Beat: Technology

Cyber UK 2018

Directors speech

Manchester, 13.04.2018, 14:20 Time

USPA NEWS - At CYBERUK 2018, the Government's flagship event for cyber security in the UK, Director of GCHQ, Jeremy Fleming, gave his first public speech since taking office last year. The speech covered: How our adversaries are proactively using technology to further their cause; How what we face constantly changes and becomes more complex; and How GCHQ is changing operationally, technologically, and culturally, to keep our country safe. To illustrate that, the Director explained some of the operational steps that GCHQ has taken in recent years, the impact working in partnership has, and the steps we are taking to recruit the type of people that we need to succeed now and in the future.

Speech at CyberUK18
Director GCHQ

Good morning, I´m delighted to welcome you all to Manchester this morning to the UK´s premier cyber security showcase, CyberUK2018.

This is my first CyberUK and my first public speech as Director GCHQ.
It´s great to be back in Manchester.
I´m sure we can all recall the moment when we realised that this brilliant City, known for its tolerance and inclusivity, was attacked by someone who had neither.
I´d like to pay tribute to the first responders that night. I´m hugely proud too of the way GCHQ responded in the days and weeks after. The pressure was intense as we worked with the Police and MI5. The hours were long. It was even harder for those with family and friends close to the tragic events.
And in that difficult time, we drew strength from the togetherness and resilience shown by all of Manchester´s communities.

That´s how you tackle terrorism.
Today is my first opportunity to talk publically about the way the threats we face are developing and how we must respond.
For the majority of my working life I´ve not been in public facing roles"¦up until I joined GCHQ last year, I´d been an MI5 officer for nearly 25 years.
During that period I was part of a fantastic team tackling some of the UK´s toughest security challenges: Northern Ireland, Al Qaeda inspired terrorism, old and new counter espionage, securing the London Olympics; and the rise of Daesh in Syria and Iraq.
And I´m now honoured to be leading GCHQ as it enters its 100th year. It´s an incredible history full of amazing intelligence and security breakthroughs, of improbable ingenuity and innovation.

Above all, it´s a history of amazing people working hard to keep us all safe. I´m clear that it´s their brilliant work, the quality of our people, that defines us today.
They know we´re involved in a race to make sure we´re relevant in the cyber age, and to keep up with the threat.
I´ve seen the impressive way they respond to this challenge at close quarters, over many years.

And now I´m in GCHQ I feel even more strongly how central what we do is to the nation´s security. It´s both an exhilarating and humbling responsibility to lead them as we enter our second century. And, I give them heartfelt thanks for everything they do. Which brings me to CyberUK. This is only the third year we have held the Conference, but already it has become
the UK´s pre-eminent Cyber leadership event.

It´s a great privilege to be here, to be able to feel the energy in the room, the buzz that comes from solving security problems, and the creativity of all of you present.
These are qualities I see in GCHQ every day. They´re a key part of our counter terrorism and our serious crime missions, of our work supporting the military and in tackling the threat from hostile states. They´re also key to our cyber security mission. Protecting the UK´s critical information has always been an essential part of what we do in GCHQ; and in this cyber age it has never been more important.

I´d like to thank the whole NCSC team for putting on such an excellent event.
Today I´m going to talk about the way in which the threats we face are developing and how we´re approaching this challenge.

´ll talk about what we´re doing to take the terrorism fight online"¦how our adversaries are becoming more tech savvy"¦and how we in GCHQ are responding, operationally, technologically, and culturally, to keep up.
But to set all that in context, I want to start by explaining how the broader technology and threat picture is changing.
THE WORLD WE OPERATE IN
Thankfully, I´ve always been an optimist where technology is concerned.
I didn´t fear Azimov´s three rules of robotics. The threat of Skynet taking over. Or the menacing voice of HAL.
Like many of my staff, I like to see the wider societal promise in technology not the threat.
That said, the pace of breakthroughs today is truly unrelenting"¦Moore´s Law shows no sign of being repealed.

Things previously unimaginable are already commonplace. Ten years ago, the tablet didn´t even exist. It wasn´t missing from our range of smart devices, it came to life in a big-bang style. It´s changed the way we shop, interact, create art "" live.
Scanning the horizon, there´s so much to excite us. The idea of hyper connectivity "" the internet of things expanding our networks "¦making the links and activity within them intuitive, instantaneous.

The power of analytics to improve social services and transform healthcare.

The benefit of playing games "" for example using Pokemon Go to break down intimidating social barriers for children with autism.
The use of Augmented Reality, to make the scary .... familiar. Imagine helping your child to find their way around a hospital in advance of a visit.

And, over the next 18 months, 5G really is coming. We can already see how it will change app development. How it will alter irreversibly the speed at which we can connect with the world.
Of course, there are dangers and pitfalls in this progress. We must look for equality in this digital revolution. There´s a widening gulf between the capacity for connectivity in rural areas and cities. And 5G, in all its glory, will come at a price that will be beyond many.
That´s the subject for another time, but I know our colleagues in the Department for Digital, Culture, Media and Sport are working hard to make sure that no one is left behind.
In my world, these huge strides have both enabled what we do and made the business of intelligence and security much harder.
Hostile states, terrorists and criminals are emboldened and assisted by technology. They´re early adopters of new products and services, investing heavily in strategies and tactics to further their causes.

You only have to examine the investment some States are making in the development and use of cyber tools to disrupt, steal, and intimidate.
And at a smaller scale how Al Qaeda and Daesh have used online platforms to spread propaganda.
The way that criminal groups have built massive online spoofing schemes to line their own pockets at the expense of thousands of people up and down the country.
And at how paedophiles use both the Dark and Open parts of the Web.
They´re all exploiting developments that in many cases have been designed to make data and users safer. Whether

it´s tools that anonymise use“¦ obscure locations“¦or even popular platforms offering end-to-end encryption“¦their hijacking by criminals is something that we work hard to combat.
And encryption is of course a vital cornerstone of the internet. However, it is clear that our adversaries take advantage of these positive features to pursue their damaging and criminal ends.

Alongside these new dangers, we must not and have not forgotten the old foes.
For decades, we have collected intelligence on Russian state capabilities, on their intent and on their posture. And for over twenty years, we´ve monitored and countered the growing cyber threat they pose to the UK and our allies.
This has never gone away. But nevertheless, recent events are particularly stark and shocking.
You´ve heard it said, and I´ll repeat, the attack on Sergei and Yulia Skripal in Salisbury, was the first time a nerve agent has been deployed in Europe since the Second World War.
That´s sobering. It demonstrates how reckless Russia is prepared to be. How little the Kremlin cares for the international rules-based order. How comfortable they are at putting ordinary lives at risk.

The robust response from the UK and from the international community shows the Kremlin that illegal acts have consequences.
And it looks like our expertise on Russia will be in increasing demand. We´ll continue to expose Russia´s unacceptable cyber behaviour, so they´re held accountable for what they do, and to help Government and industry protect themselves.
The UK will continue to respond to malicious cyber activity in conjunction with international partners such as the United States. We will attribute where we can.
And whilst we face an emboldened Russia, we also see the tectonic plates in the Middle East moving. We see Iran and its proxies meddling throughout the region. The use of Chemical Weapons in Syria. We´re watching the dispersal of Daesh fighters. Serious Crime Gangs smuggling people from Eastern Europe and Northern Africa.

I know I´ve painted a dark picture with that summary. Of course, it´s not all doom and gloom.
The last 50 years has seen huge progress in the eradication of disease, the spread of knowledge and freedom, and the prevention of conflict. The last decade has witnessed technology transform the way we live. There´s much, much more to come.
Even so, I think we can all appreciate the current threat landscape is both difficult and fast moving.
CHANGING THREATS “‘ THE ON-LINE FIGHT AGAINST TERRORISTS
To deal with these challenges we know we have to do things differently. In particular, we must take more active steps to counter those who misuse the power of the internet and of modern communications.
Our work against Daesh is a great example.

We´ve seen the very deliberate way it devoted so much time and energy to technology, to the creation of media content.

They understand the value of strategic communications, the power of social media, of messaging apps to radicalise and scare. They do this better than any previous terrorist group.
What they also understand, is their audience. They know potential sympathisers react well to slickly produced, unfiltered videos and magazines that can be downloaded and watched on smartphones. And they know which platforms to use to reach them.
In recent years we´ve seen the impact of this approach all over Europe. And last year it came to our shores too with attacks in London and here in Manchester.
Daesh´s ability to inspire, direct and enable attacks, and the simple tactics they use make stopping attacks much, much harder. But the UK´s CT team “‘ led by MI5 and the Police, supported by GCHQ, MI6 and the Military “‘ is evolving fast to match this threat.

For GCHQ, this expansion of the terror threat means more investment in our people and our capabilities. Closer working with other CT partners here and overseas and greater sharing of our information to improve the threat radar.

But it´s also brought a sharper focus on fighting Daesh online.

For well over a decade, starting in the conflict in Afghanistan, GCHQ has pioneered the development and use of offensive cyber techniques. And by that I mean taking action online that has direct real world impact.
In recent years, we´ve worked closely with the Ministry of Defence and key allies to grow these capabilities at pace.
Much of this is too sensitive to talk about, but I can tell you that GCHQ, in partnership with the Ministry of Defence, has conducted a major offensive cyber campaign against Daesh.

These operations have made a significant contribution to coalition efforts to suppress Daesh propaganda, hindered their ability to coordinate attacks, and protected coalition forces on the battlefield.
But cyber is only one part of the wider international response.

This is the first time the UK has systematically and
persistently degraded an adversary´s online efforts as part of a wider military campaign.
Did it work? I think it did.

The outcomes of these operations are wide ranging. We may look to deny service, disrupt a specific on-line activity, deter an individual or a group, or perhaps even destroy equipment and networks.
In 2017 there were times when Daesh found it almost impossible to spread their hate online, to use their normal channels to spread their rhetoric, or trust their publications.
Of course, the job is never done "" they will continue to evade and re-invent. But this campaign shows how targeted and effective offensive cyber can be.

And when you add this to the increased efforts CSPs have put into removing Daesh material over the past year, you begin to understand the scale and resolve of the international effort to stop them.
It worked against Daesh and it can work against other national security challenges too.

We know that these capabilities are very powerful. The international doctrine governing their use is still evolving.

And as with all of our work we only use them in line with domestic and international law, when our tests of necessity and proportionality have been satisfied, and with all the usual oversight in place.
Speculation to the contrary fails to understand the true values of my organisation, our military, and this country.
The fight against Daesh is not over. They continue to seek to carry out or inspire further attacks, including here in the UK.

We know they´re already seeking new ungoverned spaces to base their operations. Other terrorist groups will doubtless pick up their techniques "" unfortunately, their legacy is likely to be online.
And this technical savviness, this understanding of the potential of cyber capabilities extends way beyond terrorist groups.

The other protagonists are equally familiar - hostile states, and criminal gangs. They´re also using the enabling power that the internet and modern communications provides to spread their ideology and to peddle their lies.
And the harm they cause is on a much larger scale.

CYBER "" A CHANGING AND MORE COMPLEX THREAT
We´re seeing criminal gangs using malware such as Zeus and Trickbot, or ransom ware like Locky and Bitpaymer to make millions of pounds in the UK and around the world.
The attack and the attackers don´t care about the size or sector of their victim "" they thrive on the anonymity of the internet to demand payment in cryptocurrencies.
Of course, cyber-crime is not limited to financial gain "" they also go after the individuals.
Paedophiles and sex offenders are using all corners of the open and Dark Web to stream abuse, share images or boast on message boards.
The latest threat assessment by the WeProtect Global Alliance said - and I quote - 'technology is enabling offender communities to attain unprecedented levels of organisation, creating new and persistent threats´, so sadly we know the problem is here to stay.
Although the prevention of child sexual exploitation is a relatively new part of our mission, it´s an unrivalled duty

to use our skills, alongside the National Crime Agency and other partners to protect children online. Recent prosecutions are showing GCHQ can really make a difference in this space.

And yesterday you heard the Home Secretary set out the next stage of the Government´s campaign against cyber crime, including of this most pernicious sort. We look forward to supporting that endeavour and working with our partners to deliver it.
Hostile nation-states are rapidly building and enhancing their cyber tools to stay ahead in the global race.
Whether it´s stealing another government´s secrets or the IP from a defence contractor"¦some states are willing (and very able) to do it.
The Russian Government is widely using its cyber capability.
Whether that´s NotPetya against the Ukraine´s financial, energy and government sectors, which eventually spread across the world. Or the use of industrial scale disinformation to sway public opinion.

They´re not playing to the same rules"¦ they're blurring the boundaries between criminal and state activity.

And they´re not alone.

We´ve seen state-sponsored hackers conducting cyber-attacks to avoid sanctions "" the release of WannaCry by North Korean cyber actors last year, is a great example of that.
Some of their malware tools are highly complex, using extensive infrastructure and advanced tradecraft. And we track these criminals and nation-states evolving quickly to respond to new defences.
But most cyber threats are not that sophisticated.

Even the best-equipped actors will use simple tools and techniques if they work. This means that implementing basic cyber security practices remains the best way to tackle the majority of cyber threats.
But we think there are strategic level approaches that can make a real difference too. These are proactive strategies, not reactive ones. A great example is the NCSC´s Active Cyber Defence programme. This aims to remove the threats before they get to their victims.

Just last week, our new DNS filtering service blocked access to more than 2,000 malicious domains, protecting users of Government networks, and therefore the Government, from harm.
Despite these approaches, we know that we will never stop everything. So a crucial part of our ambition is to improve the nation´s ability to respond to a cyber attack. The creation of the NCSC provides a central focus for this work "" last year it responded to over 800 incidents, much more than we expected when we set up 18 months ago.
Thankfully, none of these have yet been of the highest level of seriousness. But as we´ve said all along, it´s only a matter of time.

So to be ready we continually test and exercise our cyber capabilities in the same way that our Emergency Services do.
For the last few years, the UK has conducted a national cyber security exercise, Cyber Warrior, to do just that.

It brings together knowledge and expertise on both offensive and defensive capabilities. It has provided the MoD, GCHQ and Government with crucial practice and understanding of how to deploy cyber capabilities into real world situations if, when, they are required.
I´ve gone into this in some detail because I want to demonstrate how cyber has created a new threat landscape "" both for the attackers and defenders.
To stay ahead, to match the pace of technological change, we are investing in deploying our own cyber tool kit.
It´s one that combines offensive and defensive cyber capabilities, to make the UK harder to attack, better organised to respond when we are, and able to push back if we must.

In short, cyber has become an indispensable part of modern national security statecraft, and the cyber security element of it critical to organisations of all sizes in all sectors.
The UK cannot face this threat alone. Across all of GCHQ´s work, partnerships are critical to success. The fast changing world of cyber security is driving us to build new relationships and work in different ways.

The impact of technology and the opportunities it offers is also transforming our deep and longstanding work with the other agencies, the NCA, and with the MoD.

PARTNERSHIPS

Success in our world has to be a team game.

The challenges we face do not respect or recognise borders "" they are truly shared, and that requires a joined up response.

Whether that´s working closely with MI5 and law enforcement in the UK, with MI6 overseas, with our allies in Europe now and after we leave the EU"¦or with NATO as the joint cyber mission grows "" we have to work together.

Our relationship with 5EYES partners "" after 75 years "" remains as important and relevant today as ever before.

And relations with industry, academia and other parts of the public sector are growing as we invest time and effort. Programmes like the NCSC´s Industry 100 scheme are good for all sides. And we´re looking for other ideas and ways to build these partnerships further.

All of this is underpinned by trust"¦and by the sharing of knowledge and capabilities.

We want to do this because we know that Governments alone will never have all the answers.

It´s the only way of actually getting ahead of the threat.

The realities of this way of working mean that we in GCHQ need to develop new skills and a more diverse workforce.

Most leaders of big organisations will have said something similar. But for GCHQ it´s baked into our history and I´m clear that it´s critical to our future.

Our first Head, Commander Alistair Denniston sought to create an environment where the disparate talents of individuals could be harnessed for a common goal.

As the Second World War approached, he knew that he didn´t just need engineers. He needed people who could conceptualise and implement new methods of producing intelligence. The success of that approach probably changed the outcome of the war.

DIVERSITY

The same need - to seek out diversity of talent, to recruit and retain the best minds "" is as true today as it was then.

And the truth is that whilst the lure of keeping the UK safe is appealing to a lot of people, we don´t always do enough to make a career accessible to everyone who could contribute to our mission.

The reasons for this are numerous. We´ve made great strides and I´m proud of the way some of our campaigns have received public recognition. But I know we to do better: we need to offer more flexible careers, where individuals can more easily work at
lower levels of classification, can pursue their interests in the private sector and can bring the best of that back into GCHQ.

This means changing the perception of a career in the intelligence community so that more men and women from every part of society can imagine themselves thriving in the intelligence and security world.

Yes, for some of our roles we´ll continue to need those with a Doctorate in Mathematics or Computer Science, but we also need people straight from school or those who want a career change. People who can lead and make decisions. People who can work in teams and support and celebrate the success of others. People who can be role models and mentors. People who know technology or languages. And people who can spot patterns.

The one quality we ask for in everyone is a commitment to keeping the UK safe.

And because of the challenges we face, we´re continuing to grow. We´re recruiting across our national network, including in London, Bude, Scarborough, and now here in Manchester.

You´ll have heard yesterday´s announcement, and I´m delighted that we´re opening a new site in this City. It will create hundreds of high calibre jobs for people who will have a vital role in keeping this country safe.

It´s going to open up a huge new pool of highly talented, tech savvy recruits vital to our future success.
It will also help us build on the work we´re doing across the country to reach out to minority communities to explain who we are and what we do. Events like those under the banner of Decoded, are showing that when we invite applicants from minority communities to meet our workforce and learn more about our organisation, they´re more likely to apply.
This responsibility to get the best and most diverse minds into GCHQ extends beyond our organisation.

Our people are also playing an important role in raising the national level of STEM skills, the understanding of Science, Technology, of Engineering and Maths that is crucial to our nation´s future, and an especially critical skill to GCHQ.

Last year, nearly 2000 students aged between 11-17 took part in our free CyberFirst Courses. Encouragingly, 44% of them were female. It´s the tip of the iceberg, but this is progress.
I´d like to pay tribute to the CyberFirst team. What they´re doing is incredible. I´ve met many of these young people and it´s inspiring to see the potential and enthusiasm of these leaders of tomorrow. Some of them are already opting for a career in intelligence. They understand the heavy responsibility of keeping the country safe, of protecting our liberal democracy.

OVERSIGHT & TRANSPARENCY
They also understand that to do the extraordinary things we do, to be able to exercise the formidable powers at the Government´s disposal, requires strong laws, oversight and transparency.

This was enhanced last year with the passing of the Investigatory Powers Act. We will soon have 15 senior members of the judiciary exercising their “˜double lock´ powers “ at the same time as a senior Minister - in authorising operations.
And we´re already seeing strengthened oversight from the new Investigatory Powers Commissioner, alongside the existing Parliamentary scrutiny of the Intelligence and Security Committee.

And I welcome their scrutiny. As Parliament has directed, we need it to ensure that in the coming years we have a valid licence to operate.
As good as these arrangements are “ and I believe they really are world leading “ I´m convinced there is a supporting responsibility on us, on me, to be as transparent as possible, to explain as much as we can to the wider public without jeopardising our core mission.
Just look at this event, at the way the NCSC works, at the way we recruit staff, at the way the Agency Heads are involved in public debate. All of this was unimaginable when I joined 25 years ago. And we are committed to doing more.

CONCLUSION
So for me, in all that I have said, today is about continuing that openness, and of giving you a flavour of the world we operate in.

The challenges we face are vast. I think I´ve set out the significant changes in the threats the UK faces and which GCHQ exists to combat. And the ever faster and more diverse rate of technology change that we must understand if we are to be successful.
But, I hope I have also given you a sense of the breadth of excellence and expertise that we can call upon to meet these challenges.

Whether that´s within GCHQ, with our vital intelligence and military partners, and with law enforcement partners here and overseas, or with all of you in the wider public and private sector.
We´re building a strong and confident GCHQ. It´s transparent and open when it can be. It always acts lawfully. It´s committed to attracting and developing the most diverse workforce. And it´s using cutting edge technology and technologists, to meet the challenges the second century of our service to this country will bring.
It is an incredibly energising place to be.

Thank you

Article online:
https://www.uspa24.com/bericht-13106/cyber-uk-2018.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Daren Frankish - Cyber UK

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Daren Frankish - Cyber UK

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619