National Cyber
Security Centre
a part of GCHQ

The launch of the National Cyber Security Centre

A snapshot of the past, present and future of cyber security

The launch of the National Cyber Security Centre

On 14 February 2017, the National Cyber Security Centre (NCSC) was officially opened by Her Majesty The Queen.

This report is intended as a snapshot in time that dives into the past, present and future of cyber security in the UK rather than a comprehensive testimony of the work that we will do.

By learning from yesterday's lessons, we are providing today's invaluable online protection and moulding tomorrow's digital prosperity.

Past

- We are a new organisation, but our creation has not come from a sudden overnight rush of cyber awakening. Over the last century, many milestones – including numerous ones heavily influenced by our parent organisation GCHQ – have brought us to this point, and we must prepare for many more changes.

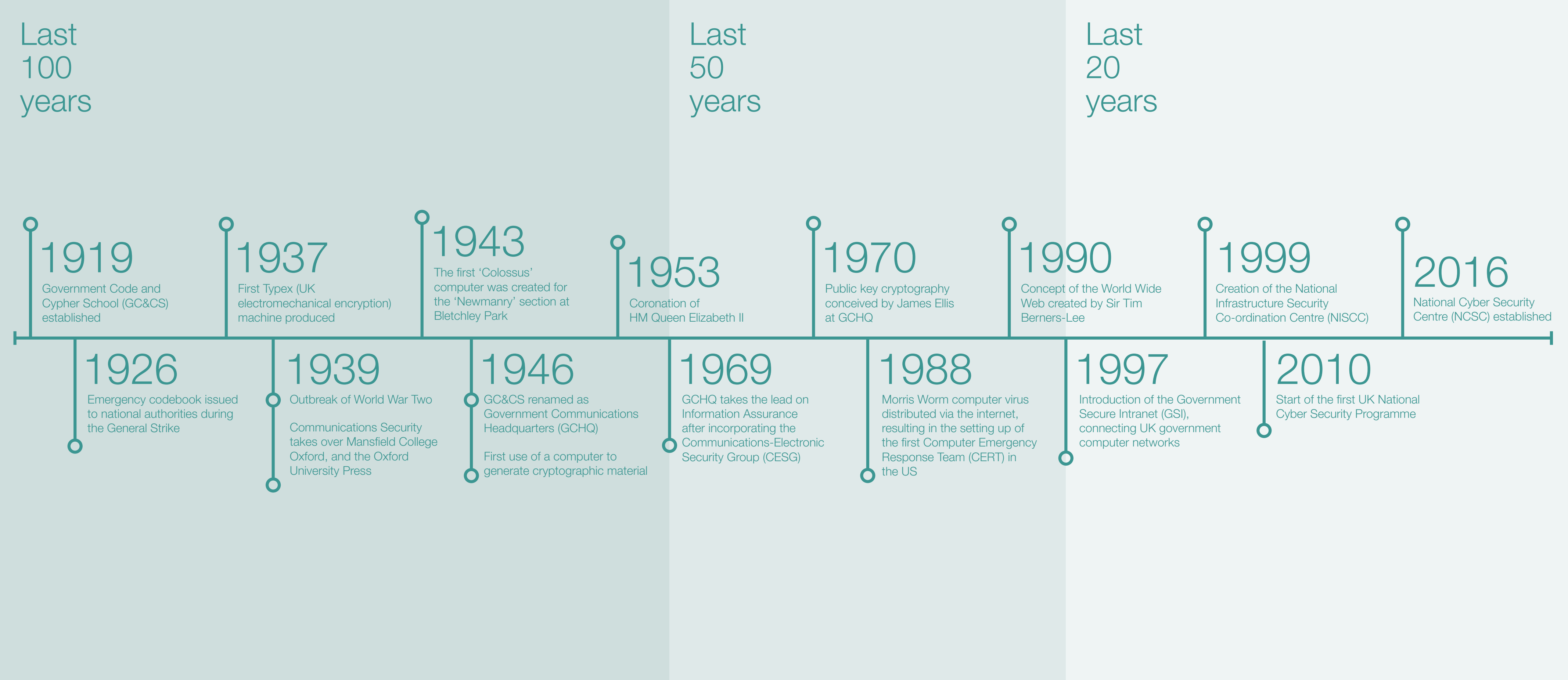
- The volume of telecommunications has increased significantly in the last 100 years, and has been accompanied by a huge rise in public awareness of the importance of staying protected.

- However, government awareness of the pressing need to stay protected has been around for centuries, with National Archive examples from as far back as the 16th century of encrypted official dispatches, particularly those being sent to and from diplomats.

- This spirit was intensified in the 20th and 21st centuries, with many technological developments coming from Bletchley Park and beyond that helped to create the current booming digital economy in the UK.

Past

Cyber events that moulded the last century



Last 100 years

1919 Government Code and Cypher School (GC&CS) established

1926 Emergency codebook issued to national authorities during the General Strike

1937 First Typex (UK electromechanical encryption) machine produced

1939 Outbreak of World War Two

Communications Security takes over Mansfield College Oxford, and the Oxford University Press

1943 The first 'Colossus' computer was created for the 'Newmanry' section at Bletchley Park

1946 GC&CS renamed as Government Communications Headquarters (GCHQ)

First use of a computer to generate cryptographic material

1953 Coronation of HM Queen Elizabeth II

Last 50 years

1969 GCHQ takes the lead on Information Assurance after incorporating the Communications-Electronic Security Group (CESG)

1970 Public key cryptography conceived by James Ellis at GCHQ

1988 Morris Worm computer virus distributed via the internet, resulting in the setting up of the first Computer Emergency Response Team (CERT) in the US

1990 Concept of the World Wide Web created by Sir Tim Berners-Lee

Last 20 years

1997 Introduction of the Government Secure Intranet (GSI), connecting UK government computer networks

1999 Creation of the National Infrastructure Security Co-ordination Centre (NISCC)

2010 Start of the first UK National Cyber Security Programme

2016 National Cyber Security Centre (NCSC) established

1830s:
Invention of the telegraph

After the invention of the telegraph it became **much easier to communicate with missions overseas,** and the Foreign & Commonwealth Office in particular took advantage of this.

Their codebooks might have provided adequate security for five or six months but they were in use for up to 20 years at a time and offered no protection against determined foreign powers, such as the Russians and the Austro-Hungarians, both of whom had cryptanalytic agencies.

Latter 19th century:
Military cipher training

The British military were aware of the vulnerability of their communications to interception but were hampered by the difficulty of encryption in the field. The Playfair cipher was invented in 1854 by Charles Wheatstone, but was named after early adopter Lord Playfair, who introduced it to the military. By encrypting pairs of letters, **the simple technique improved the encryption process and was used to protect important, yet non-critical, secrets.**

In the latter part of the 19th century, all British Army officers were trained in the use of the Playfair cipher – though some would argue that this offered an illusion of security rather than any real protection.

Early 20th century:
Wireless technology in the Royal Navy

The Royal Navy, always keen to exploit new technology, showed great interest in wireless communications from the moment it learned of Guglielmo Marconi's invention of the radio.

As early as 1900, both sides during naval exercises had rules to deal with intercepted 'enemy' signals, and by 1906 the Commander of the Home Fleet was insisting that all messages sent in code should be reciphered with an elementary transposition cipher.

World War One:
Codemaking

During the static warfare on the Western Front, technology began to supply the security that British Army communications needed. When it was realised that the Germans were exploiting the ground returns of British trench telephony systems, Captain Algernon Fuller devised a way of disguising the signal itself.

But British cryptanalysts continued to uncover evidence of German successes against British field codes and eventually, **in 1918, codemaking was put into the hands of the same part of the War Office involved in codebreaking.**

1919: The birth of GCHQ operations

To really understand what the NCSC is all about, you have to set our ambitions within the context of GCHQ's history. **Security has been part of the modus operandi since our parent organisation was first established in 1919.**

On 1 November 1919, the Government Code and Cypher School (GC&CS), the name for GCHQ until 1946, was created. Part of the Admiralty until 1922 and then of the Foreign Office, its overt role was to provide advice and training on communications security to British government departments.

This aim was flawed from the outset. The GC&CS remit was limited to advice, and the armed forces and the service ministries were explicitly removed from GC&CS's scope. This meant that the experience gained by cryptanalysts working against German and Italian naval and military targets in the 1930s was not used to inform better security for UK forces.

World War Two: Turing and Typex

On 3 September 1939 the UK declared war on Germany, and the next day Alan Turing started working at Bletchley Park. His work was key to breaking the wartime Enigma codes and Turing also laid down the theoretical plan for a programmable computer.

In 2009, then-Prime Minister Gordon Brown said: "Alan Turing was quite a brilliant mathematician, most famous for his work on breaking the German Enigma codes. It is no exaggeration to say that, without **his outstanding contribution, the history of the Second World War could have been very different."**

However, at the start of the war the security of British military encryption systems was so poor that by June 1940 the Germans were reading everything - with the exception of Typex.

Used from 1937 onwards, the rotor-based electromechanical cipher machine Typex was a British variant of the Enigma machine. Modifications were made to the Enigma design to make Typex secure. **It could be made to emulate the German military Enigma machine, and Typex was used in this configuration to manually decrypt intercepted messages.**

While it went through lots of variants, Typex was used securely until the end of the 1960s, when it was finally withdrawn from service.

Colossus and random number sequences

Also in the 1940s, **GCHQ's Bletchley Park became the first home of the world's first large-scale electronic computer – Colossus,** the brainchild of Thomas H. Flowers.

The knowledge and techniques used to design the first computer would go on to help generate the first random number sequences. This used technology from Bletchley Park to pioneer the automated production of cypher material, giving the Allies a huge technological advantage.

The Cipher Policy Group

In January 1944, the Cabinet Secretary, Sir Edward Bridges, persuaded the War Cabinet that the long term solution involved **bringing into a single organisation all of the entities involved in designing and using encryption systems**, ensuring that cryptanalysts would be integrated into this work. This also gave the newly formed organisation the opportunity to mandate standards for communications security. This proved to be a huge change in direction.

Before then, all that could be done was provide advice. As early as 1942, Sir Edward had realised that the Battle of the North Atlantic could have been lost because of poor security and that this needed a single focus to mandate common standards.

Initially, this became the Cipher Policy Group of GCHQ, but as GCHQ prepared to move to Cheltenham, Bridges persuaded ministers that the security organisation should remain London-based and be separated from, though remaining close to, GCHQ.

The London Communications Security Agency

From 1954 the new organisation, the **London Communications Security Agency (LCSA)** shared GCHQ's Central London office building but had its main offices at Eastcote, near Ruislip. It co-ordinated security standards across government, and designed new encryption systems for use by the UK, Commonwealth countries and NATO allies.

Post War: Communications-Electronics Security Department

In the years after World War Two, increasing technological change led to the LCSA absorbing service and General Post Office (GPO) elements involved in security research. This led to a change of title in 1965, as the **Communications-Electronics Security Department was formed**.

The organisational separation from GCHQ was not successful, and in 1969 CESD rejoined as CESG, the Communications-Electronics Security Group, and began a slow period of reintegration which culminated in 1978 with the closure of Eastcote and the move of all CESG functions to Cheltenham.

Public key cryptography

In 1969, James Ellis, one of the British government's leading cryptographers, conceived what we now call public key cryptography (PKC). This is a system that uses a pair of keys – one public, which can be disseminated widely, and one private key that is known only to the owner.

This was then evolved by Cliff Cocks and Malcolm Williamson's success in outlining how to make PKC work, and Whitfield Diffie and Martin Hellman's parallel discovery of exchanging keys, which ushered in an era in which a previously unattainable level of trust between two parties could be established.

This allows not only today's online shopping where customers and businesses conduct transactions online but also the possibility for citizens and government to carry out all of their business online.

The Government Secure Intranet

The ability for government departments to safely and securely communicate with each other grew to new heights in **1997 with the introduction of the Government Secure Intranet (GSi)**.

This gave staff in departments and their agencies the capacity to share information electronically, cutting down on logistical restrictions that had previously slowed down the state's work.

National Infrastructure Security Co-ordination Centre

This ability for wings of the government to safely and securely communicate with each other increased again in 1999 with the creation of the National Infrastructure Security Co-ordination Centre (NISCC). **The key aim was to minimise any threat to the critical national infrastructure** by providing advice and information on how to keep computer networks as safe as possible from the growing threat of electronic attack.

The NISCC was eventually merged with the Centre for the Protection of National Infrastructure (CPNI) in 2007, which operates to this day offering security advice to those organisations whose infrastructure the nation depends on.

The National Cyber Security Centre

In a response to the growing need to protect national security and safeguard the public online, the UK's Cyber Security Strategy was created in 2011.

Writing at its launch, then-Minister for the Cabinet Office The Rt Hon Francis Maude, said: "The growth of the internet has been the biggest social and technological change in my lifetime… at the same time, our increasing dependence on cyberspace has brought new risks in ways that are hard to detect or defend against."

Both the positives and the negatives of the cyber age continued to increase through the decade, culminating in the establishment of the government's National Cyber Security Centre (NCSC) in 2016.

With a vision to help make the UK the safest place to live and do business online, the NCSC was set up as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents.

Present

- The National Cyber Security Centre (NCSC) is a part of GCHQ and is the UK's authority on cyber security.
- Our main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience.
- The NCSC brings together and replaces three existing cyber security organisations – the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and CESG (GCHQ's information security arm) – and includes the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).
- We recognise that, despite all our efforts to reduce risks and enhance security, incidents will happen. When they do, the NCSC will provide effective incident response to minimise harm to the UK, help with recovery and learn lessons for the future.
- The NCSC will work together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. This is underpinned by world-class research and innovation.

Present

What is the NCSC doing to help the UK prosper in the cyber age?

The NCSC is at the cutting edge of proactively making Britain as safe as possible to both live and work online.

Since launching in October 2016, the NCSC has already shown its huge value by working with the public and private sectors in building cyber security skills, developing innovative defences and helping to manage cyber incidents.

But we are much more than incident management. Embedding good practice among all computer users is a key target, and in the words of our Technical Director Dr Ian Levy, the strategy is to ‘use government as a guinea pig for all the measures we want to see done at national scale’.

One key element of our work to help reduce cyber attacks is the Active Cyber Defence programme. This is intended to tackle, in a relatively automated way, a significant proportion of the cyber attacks that hit the UK. We hope to demonstrate to the government that these measures have been effective and reliable, before encouraging the private sector to adopt them.

Making your emails safer

The most common vehicle for cyber attacks is emails. Phishing is an email attack where a victim is tricked into handing over sensitive information or compromising their device, usually by clicking a link or opening an attachment. This has led to the accepted advice being 'never open an attachment or click a link in an email from someone you don't trust'.

But targeted phishing emails could seem to be from someone you know and be so sophisticated that even an expert would struggle to tell if it's malicious. **We want people to be able to trust email, because productivity suffers as a result of the fear that emails can carry a hidden danger.**

Trying to eradicate every single bad click is an unrealistic and harmful goal. Users have a limited amount of time and effort to spend on security. Instead, we want them to put their effort in places where it will get the best results.

There are some email security technologies that make it difficult to spoof popular brands. We want government to use these anti-spoofing technologies to protect its brands, but also to set a good example to other sectors. To advance this work, the **NCSC has worked with Government Digital Service on an email security standard for government.** We supported HMRC, one of the world's most-phished brands, in implementing these anti-spoofing technologies – and **abuse of their brand has dropped significantly as a result.**

Key to the success of delivering this email protection across government is the role of the NCSC in developing a service to track adoption of the standard and to analyse the automatically generated reports produced by email services to help organisations understand, and put a stop to, spoofing of their domains.

Free vulnerability scanning service for public organisations

We are improving security for both central and local government – helping them to deliver great public services. There is a lot to do in this area and we have to be careful that people don't think we're absolving them of their risk management responsibilities, but we are committed to helping them.

We are developing a service to track and promote the adoption of 'WebCheck' that will allow government organisations to create an easy-to-read report about any common vulnerabilities on internet domains they own and help them to put them right.

We want to build reputation services to help digital service owners make transaction risk decisions. Initially this service will give reputation information for IP addresses connecting to the service and credentials that are used, but we're looking to extend that over time.

We are also looking to **experiment on government with novel cyber security techniques and capabilities.** One example is a software agent that runs at low privilege on a government workstation and sends metadata back to a central processing facility for analysis. We don't know yet whether we can detect unknown attacks and exploits using this sort of technique, but there are some experiments taking place to find out.

Encouraging innovative alternatives for identity/authentication

Passwords are synonymous with proving identity on a computer – and there is little incentive for industry to take a commercial risk in trying out new approaches. That is why **we want to stimulate research and development – and eventually a market – in novel identity and authentication techniques.**

We will use government services to trial some new techniques, once we've done the work to ensure the security. Through the gov.uk Verify platform, we have an ideal place where we can try these things out with very little impact on the actual services.

We don't want to discount anything, including using your face, your watch or anything else that is proposed. The principle is to **promote innovation and adoption of these technologies,** and doing some security design and assurance work up front.

Secure by default partnership programme

Linking closely to our work on identity and authentication, our **Secure by Default Partnership Programme helps departments trial adoption of new technologies they otherwise would not be shown the benefit of.** This will demonstrate just how good we can make the usability of devices while making sure they're secure enough and meet all the policy requirements of the organisation.

We are looking to help a number of proactive public sector organisations to successfully adopt some particular new technologies, learn from these experiences and then share the results with the wider public sector.

Together we can show that these new technologies can be adopted successfully in the public sector, for clear business benefits. We understand that adopting a new technology can seem risky – so, to mitigate risks and boost confidence, we will help where we can and the NCSC will provide technical expertise and access to our policy experts.

Automated filtering to protect the UK's computer network

The Domain Name System (DNS) is often referred to as 'the address book of the internet'. It turns memorable names that humans can use into the IP addresses that computer systems utilise to locate each other. **As well as being used to access legitimate sites, DNS can also be used to facilitate the distribution and operation of harmful malware.**

The NCSC can't – and would never want to – run the UK's DNS for everyone. **However, we can and will help prevent users from unknowingly accessing sites that are known to do them harm.** Working with Government Digital Service, we have partnered with Nominet UK to build a DNS service for the public sector that will protect their networks from attack and generate data to understand the state of public sector IT.

Following the launch of the public sector DNS service in April 2017, we will talk to internet service providers about doing something similar for their residential customers. Our intent is that, by default, the UK public will be **protected from things that would do them harm without their knowledge** – with an easy opt-out if they so desire. That should have a big impact on the scale and effectiveness of a lot of the attacks we see against the UK.

Improving the UK's software ecosystem

When users visit gov.uk, technology now automatically recognises whether the computer accessing it has out-of-date software – for example an old operating system. The site then displays a banner to warn them that they are more susceptible to their device being compromised.

Taking a similar approach on some of the most popular websites in the UK could have a significant impact in nudging users into updating their software.

Of course in doing this, we are conscious of digital inclusion. We'll be working with relevant experts in government and industry to work out how to help citizens understand the implications of running out-of-date software, while avoiding disadvantaging those who are most digitally vulnerable.

Mitigating against attacks and responding to incidents

The NCSC is working with the pioneering and innovative UK company, Netcraft, to counter common attacks which are hosted in UK IP space. The Netcraft work has also identified attacks which specifically target UK government departments and services. These attacks are hosted both here in the UK and in a wide range of countries overseas.

Since June 2016, a total of **54,456 attacks have been mitigated i.e. blocked, and the malicious content taken down by the host.** 36% (19,906) of these attacks were hosted in IP ranges delegated to the UK (phishing and web-inject malware). The remaining 64% (34,550 attacks) specifically targeted UK government departments to exploit British citizens by fraudulently obtaining their online credentials and personal data.

The countermeasures are automated in nature and have reduced the mean time an attack lasts. For example, phishing sites hosted in the UK now have a mean duration of less than one hour (before takedown) where previously a mean duration of 27 hours existed in the three-month period prior to the service becoming operational.

Incidents will still happen, and when they do we will provide effective incident response to minimise harm to the UK, help with the recovery and learn lessons for the future. If anybody feels they are the victim of a significant cyber security incident, the NCSC offers support 24 hours a day, 7 days a week, 365 days a year.

Building the UK's cyber security capability in research, innovation and skills

The NCSC is tirelessly committed to enhancing the UK's reputation of being a world centre for cyber security research, innovation and skills.

Our popular CyberFirst programme is inspiring, encouraging and developing a cyber-savvy cohort of students to help protect the UK's digital society. Over 2,500 11–17-year-olds can take part in our free cyber courses and there is a girls' competition for 13–15-year-olds. In addition, 250 students will receive bursaries worth £4,000 per year. This programme has grown in each of its three years and we hope to be giving bursaries to 1,000 students by 2020.

Of equal importance is our education programme to ensure University higher education maintains its world-class status in cyber security. A programme has been developed which identifies and recognises good Master's degrees in cyber security and the NCSC/GCHQ has certified 20 Master's courses at 15 universities across the UK. Over the past year, the Master's certification has been extended to one-year postgraduate degrees in digital forensics and four-year undergraduate Integrated Master's degrees which provide a foundation in computer science and cyber security.

The NCSC has established a number of research initiatives to ensure the UK is best placed to stay at the forefront of cyber security. This includes identifying 13 Academic Centres of Excellence in Cyber Security Research (ACE-CSR), funding three Research Institutes and funding over 30 Doctoral studentships drawn from the ACE-CSRs.

In addition, the NCSC has brought industry and academia together via the **CyberInvest programme – an initiative which commits industry to invest in cyber security research within UK universities.**

The NCSC has also established the first government cyber security innovation centre. As part of this, seven start-up companies have joined the Cheltenham Accelerator and will be working with experts to help them develop their ideas into commercial reality.

Future

- The NCSC will provide security for the UK during a period of significant change. While no one knows exactly what technological jumps there will be over the next decade, there are a number of trends that allow us to make some bold predictions.
- As we embrace the world becoming more cyber-educated, defences will need to adapt to counter advancing cyber threats.
- Improved cyber security is essential to promote a robust and prosperous cyberspace, allowing reliable and trusted infrastructure for better business and government connectivity.
- Critical to this will be the ability to monitor and defend that infrastructure from hostile attack.

Future

What cyber threats will the UK face in the next decade?

Predictions of the future seem to fall into two categories – utopian fantasies and dystopian warnings. Our job is to mitigate as much against the latter to make the former as deliverable as possible.

While predicting the future is impossible, the NCSC is absolutely committed to using our expertise to track and forecast upcoming changes in the cyber landscape so that we can continue to safeguard people's lives and work online.

Not everything that is developed will be a danger – but all advancements will require our attention.

More threats from more states

The ever-higher incentive for cyber attack will be matched by the **growing number of potential attackers.** The gap between developed and developing world, where cyber is still in its infancy, will rapidly **decrease due** to falling costs making technology more accessible.

Internet usage in Asia, Africa and the Middle East is rising rapidly and some analysts predict a **90% worldwide computer literacy rate by 2025. It is likely that cyber security will experience a 'see-saw phenomenon'**, with one technological development giving the offence or defence the upper hand.

Most countries will recognise that **cloud technology** is not only a necessity for meeting the information demands of their citizens, but is also required for participation in the global economy. We judge that businesses will lead the adoption of cloud technology in order to remain competitive and efficient.

Governments will follow quickly to cut costs, enable services and mitigate dependencies on legacy equipment. As the cloud becomes increasingly necessary to the development and delivery of critical services, the **security, privacy and reliability of data will become increasingly acute.**

We judge that the increasing reliance on the internet by governments, businesses and individuals will make **the acquisition of espionage and offensive cyber capabilities attractive to more states.**

Quantum technologies

Thirty years after they were first proposed, quantum computers remain largely theoretical. But given advances, it is possible that quantum computers could leap out of the lab in the next 10 years.

If they did, quantum processing could factor large numbers quickly to crack public-key encryption technology, **necessitating a new approach to security.**

Quantum technology is a radically different way of making computers – working at an atomic level, **with processors that could work millions of times faster than the ones we use today.** Innovations such as **atomic clocks** for communications and **GPS resilience** are likely, but it is unclear whether widespread, commercial and practical quantum computers will appear.

4,000 low-orbiting satellites

Today's satellite internet is expensive and experiences high latency (time between data being sent and received) due to satellites' high orbits. This makes it a poor option for several applications such as gaming, videoconferencing, live streaming and browsing.

But satellites are being developed to deliver internet across the world far cheaper and faster (communicating with earth-based receivers using the radio spectrum).

Eventually some 4,000 satellites may be active in low-earth orbit. Estimates suggest the latency at this height would be **comparable to, or better than, existing broadband solutions which use a network of fibre-optic cables laid on the seabed.**

Increasing technological dependency

Increasing dependence on information and communications technology will mean cyberspace will be widely exploited by all types of actors. The effects of their actions will vary. **End-to-end encryption is likely to become increasingly common, and probably ubiquitous, over the next 10 years.**

The increasing ease of use and importance of computers and networks in many aspects of life is likely to lead to widespread dependence on them by citizens, industry and governments, creating critical vulnerabilities for potential adversaries to attack.

However, vulnerabilities could be reduced by new technologies such as the development of intelligent, self-repairing networks, and virtual databases.

Rise of the robots

Robotic, unmanned and autonomous systems will increasingly bridge the gap between the virtual world and the real world over the next decade. **3D printing allows new forms of home manufacturing, and consumer robotics now extends to personal drones and home automation.**

Corporations and communications providers will use cutting-edge technology such as robotics to provide remote wireless access to inaccessible locations. Governments will continue to expand the use of robotics and unmanned aerial vehicles (UAVs – or drones) into expanded combat and surveillance roles.

Internet of Things (IoT)

IoT refers to the connectivity of **anything** to the internet. Anything connected in this digital mesh of mobile devices, wearables, consumer and home electronics, automotive, environmental sensors and more can interact with people, social communities, governments, control systems and businesses.

The information goes beyond textual, audio and video, to include sensory and contextual information. **While this poses new opportunities, it will also present many new challenges.**

Future

Ten things to get excited about in the next ten years

It’s impossible to say with certainty exactly what will happen, but for some fun, here are ten things to get excited about that could improve the cyber landscape in the next ten years.

1. Smart cities, smart governance

The way data is used could revolutionise how the human race builds its future cities.

Smart is the new ‘Green’. Smart cities will emerge that allow planning and governance to make **data-driven decisions**. Asset tracking, optimisation of traffic and utilities will be possible from smart devices and infrastructure.

This technology will be used to **optimise processes, pollution, people and security – reducing costs, waste and risks.**

2. Next generation productivity

Are swathes of your working day taken up spending excessive time in meetings? The cyber revolution could help save your sanity!

Over the next decade, new technology will bring productivity to new environments. **For example, Augmented Reality and Virtual Reality displays will enable massive leaps in visualisation of big data,** and personal displays for displaying any data in any location.

Further use of desktop videoconferencing and telepresence will bring cultural changes through organisations across the extended enterprise, **meaning less time in meetings and travelling, and more time producing.**

3. The new space race

By 2020, the commercialisation of space – both launch vehicles and commodity microsatellites – **will mean a lower barrier to entry for those wishing to innovate and exploit the benefits of orbital platforms.**

This new space race between corporate interests, government control and the physical limits of space travel will provoke and spark new ways of working and capabilities.

Without space programmes we wouldn’t have today’s laptops, televisions or even smoke detectors, so there is scope for a lot of innovation with more space exploration.

4. The internet of ‘me’

Location is a key service that underpins the majority of services and applications in the Internet of Things. Wearable technology, smartphones and even cars will find new ways to use geolocation as a service.

The pursuit of location-based services, **targeting advertisements and market segmentation will lead to new advances in the way geography and our travel will affect our online experiences.**

The internet of everything will be tailored to each and every user, with preferences and habits from a number of sensors – from central heating, to social media to bio-physical. This will create exciting new ways to provide **a tailored, personal experience for consumers.**

5. The context cloud

Similarly, there will be a change from 'big data' to 'rich data' which will be powered by context and focus. Context, generated by analytical judgements, reference data and historical understanding, is needed to enrich new data and automatically piece the jigsaw together.

Context will provide new ways for queries and analytics to be built based on behaviour, demographics, geography and social identity.

6. Virtual databases

The continual evolution of networks will probably result in the development of a **'semantic web'**. Machines will **recognise, identify, capture, manipulate and interpret data with minimal or even no human intervention.** This unprecedented speed and level of access could be exploited by reasoning techniques to provide more sophisticated forms of analysis.

7. Autonomous agents

Autonomous agents will **analyse automatically and in real time huge volumes of data.** Crawling across disparate datasets, they will provide **ranking and stacking algorithms to promote and pre-compute valuable insights.**

Driven by analyst recommendations and Deep Learning technologies, they will change and adapt in new ways to discover information of value, and **predict future states.**

8. Digital natives in the connected workforce

Anyone with a toddler and a tablet will know that technology is so embedded with the next generation, using it will come naturally. The internet is at the heart of the connected workforce. Employees are able to develop and learn from all the same sources and platforms available to consumers, in a safe and secure manner.

Work and life will be balanced with more opportunities to communicate and utilise modern technology and tools. **Employees will thus be 'digital natives', mastering technology for any necessary purpose,** being able to exploit this knowledge and experience or provide guidance for any potential utility.

9. Getting fit through biometrics

Technology has often been criticised for its effect on our health, but there is significant cause for great optimism that the reverse will be true in the future.

Biometrics is already a significant growth area. Looking forward, **biofeedback sensors will permeate personal fitness allowing new data-driven understanding about biology,** with security concerns inevitably emerging at this fundamental interface between man and machine.

10. Anything your mind can imagine… and more!

Nobody could have predicted everything that has happened in the cyber landscape in the last ten years, and with the world's brightest and best brains flocking to the technology field, we are sure that all sorts of magnificent things will come in the next decade.

What we can say with certainty is that the NCSC is building on the success of our forerunners, to ensure the UK remains a world leader in cyber security.

The issues facing the nation in cyberspace are numerous, evolving and exhilarating; whatever the future holds, it is the creativity and innovation within the NCSC that will help to make the UK the safest place to live and do business online.