Beat: Technology

Securing the next generation of technology

Director GCHQ

Cheltenham, 14.08.2018, 16:34 Time

USPA NEWS - Director GCHQ writes about the importance of securing the next generation of technology. In an opinion piece for the Sunday Times in August 2018, Jeremy Fleming underlines the importance of partnerships in the new digital age.

Jeremy Fleming, Director GCHQ, August 2018

We have entered a new technological age, one that will fundamentally change the way we live, work and interact with each other. This new digital landscape will transform lives and economies as data analysis, artificial intelligence, 5G, the internet of things, quantum computing and many other technologies still being developed permeate all areas of human endeavour.

These changes will bring huge benefits to us all. They will transform healthcare, create smart, energy-efficient cities, make work lives more productive and revolutionise the relationship between business and the consumer. But they also bring risks that, if unchecked, could make us more vulnerable to terrorists, hostile states and serious criminals.Getting the balance right requires new partnerships and different ways of working at a global level.

The key to securing the benefits of this new age lies in the way in which we secure personal information and new technologies from those seeking to do us harm. In the past we have often seen security bolted on to technology as new risks emerge. For an environment where the cycle of development to deployment is accelerating and where our dependence on overseas technologies is increasing, this approach no longer works.

New systems - and their supply chains - need security built into the earliest stages of design if we are to protect liberties, ensure public confidence and counter threats to internet freedom.

GCHQ has always played a prominent role in this space. Now it is the mission of the National Cyber Security Centre (NCSC) - part of GCHQ - to make the UK the safest place to live and do business online.

This is an enormous challenge, but less than two years after its formation we can already see how its leadership role is making a difference to the cyber-health of the nation. Since the NCSC's inception we have been critical in responding to and reducing the harm from more than 1,000 cyber-attacks against the UK.

It is also increasingly clear that as the world becomes ever-more networked, we need to work even harder with businesses, technology companies, academia and privacy groups to protect the public from real-world and online harm.

We need honest, mature conversations about the impact that new technologies could have on society. This needs to happen while systems are being developed, not afterwards. And in doing so we must ensure that we protect our right to privacy and maximise the tremendous upsides inherent in the digital revolution.

This isn't easy. However, I can see it taking shape in some key areas. There is already an important public debate about the exceptional circumstances when law enforcement and the intelligence services should access encrypted communications - something we know has potential technical solutions in most cases.

We believe some principles allowing industry and governments to demonstrate responsible access that protects privacy are within reach.

These do not require unfettered access for governments through so-called "back door" or global "skeleton key" schemes. But they do require public debate and close, open co-operation and agreement with technology companies. And when these solutions exist, they also require modern legislation and strong oversight to maintain public confidence.

We now have that in the UK where the Investigatory Powers Act is world leading in the oversight of exceptional access requests, with legal authorisations jointly signed by a secretary of state and an independent judge.

For this kind of approach to succeed we must work more closely with partners - not just here in the UK, but across Europe and the globe. We and our allies all face the same challenges.

The globalisation of technology is here and we need to learn to deal with it. Critical technologies - for example, in 5G - are increasingly likely to come from China. The British government recently published its national security and investment white paper on foreign direct investment into the UK and we are looking at how we can better manage supply to our critical national infrastructure (CNI).

We must ensure that processes represent industry best practice so as to avoid real risk to the UK's CNI. We need to consider early, robust and fair solutions to the global challenge of balancing investment, trade and security.

Just as our adversaries are not constrained by international boundaries, we must make sure that our legislative and technology arrangements are able to keep pace. The ability for countries with strong privacy protection such as the UK to request a user's data held by US communication companies on serious criminal and terrorism grounds - the Cloud Act - is an excellent example of what is possible.

This is just one step towards agile security. As a nation, there is still much to be done to respond to the challenges to come. Stepping up to that responsibility, GCHQ will continue to build on our world-class understanding of technology to inform government policy and protect the UK. And we will continue to harness the nation's full diversity of thought and talent and demonstrate the kind of ingenuity that has defined GCHQ and our people for almost 100 years.

By working with partners - both here and abroad - we can be prepared for the unparalleled opportunities that the new data-driven world will bring.

News article - 12 August 2018

Director GCHQ, Jeremy Fleming, writes about the unparalleled opportunities and challenges we face as the world becomes ever more digitally connected. With the globalisation of technology, he explains how GCHQ will continue to work with businesses, technology companies, academia, and privacy groups, to protect the public from real-world and online harm.

Originally published in The Sunday Times on 12 August 2018.

Article online:
https://www.uspa24.com/bericht-13968/securing-the-next-generation-of-technology.html

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

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 - GCHQ

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