we also need a broader alliance of people involved including teachers and researchers, businessmen and women, and diplomats who understand how to make the best of the power of new technology.

We need the combination of resilient defences, offensive capabilities, and the global diplomatic clout which make up a modern cyber power.

And in the UK, that starts with our underlying comparative advantage in science and technology.

We've got a great foundation.

With less than 1% of the world's population, we have got more Nobel Prize winners than any other country outside the US, and 14% of the most cited research.

We have got 1 in 5 of the world's top universities.

We are home to leading medical research, including the Jenner Institute that

developed the Oxford AstraZeneca vaccine to tackle Covid.

By the way, the Jenner institute also led trials on the Ebola vaccine, which was funded by UK aid spending, and last month it developed a game-changing vaccine for malaria.

So we're good at this and it's not just a one off.

When it comes to business growth, the UK has the most tech unicorns in Europe.

And we are 4th in the Global Innovation Index, produced by Cornell University, INSEAD, and the World Intellectual Property Organization.

So, the point I am making is innovation is in our DNA.

And that's why the Integrated Review of Foreign policy identified science and technology as one of our great strengths, which we must nurture and reinforce in the years ahead.

It is vital for jobs and livelihoods.

And it is vital to the levelling-up agenda, right across the UK.

And London I think is well known as a magnet for tech start-ups.

But don't forget that Belfast is a world-leading cyber security hub, and a top international investment location for cyber security firms.

The tech sector is thriving across the whole of the United Kingdom.

So it's not just at home but in 2019 we exported cyber products and services worth £4 billion.

And just last week saw the successful stock market launch of Darktrace, which is a world leader in using AI to prevent cyber-attacks.

So UK tech creates jobs and protects our security.

But it is also helping us to be an even stronger force for good in the world.

Think of the difference that mobile phone banking has made across Africa and Asia. Boosting economic activity by giving millions of people access to the formal financial system.

People who otherwise wouldn't have been able access business and services.

It started back in 2003 with an R&D grant from British aid, and support for Vodafone to launch a mobile currency service to support micro-finance.

And that led to banking services like M-Pesa, which is now used by over 28 million people in East Africa.

For a woman in rural Kenya, toiling to support her family through subsistence

farming, M-Pesa has been a total game-changer.

It provides her with access to small loans and remittances from relatives.

It allows her to set up a business, whether a small kiosk or something that can scale up bigger.

It gives her and her family a ladder out of poverty.

And just to give a sense of scale

In Kenya alone, mobile money has helped around 185,000 women make this transition.

So, my starting point in this debate is that UK tech is a massive force for good.

But I do think we need to acknowledge there is a darker side.

The Integrated Review highlighted the increasingly competitive world we live in, and the clash of values that is playing out today between the countries that want to protect and preserve a system based on open and outward looking societies, and those on the other hand who are promoting an authoritarian international system.

We can see this clash between authoritarian and democratic states playing out very directly, right now, in cyberspace.

You've got authoritarian regimes including North Korea, Iran, Russia and China using digital tech to sabotage and steal, or to control and censor.

And perhaps we saw that most ruthlessly recently when the military junta shut down the internet in Myanmar.

So, how do we safeguard our vision of a free, open, peaceful and secure cyberspace?

One which emancipates the citizen through a world of new online opportunities, while at the same time striving to protect them from online predators, whether paedophiles, criminal gangs or hostile states?

Well First, I think it's important we need to understand the full spectrum of threats we face.

Let me just give you a flavour of the kind of malicious and dangerous activity that is happening all the time, although often it is out of the public's view.

This weekend, the largest pipeline in the US was knocked out by a criminal gang in the latest ransomware attack.

That pipeline, which runs from Texas to New York, transporting gasoline, diesel and jet fuel, provides 45% of the supply to the US East Coast.

So an outage like that threatens price spikes and shortages.

Very severe economic disruption.

And then again in March this year, Microsoft reported a cyber-attack on the Microsoft Exchange Server by a state-sponsored group operating out of China.

Now the Early indications as best as we can glean them show that at least 30,000 organisations were compromised in the US, and around 3,000 in the UK. Right from businesses to citizens.

These attacks can have global impacts beyond their initial target.

In 2017 the Russian military mounted the NotPetya cyber-attack on Ukraine. Now that was originally intended to hit the country's banks, its government, and its energy companies, but the impact spread rapidly, from New Jersey to New Zealand.

The world's largest shipping company went offline for a full week.

That meant in practical terms for people living their daily lives household goods, food and components destined for factories were stuck at the port.

The resulting chaos and delays caused over £7.5 billion in economic damage.

Now, of course, today one of the most valuable cyber targets is the Covid vaccination supply chain.

In July last year, we called out the Russian Intelligence Services for mounting cyber-attacks on vaccine developers.

It seems that almost nothing is off limits for cyber criminals.

As schools and universities prepared to re-start face-to-face teaching in March.

We found that around 80 different schools, colleges or universities were hit by ransomware attacks, forcing some to delay the return to the classroom.

So that's why we are working to help organisations across the UK from private sector to public sector to protect themselves.

But I'll come back to that point a little later on.

There's also a democratic element to the threats we face.

Elections are also a prime target.

Russian actors tried to interfere in the 2019 general election spreading lies online, taking aim squarely at British democracy.

The US Presidential Elections in 2016 and 2020 multiple cyber-attacks.

Let's put this in context in terms of scale

In the last year the National Cyber Security Centre dealt with 723 major cyber security incidents, that’s the highest figure since the NCSC was formed five years ago.

In total, last year, they stopped 700,000 online scams targeting the UK.

Now some of this activity is aimed at theft or extortion.

But it is all too often just focused on sabotage and disruption, and I think its worth saying these actors are the industrial-scale vandals of the twenty-first century.

But, that doesn’t mean it is random.

These hostile state actors and criminal gangs want to undermine the very foundations of our democracy.

And let’s be clear, when states like Russia have criminals or gangs operating from their territory they cannot hold up their hands and say not them but they have a responsibility to prosecute them, not shelter them.

These cyber-attacks pose a real risk on a daily basis,

Because what they really want is to undermine our confidence in doing simple things, like checking our bank balance or paying for a food order online.

So we’ve to adapt to that threat, not just to defence to defend our way of life.

Against that backdrop, let me set out three practical concrete ways in which we are upping our game.

First, we are building up our domestic defences.

I am particularly focused on this as Lindy said because I Chair the cross-Government Ministerial Group on Cyber.

We have already delivered a sustained programme of investment through GCHQ and the National Cyber Security Centre to establish the UK as a global leader in cyber.

We are expanding the NCSC’s Active Cyber Defence services.

So for example by taking down malicious sites and helping the public sector to increase their email and website security.

But we’re not just reinforcing resilience around the government.

We are helping everyone from businesses to families to take the basic, necessary steps to stay safe online.

Some of it is relatively simple but essential stuff.

Helping people to create strong passwords, turning on two-factor

authentication, updating our devices and backing up data.

These are the basic bread and butter things we can do to keep ourselves safe

The NCSC does great work getting businesses to do this kind of due diligence, helping them to defend themselves.

They helped over 23,000 companies in the last 12 months.

Over a million companies have accessed NCSC advice on staying safe online,

Advice like giving boards the information they need to understand their cyber risk,

Right the way to providing detailed technical advice for Chief Information Security Officers on how to configure their operating systems.

And just yesterday this conference heard about the NCSC's new Early Warning System which will help alert businesses and other organisations to potential cyber attacks

So, we are working to improve resilience across Government and across society.

Yesterday, the Queen's Speech announced legislation to protect consumers from the harms associated with cyber-attacks on things like smartphones, smart TVs, cameras and speakers.

So there's a huge effort going into this. Although it is a diverse threat, and our approach is working.

We are getting better at detecting, disrupting and deterring our enemies.

Acting with our partners around the world, we name and shame the perpetrators.

We did this last month with the SolarWinds attack, Exposing the depth and breadth of the cyber activities conducted by Russia's intelligence service, the SVR.

And by revealing the tools and techniques that malicious cyber actors are using, we can help our citizens and businesses to see the signs and that will help them protect themselves from the threats.

I want to be clear about the time period.

This is going to be a marathon.

It is a war of attrition.

And we will keep relentlessly shining a light on these predatory activities.

This brings me to my second point. We are also building up our offensive cyber capabilities.

We're not just going to guard against attacks, we are going to target and impose costs on those who are taking aim at us.

So last year we established the National Cyber Force, bringing together defence and intelligence capabilities under one unified command for the first time.

The NCF conducts targeted offensive cyber operations to support the UK's national security priorities.

We don't talk much about our capabilities here for obvious reasons.

But this technology can prevent the internet from being used as a platform for serious crimes.

For example by denying access to a particular part of a criminal gang's infrastructure or undermining their network.

We can use it in military operations, we did it in Iraq during the Battle of Mosul,

To disrupt Daesh's battlefield communications,

Which helped coalition forces to take ISIL fighters by surprise.

Then again in Syria, we also impaired the ability of Daesh to produce and spread their poisonous propaganda.

And so we will continue to use these capabilities where necessary in a proportionate way, and in line with international law.

Because, ultimately, the difference between us and our adversaries isn't just about our capabilities.

It's about how we choose to use them.

Here in the UK and amongst our partners we insist on democratic oversight and accountability.

We demonstrate respect for international law.

And we use our capabilities to defend our citizens, to safeguard international collaboration as a force for good in the world.

Whereas our adversaries use their cyber power to steal, to sabotage and to ransack the international system.

And that brings me to my third point which is how we are working with like-minded partners,

To make sure that the international order that governs cyber is fit for purpose.

Our aim should be to create a cyberspace that is free, open, peaceful and

secure, and which benefits all countries and all people.

We want to see international law respected in cyberspace, just as we would anywhere else.

And we need to show how the rules apply to these changes in technology.

The changes in threats, and the systematic attempts to render the internet a lawless space.

Hostile states using cyber to warp a democratically held election that violates international law.

Governments and gangs using cyber to paralyse another country's healthcare system that violates international law.

So our challenge is to clarify how those rules apply, how they are enforced, and guard against authoritarian regimes bending the principles to meet their own malicious ends.

Now we've been at this a while.

Ten years ago, the UK government brought together in London more than 60 countries,

To try and establish principles for governing behaviour in cyberspace.

Basic principles like universal access to the internet, and protecting individual rights online.

It was a good point of departure, but only a point of departure. You have to start somewhere.

Today, as you would expect, we are working closely with traditional partners like the 5 Eyes and in NATO.

But here we are also seeking to bridge old geopolitical dividing lines, between the West and the G77, the Global North and the Global South.

Last month the UN General Assembly unanimously agreed a set of voluntary principles for how states should behave in cyberspace, including things like the importance of protecting health infrastructure.

So that was another important stepping stone.

But we want this to lead to a wider agreement on how to respond to those states who systematically commit malicious cyber-attacks.

Now here in London last week, we had a good conversation about these issues at the G7 meeting of foreign ministers.

And it wasn't just the usual G7 group.

We invited ministers to join the meeting from India, Australia, South Korea,

South Africa and Brunei, the current ASEAN chair.

Because we wanted to broaden the group of like-minded countries cooperating on cyber.

We have got to win hearts and minds across the world for our positive vision of cyberspace as a free space, open to all responsible users and there for the benefit of the whole world.

And frankly, we've got to prevent China, Russia and others from filling the multilateral vacuum.

That means doing a lot more to support the poorest and most vulnerable countries.

So today I am very pleased to announce that the UK government will invest £22 million in new funding to support cyber capacity building in those vulnerable countries particularly in Africa and the Indo-Pacific.

And that money will go to supporting national cyber response teams.

Advising on mass online safety awareness campaigns.

And collaborating with Interpol to set up a new cyber Operations hub in Africa.

The idea of that will be to improve co-operation on cybercrime investigations, and support the countries involved to mount joint operations.

So my perspective, at least from a diplomatic point of view, is that as Global Britain we must be agile and work with new partners.

So just take ASEAN, the Association of South East Asian Nations, a good example

It's a leader in this field, with the ASEAN-Singapore Cybersecurity Centre of Excellence which is working to build capacity across the region.

And this is a good example of the cooperation that we can really intensify, really energise, now that ASEAN leaders have signalled they accept the UK's application to become a formal Dialogue Partner later this year.

So, to sum this all up.

The threats we face from reckless cyber-attacks, like NotPetya, or the attacks on our NHS, and on our democracy, are all too real.

But at the same time we should also be confident, even optimistic about what lies ahead.

Because we can grasp the opportunities the internet presents today.

And, protect those at risk from the online predators.

We can lead internationally in protecting the most vulnerable countries, and at the same time bring together a wider coalition of countries to shape international rules that serve the common good.

And Britain has a real comparative advantage in this space.

We've got the world-beating coders and scientists, the Ground-breaking innovators.

And, at the same time, from GCHQ to the NCSC to the National Cyber Force, we have the capacity to defend our liberties at home,

And protect the world's online freedoms from those who would poison the well.

And that's our mission as Global Britain, to flourish as a tech superpower.

And to serve as an even stronger force for good in the world.

Thank you.