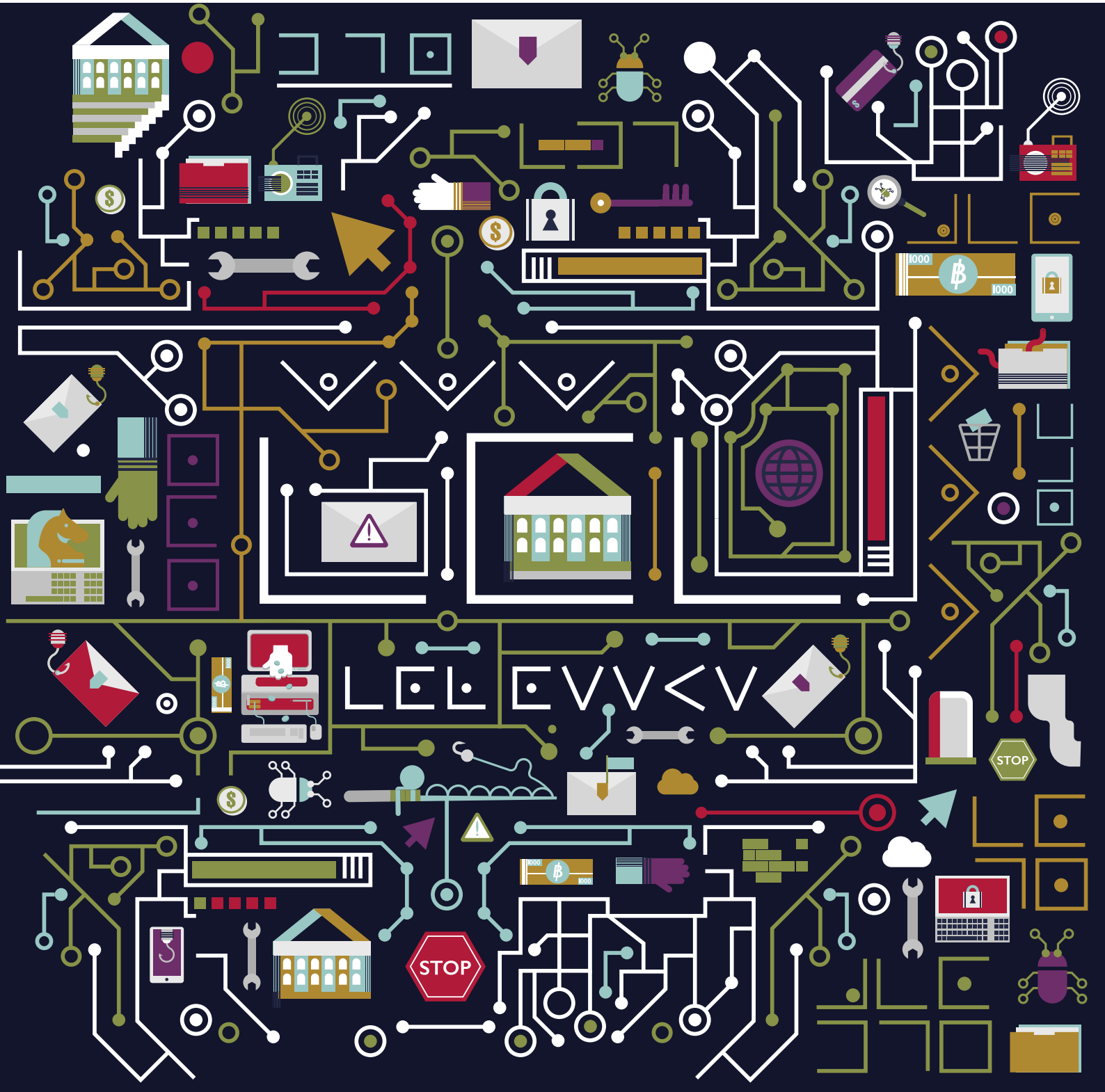
National Cyber Security Centre
a part of GCHQ

annual review

2017

Making the UK the safest place to live and work online



Introduction

Responding to the threat

Building the UK's defences

Cyber skills and growth

foreword

I am proud to introduce the National Cyber Security Centre's first annual review.

We were set up last October in support of a national ambition, outlined in the National Cyber Security Strategy, to make the UK the safest place to live and do business online. We are a 'one stop shop' for cyber security, uniting separate parts of Government that had a role in this area within GCHQ.

This report sets out the progress we have made in our first year of operations. The reality of the threat we face – large, growing and diverse – means that some attacks will get through, and the first duty of the NCSC is to help manage and mitigate the impact of those attacks. In our first year, we responded to 590 significant attacks, ranging from attacks on key national institutions like the National Health Service (NHS) and the UK and Scottish Parliaments, through to attacks on large and small businesses and other organisations.

> We are proud to be a part of GCHQ, a fantastic organisation that has served the country with world-class knowledge and expertise since 1919.

But so much of our work aims to make successful attacks less likely. A core part of this work is in protecting critical national assets. Over the course of the past year we produced over 200,000 protective items for Armed Forces communications. We have supported the Cabinet Office in developing more secure communications for key Government organisations, and the Home Office in ensuring the security of new mobile communications for our vital emergency services.

And a crucial part of our role is to help everyone to operate more securely online. Through a pioneering partnership with the private sector, tens of millions of suspicious communications in the UK are being blocked every month. Our world-leading Active Cyber Defence programme has developed capabilities which have seen the average lifetime for a phishing site hosted in the UK reduce from 27 hours to less than an hour. Our information-sharing platform with industry grew by 43% over the year. We are forging new partnerships in key industries like retail.

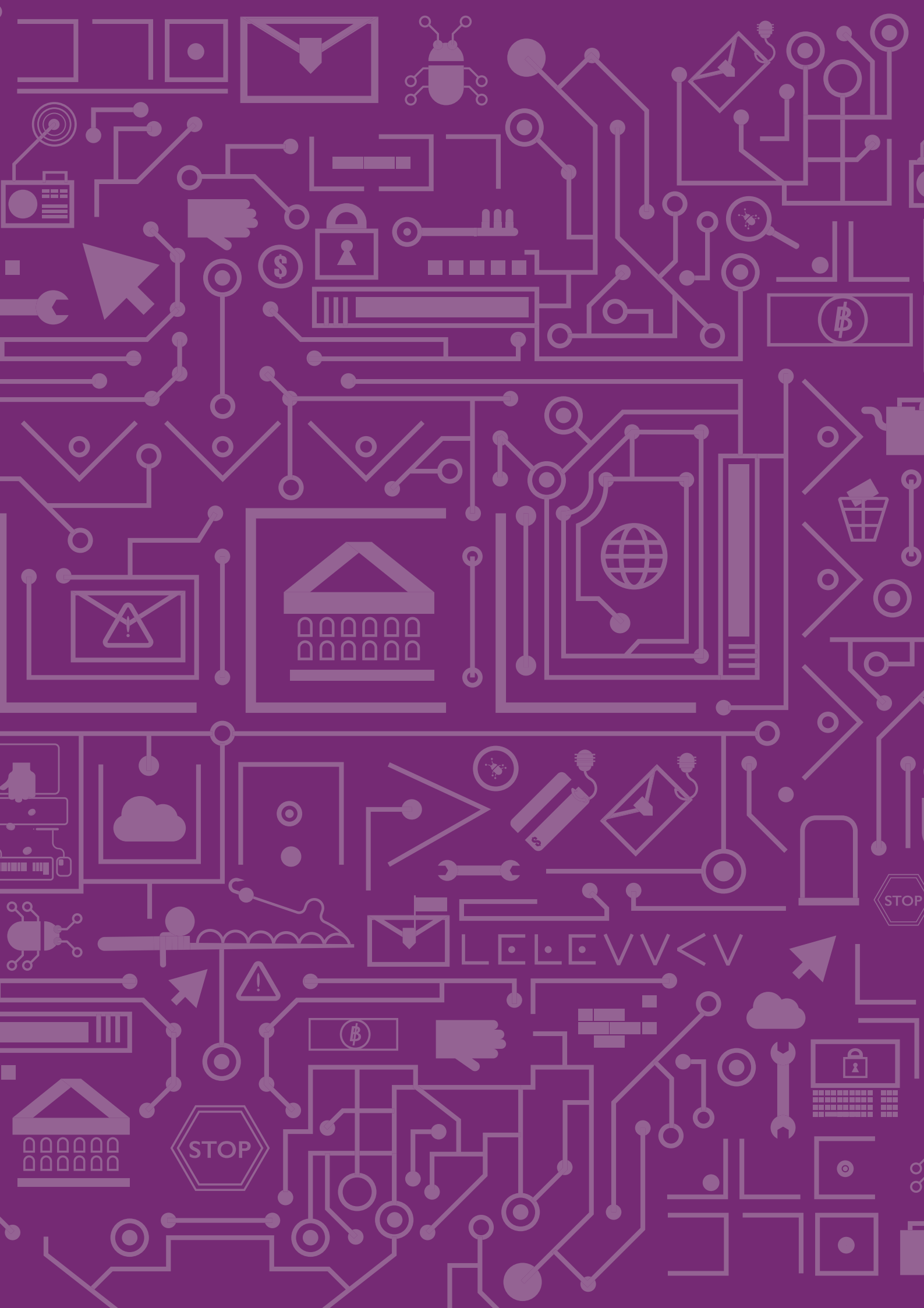
And we are helping nurture the next generation of skilled professionals we need. For example, our CyberFirst Girls competition saw 8,000 talented 13-15 year olds take part; this is an initiative we hope will play a role in the long-term in addressing the damaging under-representation of females in the cyber industry.

So we are proud of what we have achieved in our first year. We were particularly honoured by the visit of HM The Queen and HRH The Duke of Edinburgh in February to open officially our new headquarters in central London. But there is so much more to do in our second year, and in the years ahead, to counter this strategic threat to our values, prosperity and way of life. We know that as well as our talented and dedicated staff, we can also count on our partners – in the rest of GCHQ and the UK intelligence community; in law enforcement, particularly the National Crime Agency; in wider Government; in industry and internationally – as we set about meeting that challenge.

Ciaran Martin
Chief Executive Officer
National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

GCHQ


STOP
STOP

executive summary

The NCSC was created in 2016 to make the UK the safest place to live and work online. Operating as part of GCHQ, it is a cornerstone of the UK Government's National Cyber Security Strategy.

The creation of the NCSC has brought together previously separate parts of government, MI5 and GCHQ to create a single lead authority on UK cyber security. We moved into our new London headquarters after an official opening by Her Majesty the Queen, accompanied by His Royal Highness the Duke of Edinburgh.

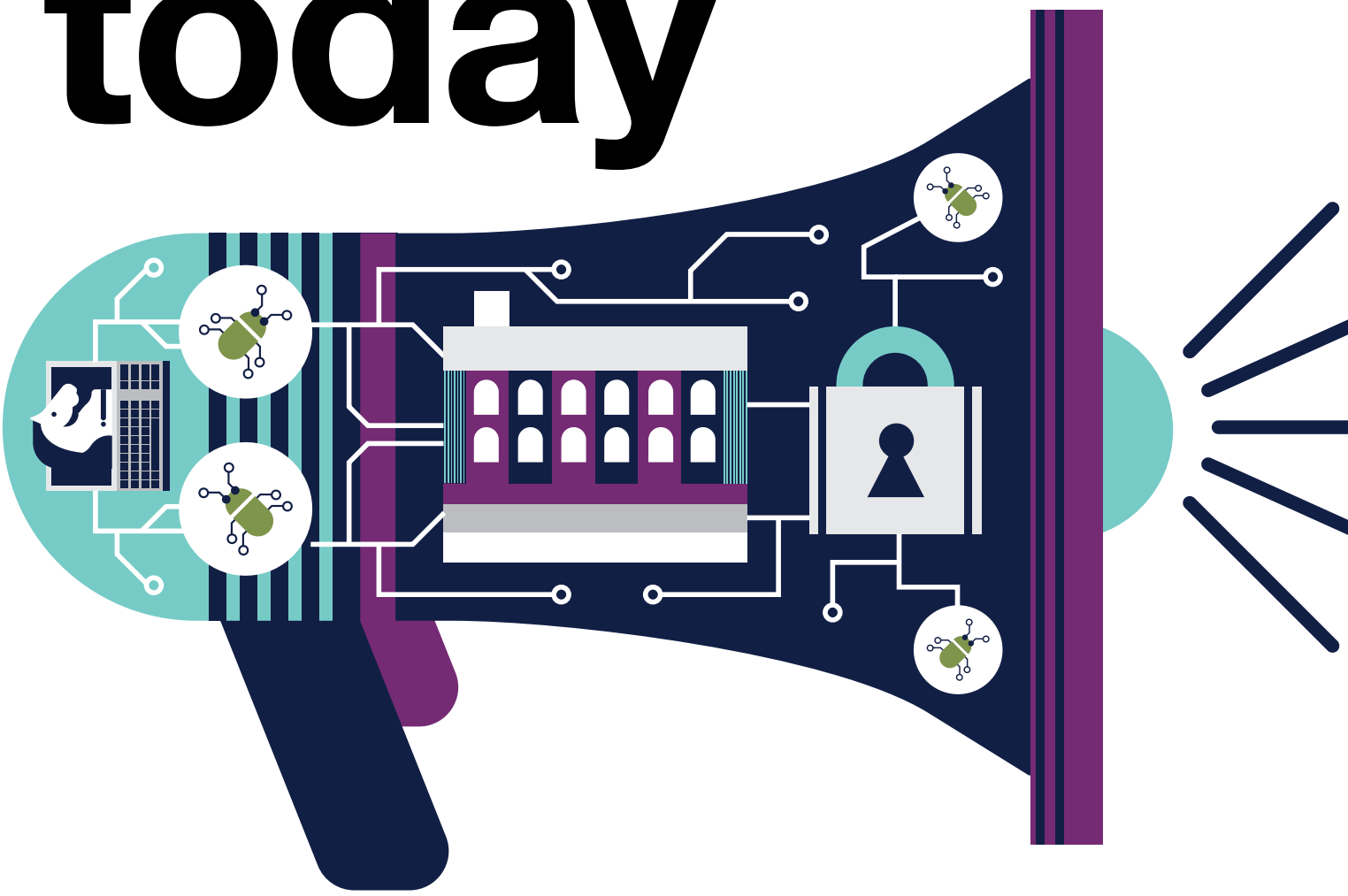
While we are still early on in our journey, our successes over our first 12 months are outlined in this report.

In summary, the NCSC has:

- launched the Active Cyber Defence, which has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour
- responded to more than 590 significant incidents, co-ordinating government's response and providing reassurance to the public
- led the UK response to the global WannaCry incident, which affected 47 NHS trusts, providing vital assistance and reassurance to those impacted
- created a website to provide easy-to-understand advice and information to the public. The site received 100,000 visitors in a single month and we issued 2,000 tweets over the year
- hosted 2,300 delegates and 173 speakers at our three-day CyberUK conference in Liverpool, to share insights and build their understanding of cyber security
- seen a 43% increase in visits (4,000 visitors per month) to the Cyber Security Information Sharing Partnership (CiSP), which allows the community to share information about cyber threats
- produced 200,000 physical items for 190 customer departments through the UK Key Production Authority, securing and protecting the vital communications of our Armed Forces and the national security community
- helped nurture the next generation of cyber experts by hosting more than 1,000 young people on CyberFirst courses and inspiring 8,000 young women to enter our CyberFirst Girls competition
- created the pioneering Industry 100 initiative to work with or embed one hundred industry professionals within the NCSC, to provide challenge and innovation
- worked with more than 50 countries across five continents, including signing NATO's ground-breaking Memorandum of Understanding

*number correct at time of going to print

the cyber threat today



The cyber threat is real and growing, and the type of threats we face are always evolving.

There are now more devices connected to the internet than there are people in the world and with the growth of our dependence on technology comes an increased risk. Despite the NCSC's best work in defending the country from that threat, we can't prevent every attack.

In our first year, the NCSC has communicated directly with industry, individuals and organisations about the threats we all face daily. We are committed to being fully transparent and do all we can to make our advice public and accessible, while also facilitating a private collaborative environment to share more sensitive information. That's why our assessments and advisories are shared through various platforms such as our website, the Cyber Security Information Sharing Partnership (CiSP) and in speeches.

Ranging from high volume attacks available to order online to bespoke malware attacking specific targets, the lines between those committing attacks continue to blur. We know that criminal groups imitate states to attack financial institutions, and sometimes vulnerabilities in systems can mean that unsophisticated techniques can pose a severe impact.

Nation state

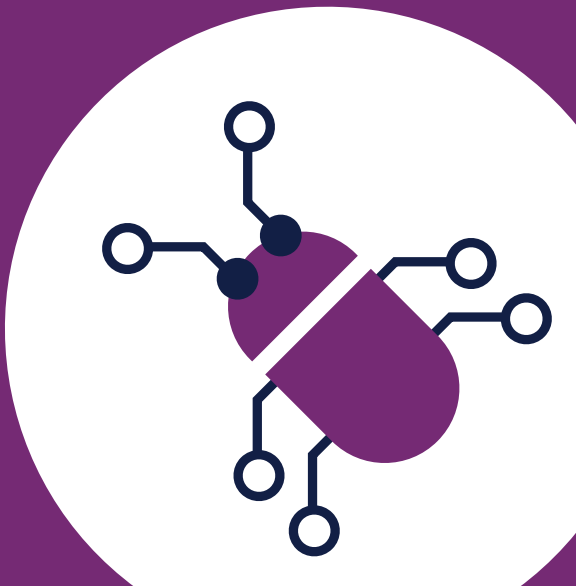
Cyber operations can give countries a strong opportunity for strategic advantages, and we know there are nation states that may seek to exploit UK organisations to further their own agenda and prosperity. Campaigns by nation states can be persistent, including espionage and intellectual property theft that take place over many years and use significant technical capability. Nation States are also starting to explore how cyber operations can support a disruptive and destructive strategy.

Cyber criminals

Cyber criminals seek to exploit UK organisations, individuals and infrastructure for profit. Their technical sophistication varies from small scale cyber-enabled fraud to persistent, advanced and professional organisations. They may directly steal money or monetise their capabilities indirectly, for example through intellectual property theft, extortion by ransoming data, or through malware.

Hacktivists

Hacktivists aim to raise awareness for their cause. They focus on propaganda, website defacement and denial of service attacks. Few hacktivists can carry out a successful denial of service attack against organisations with mitigations in place. Reputational hackers seek to compromise a business simply to demonstrate their skill. They range from very low skilled individuals using tools purchased online to highly skilled experts.




STOP

responding to the threat

It is not possible to stop every cyber attack, so we are committed to delivering a world-class incident management service.

Our team is ready to respond to the most serious incidents and provide advice on reducing the harm they cause.

Our experts are constantly improving the UK's defences by learning and sharing information about the attacks we are facing.

incident management

There is no system in the world that is completely secure, and the UK faces cyber attacks of various types every day.

If organisations are affected by a significant cyber attack, we offer an incident management service to respond to incidents and to reduce the harm they cause.

Thanks to the organisation's collaborative ethos and the long-standing expertise that comes from being part of GCHQ, we are developing a level of support to both government and industry that has never been seen before in the UK.

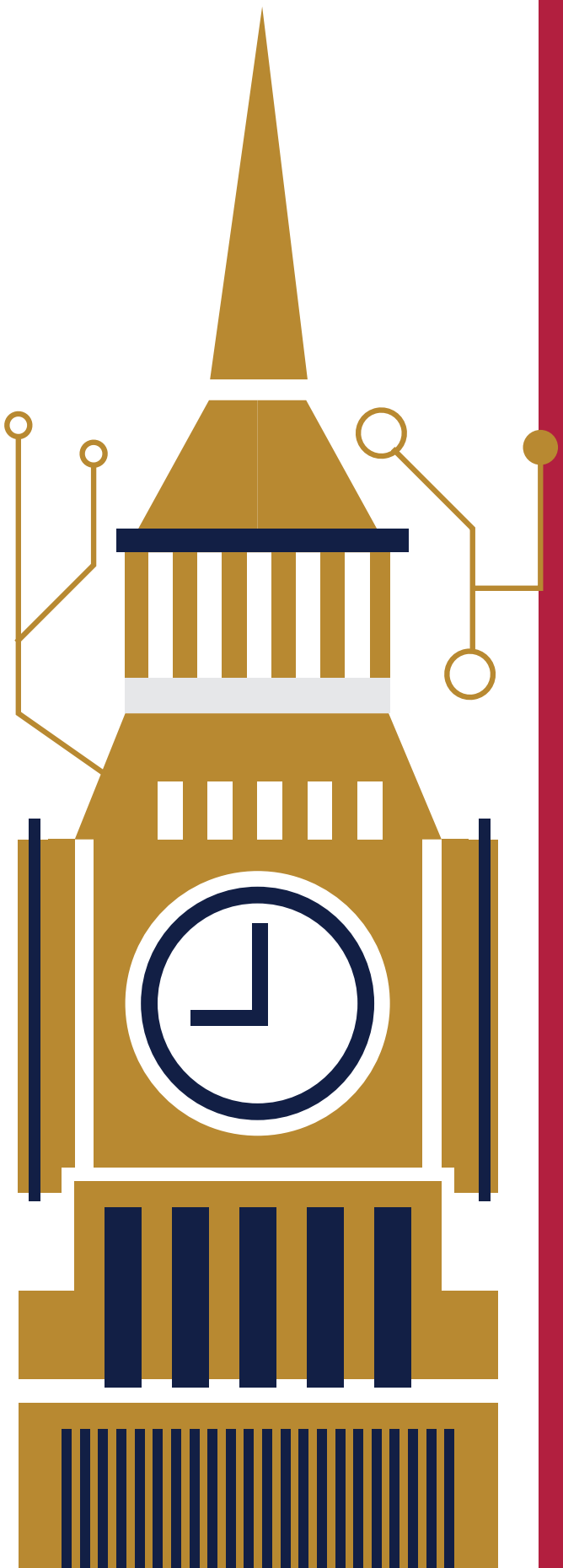
In our first year, the NCSC received **1,131 cyber incident reports** which resulted in **590 being classed as significant**. More than 30 of these were assessed as being sufficiently serious to require a cross-government response process, coordinated by the NCSC.

Crucial to our response is the partnership between the NCSC and law enforcement, including the National Crime Agency (NCA).

Our objective being to provide victims with a joined-up reporting and response service that harnesses our complementary capabilities.

Reporting from victims, either in government or private sectors, allows us not only to investigate incidents, but also to identify attackers and further affected parties. For the most serious attacks, we provide direct assistance to organisations.

We are learning more from every incident and our first year has taught us there are benefits to working even more closely with law enforcement agencies. Much progress has already been made, supported by NCA officers embedded within our incident management team and we continue to work ever more closely together.



25 June 2017 - Cyber attack on UK Parliament

The NCSC, working with the Parliamentary Digital Service (PDS), detected that the email accounts of UK MPs, Peers, their staff and parliamentary officials were the subject of a sustained and determined cyber-attack.

NCSC Incident Management worked with PDS and the Parliamentary authorities to investigate, advise and mitigate the attack.

PDS determined that email accounts were being targeted due to weak passwords, and that far fewer than 1 per cent of accounts were compromised.

Advice from PDS and the NCSC was given to all users on how to improve their security immediately and in the future. The NCSC also supported the NCA's work engaging with individual victims to collect evidence and offer ongoing victim care.


NCSC
NCSC
NCSC
NEWSPAPER
NCSC
STOP
LOVE
RANSOM

wannacry

On 12 May, the NCSC faced its biggest test of the year.

The global outbreak of WannaCry ransomware affected a significant number of networks in the UK and, most significantly, parts of the NHS. This led to the first ministerial COBR meeting following a cyber attack.

Ransomware has been an increasing threat in recent years. This incident affected more than 100 countries, including Spanish telecoms and German rail networks. In total, 47 NHS trusts and Foundation Trusts were affected in the UK, and the NCSC worked with NHS England's emergency response teams, the Department for Health, NHS Digital, and NHS Improvement to coordinate actions.

Our work with Regional Organised Crime Units and the NCA furthered the investigation into the attack which had infected more than 230,000 computers globally. Ambulances were being diverted from some hospitals, and a number of operations were cancelled.

The NCSC reacted quickly to offer victim support and advice on the day of the attack, updating our ransomware guidance. Experts from the NCSC were deployed to Barts Hospital Trust to provide bespoke advice. We continue today to work and support government departments in identifying vulnerabilities and mapping out what data matters and should be backed up.

The WannaCry ransomware encrypted data and demanded that victims pay to get it back. On Friday 12 May, countries across the globe experienced widespread outbreaks.

Friday afternoon: NCSC alerted to outbreak

Amongst those affected were **47** NHS trusts

Within 90 minutes, NCSC issue statement to media.

NEWSPAPER

Record numbers of professionals shared information on a collaborative and secure space to try and defeat the attack.

NCSC experts are deployed to victim sites and work with hospitals and law enforcement.

CiSP members collaborated to share information of the incident.

All weekend: Guidance issued and updated on NCSC website. NCSC experts conduct in house analysis, collating information online and producing quick and simple advice which was constantly updated.

Website:
4,000+ visits on website during weekend.

CiSP:
4x ↑ in page views on CiSP.

7x ↑ in daily CiSP coverage.

40x ↑ in visits to NCSC alerts and advisories.

Within 24 hours of the incident, the Home Secretary runs the first cyber COBR – with NCSC providing the communications lead.

We issued **27** tweets, which received **4,967** retweets (average of 184 per post) – significantly higher than the average when an incident is not ongoing.

Guidance updated and issued on our website and social media.

NCSC CEO interview on evening news - showing leadership and reassurance to the public.

NHS services back online.

Continued support from NCSC including best practices to sites.

The NCSC led the government's review of lessons learned, which included the need for increased collaboration with law enforcement and, improving the resilience of NHS networks.

nova south

We are proud to operate across a number of UK sites, and at our headquarters in London, where our incident management service facilitates our victim support work.

The NCSC became operational on 3 October 2016, but we officially moved into our new headquarters in Nova South on 14 February 2017. Our expertise was not born overnight and the NCSC brings together previously separate parts of government, parts of MI5, and GCHQ, creating a cohesive single authority that leads on UK cyber security. The NCSC enjoys close working and partnership across the three security agencies, and as a result, boasts a unique range and depth of expertise among our team.

The building is in Victoria, London, within minutes of Whitehall and with excellent transport links for the UK and beyond. Hundreds of staff use the building daily and Nova South has served as a venue for numerous events, meetings and workshops.

Fittingly for this crucial role, the building was formally opened by Her Majesty the Queen, accompanied by His Royal Highness the Duke of Edinburgh.

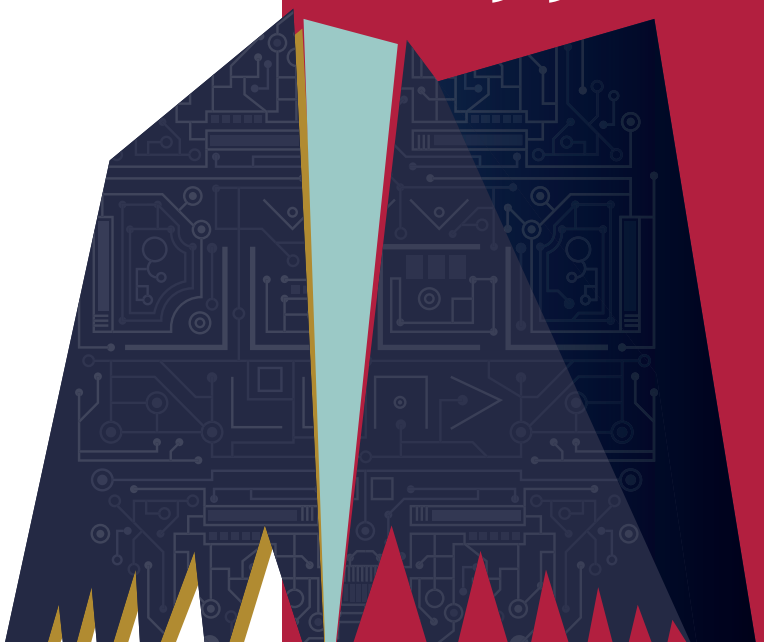
Also in attendance were Secretaries of State and Ministers including Chancellor Phillip Hammond, Home Secretary Amber Rudd, Defence Secretary Sir Michael Fallon and Minister of State for Digital Matt Hancock.

Speaking at the launch, Phillip Hammond said:

"As Chancellor, I know how significant our digital sector is for the UK economy - worth over £118 billion per year.

"This cutting-edge centre will cement our position as world leader in cyber security and work carried out here will ensure our country remains resilient to potential attacks.

"Britain is transforming its capabilities in cyber defence and deterrence. It's crucial we take action now to defend ourselves and protect our economy."



CiSP

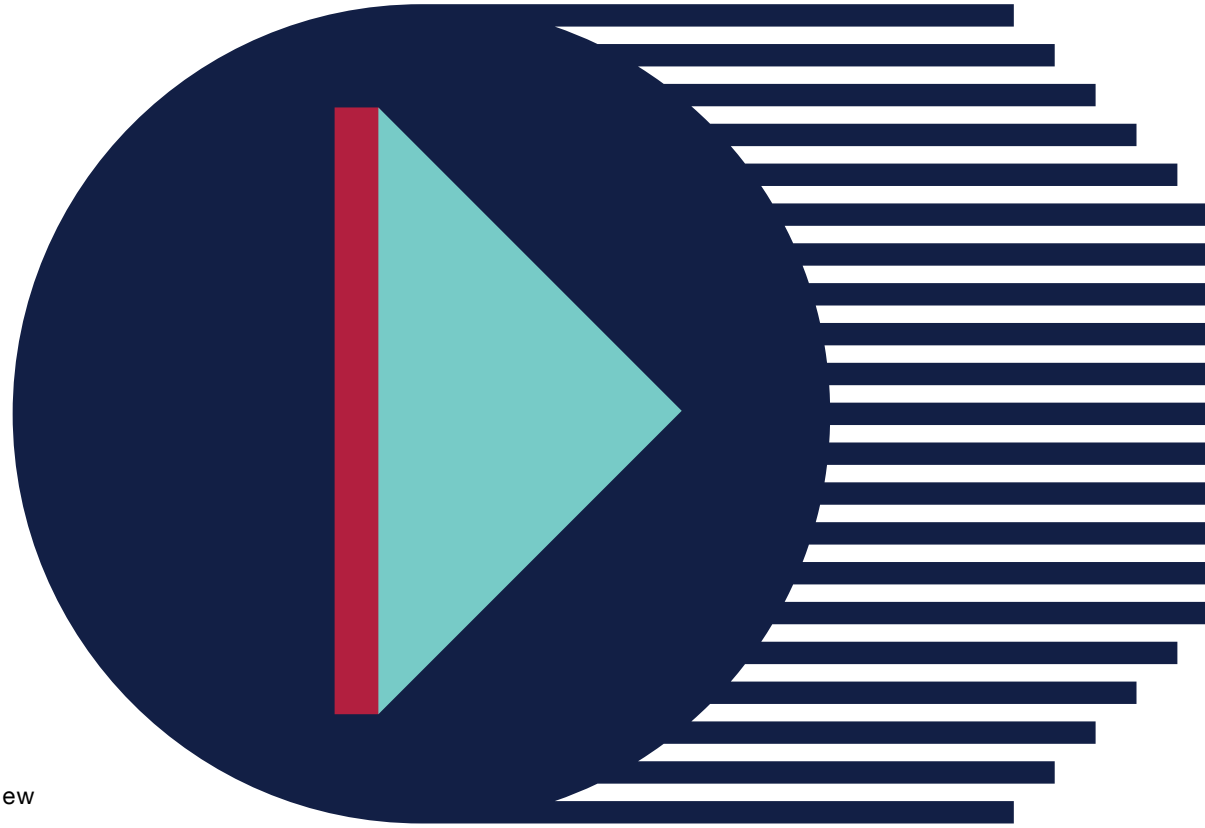
The Cyber Security Information Sharing Partnership

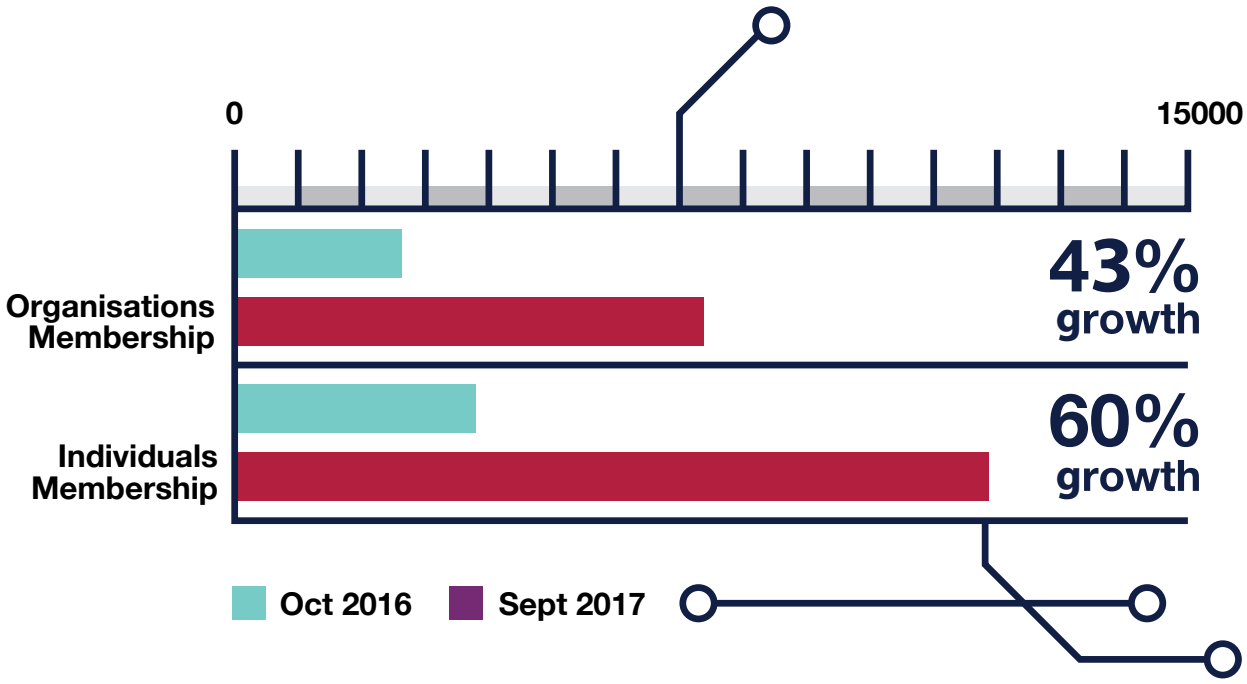
As a cyber organisation, we bring expertise together virtually as well as physically.

CiSP is a joint initiative between government and industry that provides a confidential environment where threat information can be quickly and securely exchanged.

The NCSC regularly publishes threat reports, advice and guidance to CiSP, which we produce with our industry partners. The platform receives more than 4,000 visitors per month and the community has grown by 43% in the last year, now boasting membership from organisations across 30 different sectors. Membership ranges from charities, businesses and academia to parts of the UK's critical national infrastructure.

CiSP has proven to be an extremely valuable resource during large-scale cyber incidents. Following the WannaCry ransomware outbreak there were more than 23,000 visitors to the online platform, including 15,000 during the first weekend. CiSP was invaluable, providing up to the minute mitigation advice whilst also debunking false rumours.





The NCSC website

Our website is also host to a wide range of regularly updated information. In the last 12 months, our experts have contributed 51 reports and 37 pieces of guidance or advice. Everything on the website is written for public consumption to ensure everyone can access our information as fully as possible.

Our communications team works both proactively and reactively with journalists to update the public with cyber advice through broadcast, print and online media. Our website has hosted verbatim transcripts of NCSC directors' speeches, 47 news items and press releases, and a weekly Threat Report that explores the most recent threats and vulnerabilities. As a result, our website has become a cornerstone of the cyber community – for example, receiving up to 100,000 visitors in a single month.

Complementing this work is the NCSC Twitter account, which has provided an invaluable service in keeping people updated by sending 2,000 tweets in one year.

Our security research and technical expertise have helped mitigate several critical security issues before they caused real harm. In the last year, the NCSC was publicly credited with the disclosure of many vulnerabilities, including in major software products in common use by UK Government, industry and citizens.


STOP

building the UK's defences

The NCSC is not waiting for attacks to happen – we are creating dynamic solutions to prevent as many as possible from getting through in the first place.

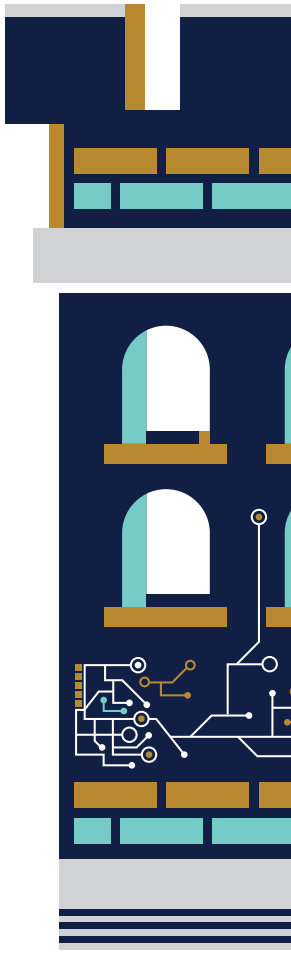
We are dedicated to reducing the cyber risk to the UK and helping businesses, people and government through our Active Cyber Defence programme and essential work to ensure our Armed Forces can operate effectively and securely.

active cyber defence

The NCSC has prevented waves of attacks through our Active Cyber Defence programme.

In June 2017, the NCSC launched four services as part of the programme which help to improve basic cyber security across the public sector. After the initial roll-out, we expect UK businesses to see the benefit from the increased protection of government's brand and be able to use some ACD services themselves in the future.

The four initial measures have already had a significant impact. They are simple to implement and will deliver strong benefits across the public sector.



1. Blocking fake emails

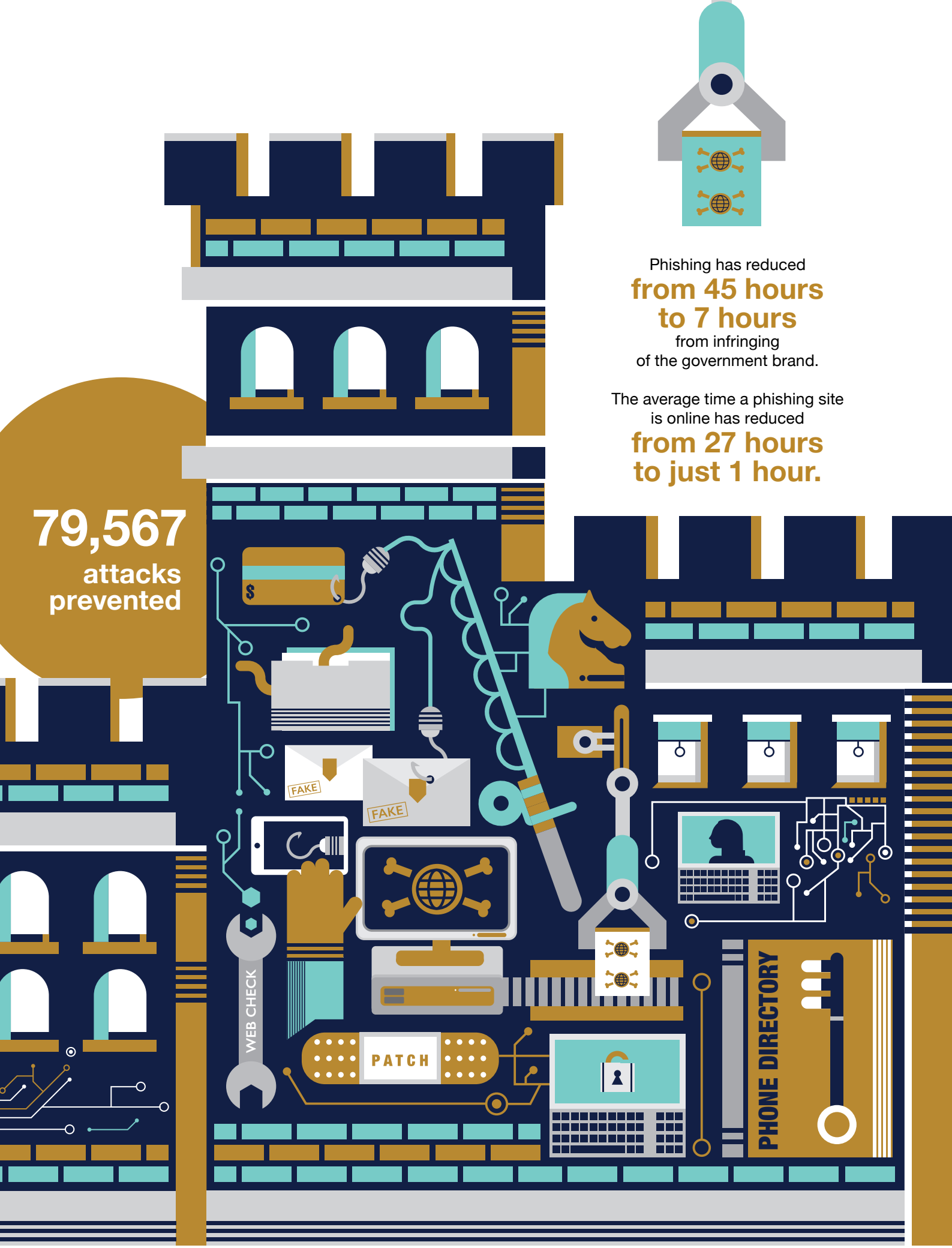
One of the biggest problems in UK cyber security is attackers spoofing the government to send fake emails. That is now much harder if bodies adopt the Domain-based Message Authentication, Reporting and Conformance protocol – better known as DMARC - which helps to authenticate whether the communications come from the said organisation.

The concept is simple. The most common way to expose victims' systems to attack is through email spoofing and spear-phishing (where emails are tailored to increase the likelihood of the recipient clicking on a malicious link).

Through this, attackers steal credentials that make identity fraud and theft easier.

In parallel, we have built the Mail Check service that monitors adoption of the standard and provides data on trends.

DMARC has already prevented a huge number of potential attacks – for example, blocking at least 120,000 emails from a spoof "@gov.uk" address.

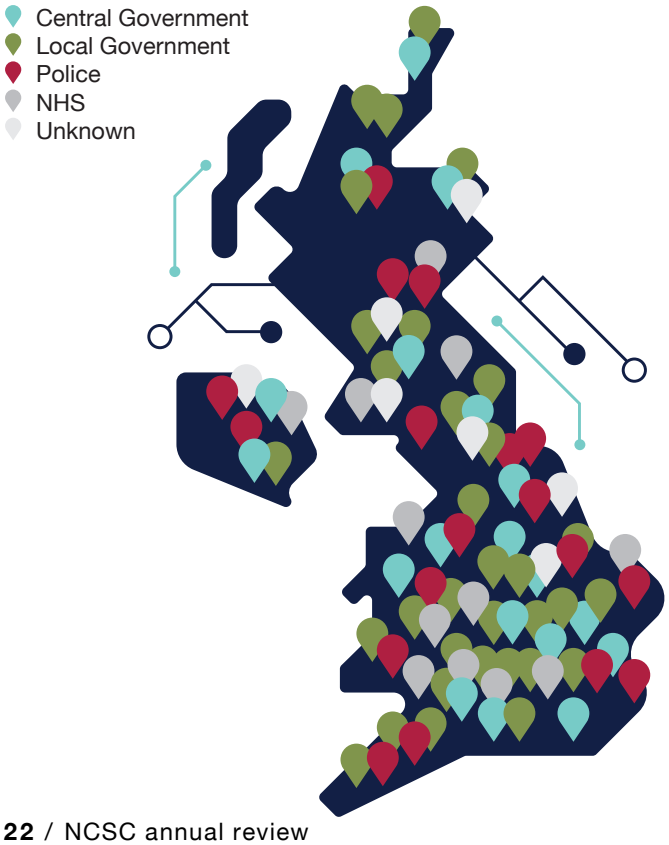

79,567
attacks
prevented
Phishing has reduced
from 45 hours
to 7 hours
from infringing
of the government brand.
The average time a phishing site
is online has reduced
from 27 hours
to just 1 hour.
FAKE
FAKE
WEB CHECK
PATCH
PHONE DIRECTORY

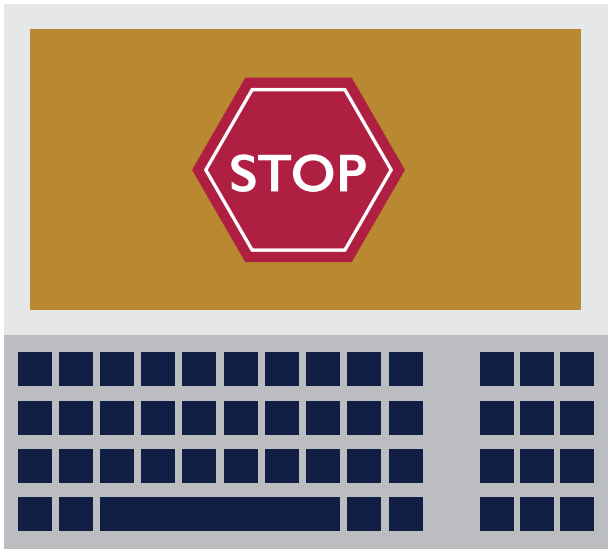
2. Stopping government systems veering onto malicious websites

Cyber attacks commonly involve redirecting a user away from the domain that they intended to access and on to a domain or website that contains malware or is fraudulent. We have worked with a commercial partner to set up a filtering service for public sector bodies that stops this from happening for registered users.

Domain Name Service (DNS) is the phonebook of the Internet, and our new service focuses on data gathered by GCHQ and commercial partners on malicious addresses or automatically detected by the analytics in the system. It then simply blocks the user from going there – providing automatic protection for staff visiting infected sites whilst using work systems.

Scanning public sector websites





51 organisations adopting the service. **20,410 unique domains** were blocked in August 2017.

3. Web Check: helping bodies easily fix website problems

The UK public sector has a huge digital estate to manage, and that isn't easy. Many organisations have told us they'd like help with staying protected against common problems. Web Check is a free-to-use website configuration and vulnerability scanning service, available to all UK public sector organisations.

Many websites are left unused or without updates for some time and provide a potential open goal for cyber criminals and others with hostile intent. Attackers learn what to target by scanning for vulnerabilities in internet facing services. We wanted to help potential victims do the same thing to easily identify weak spots and provide advice on implementing remedies. Web Check generates a plain English report on what needs fixing, and how to fix it.

4. Removing bad things from the internet (phishing and malware mitigation):

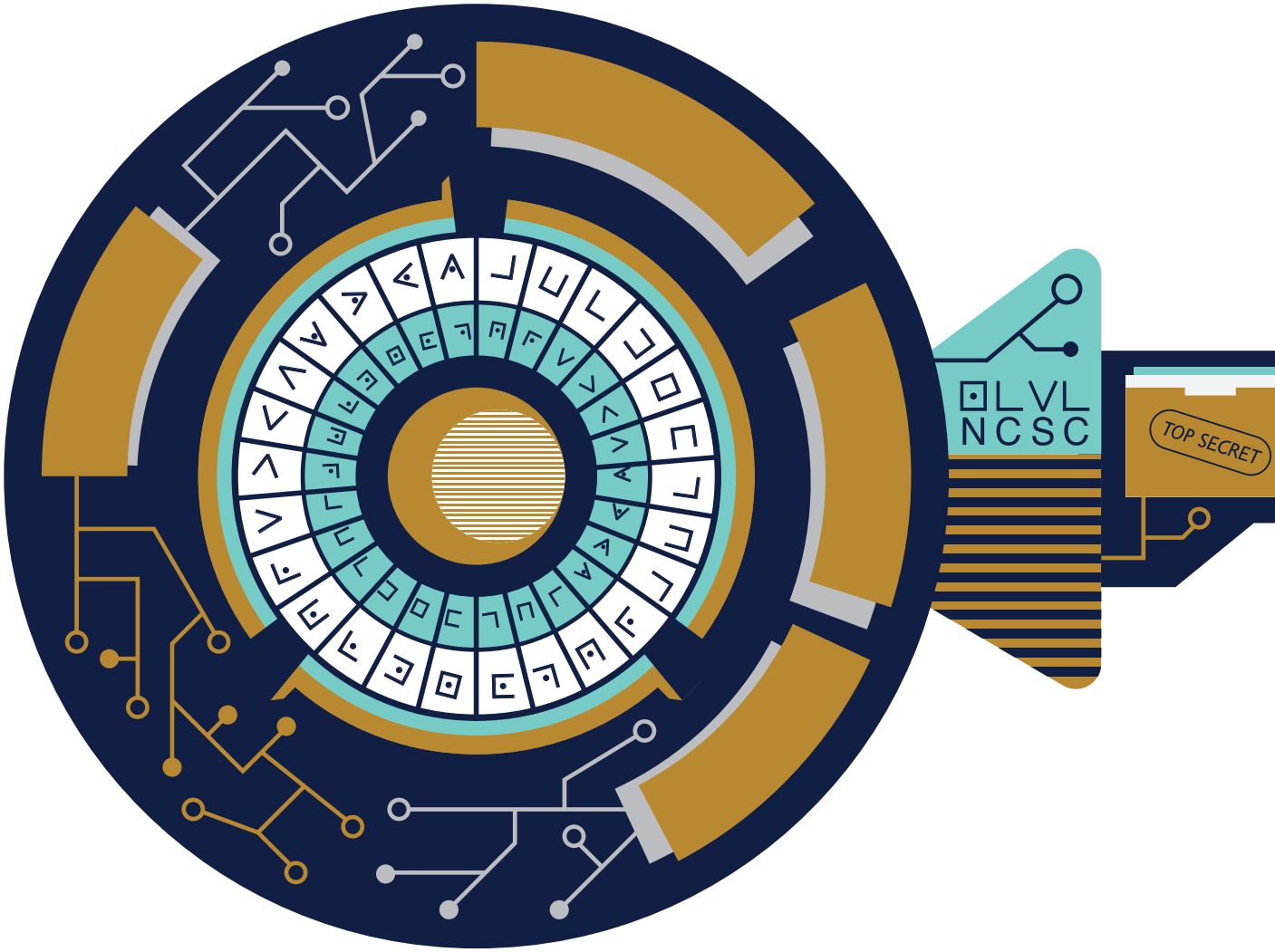
Since June 2016, the NCSC has worked with Netcraft, a private sector company, on a phishing and malware countermeasures service to protect government brands and UK hosting infrastructure. This is a protection from which government departments benefit automatically without having to do anything.

Departments can boost the service by notifying Netcraft if they themselves discover they are the target of a phishing campaign, or that there are malicious emails purporting to be from them. Netcraft then issues takedown notifications to the hosts of the email and phishing sites.

The cyber criminals who are behind these scams are seeing a much-reduced return. The Netcraft service is being expanded over the coming months to cover deceptive domains and malware apparently delivered by government.

> As one of the world's largest providers of cyber security services, BT is supporting the government's Active Cyber Defence strategy.
>
> We're already blocking tens of millions of malicious malware infections every week to protect consumers and businesses from online threats.
>
> With further technology enhancements in the pipeline, BT's pioneering cyber security capabilities will continue to evolve to keep pace with and thwart the efforts of cyber criminals.

Mark Hughes, CEO BT Security



The NCSC's technical work provides vital support for the UK's Armed Forces.

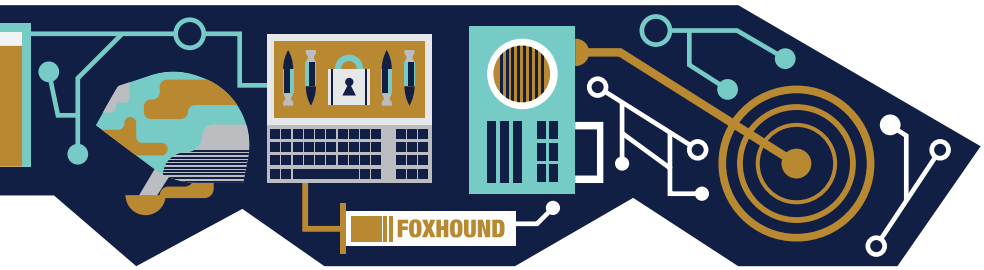
While the nature of some of our National Security work means it can't be discussed in detail, we are proud to provide this vital service to defend the country.

Our work in the encryption of communications and reliability of the systems that underpin them gives a foundation for the Government to build capability on. By ensuring systems are built to be digitally resilient, we ensure that communications can be trusted – especially in a time of crisis.

We provide robust levels of security to essential defence projects, allowing modern military platforms to operate effectively in the harsh environments they work in. Our deep expertise in cryptography and security, and world-leading knowledge and experience, allows us to support the operations of the UK's Armed Forces.

The UK Key Production Authority – which is part of the NCSC - produced approximately 200,000 physical items in the last year, delivering our services to 190 customer departments/ organisations across HMG including support to military operations, the wider public sector and the crypt key industry.

national security



Government and Defence activities supported by NCSC

Next generation of cryptographic products and services.

As part of an innovative joint programme with the Ministry of Defence (MoD), we are delivering the next generation of cryptographic products and services to protect defence capabilities. We are playing a crucial role in securing and growing our sovereign industrial capability in the Crypt Key arena, ensuring that it can deliver UK requirements and be able to deliver capabilities in the international market place.

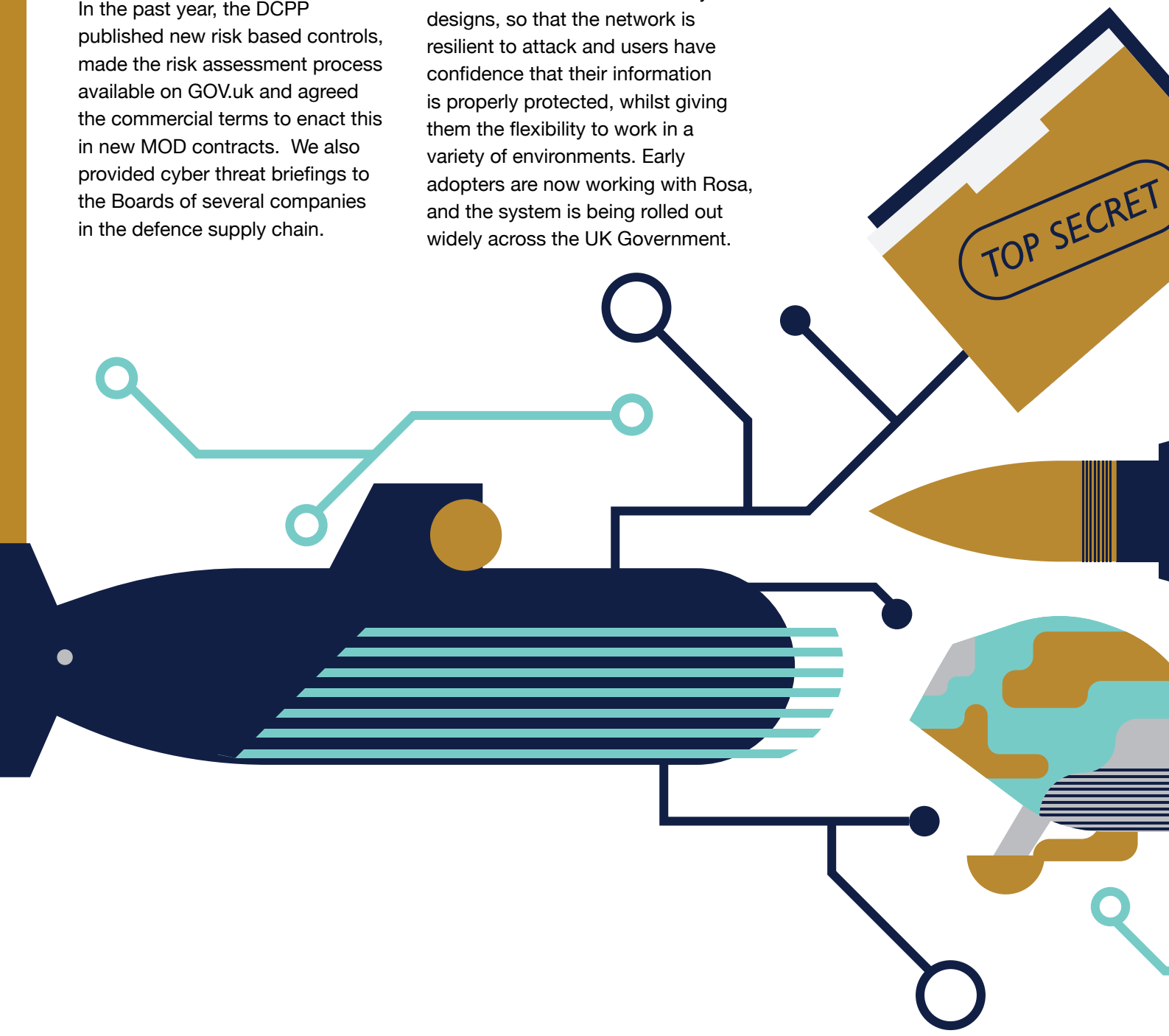
In September, we hosted the first technology day at our offices in Nova South for the High Assurance UK Trade Association, bringing together colleagues from industry, academia and others to discuss high assurance cyber security and how you create high confidence in digital systems to ensure you can be confident that they operate in the way they are intended.

Defence Cyber Protect Partnership (DCPP)

As part of the DCPP, we have been working with a joint team from the MoD and industry to improve the protection of the defence supply chain from the cyber threat.
In the past year, the DCPP published new risk based controls, made the risk assessment process available on GOV.uk and agreed the commercial terms to enact this in new MOD contracts. We also provided cyber threat briefings to the Boards of several companies in the defence supply chain.

FOXHOUND

The NCSC has supported the Cabinet Office led FOXHOUND programme to deliver a new pan central Government IT network (known as Rosa) for working at the Government security classification of SECRET. As a key advisor to the programme team, we helped develop the network architecture, and reviewed and advised on system designs, so that the network is resilient to attack and users have confidence that their information is properly protected, whilst giving them the flexibility to work in a variety of environments. Early adopters are now working with Rosa, and the system is being rolled out widely across the UK Government.



Emergency Services Network radio

We have also supported the Home Office in the crucial development of the **new** Emergency Services Network, ensuring that the network design is robust, secure, and resilient so that it is available for use in the challenging environment when it needs to be.

Electromagnetic Security and TEMPEST

The NCSC helps to increase understanding of how vulnerable ICT systems are unintentionally emitting potentially classified information, and helps to ensure that appropriate countermeasures are in place.
As world leaders in this field of TEMPEST, we are driving standards and capabilities both nationally and internationally. In October 2016, we hosted our international TEMPEST conference with representatives from 12 countries, to foster international collaboration in this field. We continue to evaluate and assure cryptographic products and cross domain solutions to provide assurance that products are cyber resilient.

Key relationships with industry and government

Relationships are key to the NCSC's success.

We foster relationships and encourage good practices with industry, suppliers and the varied users of technology and IT infrastructure, across the whole of the UK in both the public and private sector.

While prevention is better than cure, when a cyber security incident does occur the knowledge we have built is vital to our incident managers' understanding of how and who to engage when managing the impact and response.

Widening the cyber remit

Our predecessors focused mainly on central government, defence and the Critical National Infrastructure (CNI). The NCSC is here to support all sectors of the economy and we have consistently widened our reach during our first year. That's why we have created a new team to look at Economy and Society, reaching out to the voluntary sector, small and medium sized enterprises (SMEs) and educational institutions.

Earlier this year, we piloted our first Digital Government Loft where 70 representatives from local government, health, the emergency services and central government came to Nova South for a day of briefings and one-to-one consultancy sessions with our experts. It was a great success and we are now taking this out on the road, with the next events taking place in Shipley, West Yorkshire, and Scotland.

Critical National Infrastructure

The NCSC works to reduce the risks to the UK's CNI. We support owners, operators and suppliers in partnership with Lead Government Departments and the Centre for the Protection of National Infrastructure (CPNI) to ensure that security is considered holistically across cyber, physical and personnel security disciplines.

We conduct rigorous assessments of cyber risks with key companies across a range of sectors and have carried out design reviews of new critical systems. Our input has also helped to secure the UK's implementation of smart meters and developed sector-specific cyber security guidance.

A range of CNI sectors are covered by the EU Directive on Security of Network and Information Systems (the NIS Directive) and the NCSC will provide a set of top-level CNI cyber security principles, explanatory guidance and a Cyber Assessment Framework to support them.

The NCSC is working with industry partners to assess the current market place for cyber services to support CNI operators with training, testing and exercising. We will be developing a future way of working which will enable owners and operators to more easily access these services, facilitate more sharing of cyber security issues within and across sectors, and support the growth of the UK cyber services market.

economy and society

Large swathes of UK institutions fall outside the traditional public sector and critical national infrastructure. To address their needs, we have set up a dedicated engagement team concentrating their efforts among others, on retail, academia, and the voluntary sector.

Many companies have told us the first step for cyber security is the hardest. That's why we are developing the Cyber Security Small Business Guide - a series of simple, quick and inexpensive steps that any small business can work through to improve their resilience.

The NCSC has reached out to organisations delivering advice and guidance and gaining a better understanding of the risks and needs of a range of private, public and third sector organisations.

We have also developed key partnerships across government as well as with large enterprises, trade bodies, not-for-profit organisations and the NCA and police Regional Organised Crime Units (ROCUs).

We have worked alongside law enforcement's wide-ranging communications channels to share accurate and consistent advice with hard to reach groups. For example, our staff assisted ROCUs in understanding and prioritising the vulnerabilities of organisations and communities during the WannaCry incident. This meant the NCSC's guidance reached thousands of businesses and hundreds of thousands of individuals in the early stages of the incident – providing invaluable mitigation against the spread of the ransomware.

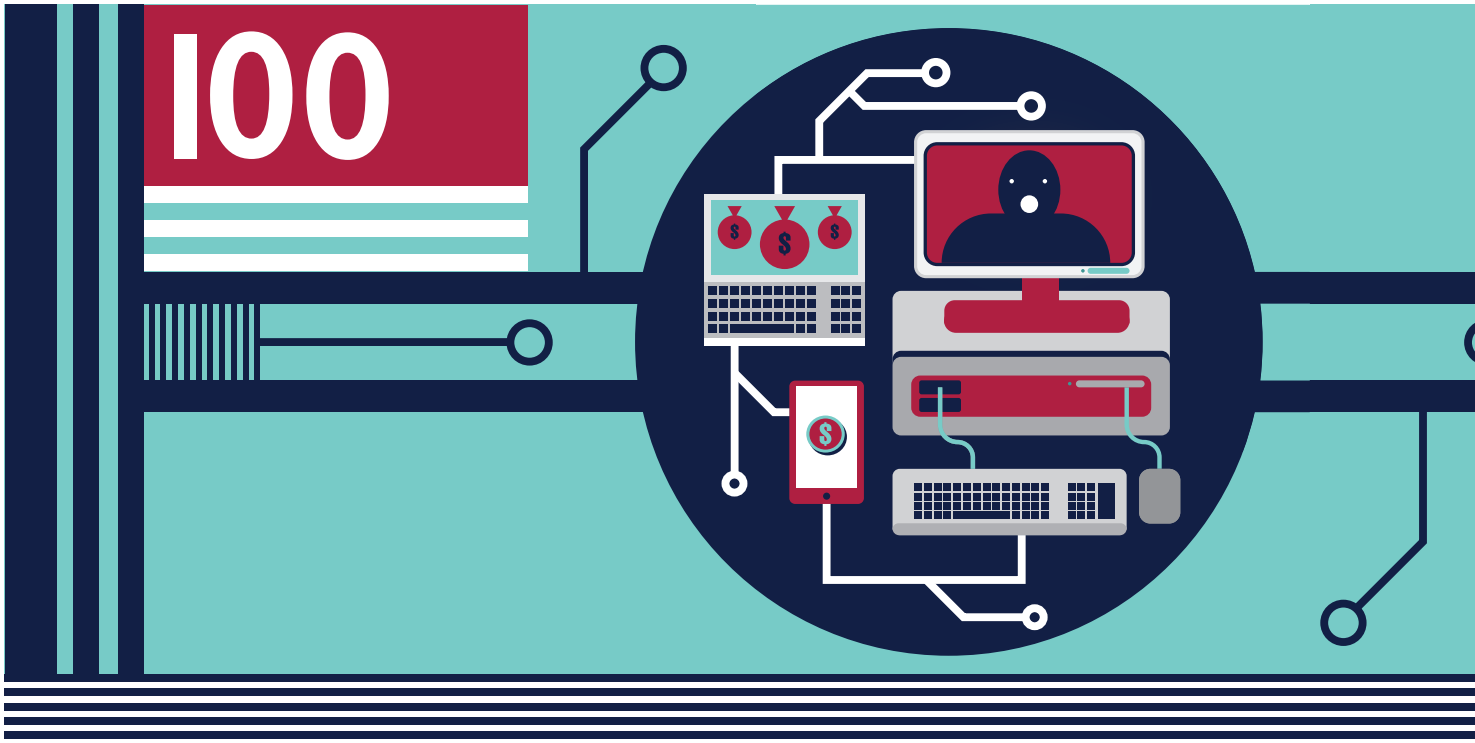
Economic sectors

With online retail sales increasing by around 10 - 15% annually, fraud and cyber crime is a growing concern, as is loss of personal data, of which retailers hold vast amounts. To understand the cyber security needs of this sector better, we work with large medium and small retailers all the way through to their supply chains.

Working with the British Retail Consortium (BRC), the NCSC developed several initiatives aimed at raising UK retail's cyber resilience capability – galvanising CiSP membership and partnering the BRC in producing a cyber security toolkit tailored to UK Retail's needs.

Educational institutions

The NCSC is forging new relationships with universities, colleges and schools to ensure advice and guidance is relevant, actionable and will help educational institutions better understand the threat and steps they can take to protect themselves. This will also include identifying specific requirements by working with key partners, such as the Department for Education and the Department for Business, Energy and Industrial Strategy.



Voluntary sector

We have begun to work with the voluntary sector to understand its specific needs to help protect them from cyber attacks and ensure they can keep their information secure. The sector is a vital part of society, delivering numerous important services to benefit the public. Many organisations in the sector hold sensitive data and information on vulnerable people and use online tools to raise funds.


STOP

cyber skills and growth

One of our core tasks is to help the UK prepare for future threats.

To do this, the NCSC actively promotes a culture where science and technology can thrive. We work tirelessly to help companies develop cutting edge ideas and ensure the next generation of frontline cyber experts flourish in an education system that supports the skills they will need.

As the lead technical authority on cyber issues, we are doing everything we can to remove any barriers preventing talented people from entering the sector.

That's why we are challenging the stereotype of the technology industry being male-dominated.

CyberUK 2018 will have a focus on women in cyber security. We have plans to create a mentoring programme and are developing a 'cyber code of conduct' to facilitate greater gender equality within the sector. Half our senior management team are women and close to a third of our staff are female – a figure we are keen to improve further.

CyberFirst

CyberFirst is a pivotal part of the UK Government's National Cyber Security Programme (NCSP), supporting UK national security by identifying and nurturing young talent. CyberFirst Girls is aimed at inspiring girls and young women to consider a career in technology and cyber security.

More than 20 cyber security companies were involved in the first year of the programme. Here are some examples of the great work CyberFirst has done.

> After enjoying the CyberFirst course, I know that cyber security is the career for me. We had some amazing speakers, and they far exceeded what I expected. I enjoyed my time at CyberFirst Futures and I will 110% be signing up for CyberFirst Advanced next year.
>
> **Harry (16)**

CyberFirst summer activities

1,060 budding cyber experts aged 14 to 17 - of which 44% were female - attended our summer courses across the UK. The short programmes, including expert speakers, introduce young people to the fascinating world of cyber security.

CyberFirst Girls Competition

This competition was created to inspire girls to consider a career in cyber security. 2,171 teams entered the competition this year, consisting of more than 8,000 girls aged 13 to 15 years old, with the top ten teams qualifying for the grand final in London. This year's winners were from Lancaster Girls Grammar School, whose pupils Emily, Evie and Lauren entered under the team name 'Circular Logic'.

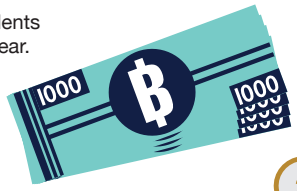
Our second CyberFirst Girls competition will take place from January to March 2018. This year the age limit for the competition will be for Year 8 girls only, aged 12 to 13.

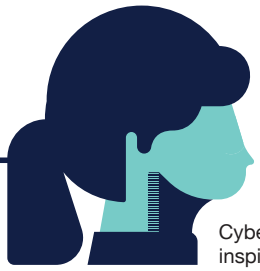
> The thing we enjoyed most about the CyberFirst Girls competition was the ability to see our progress. We learnt a lot about cyber security in the process - and we would now definitely consider careers in Computer Science
>
> **Winners of our CyberFirst Girls contest Lauren, Evie and Emily (all 15), from Lancaster Girls' Grammar School**

The UK needs capabilities to protect against future threats

The NCSC nurtures talent from school, through university, and beyond, to ensure there are no barriers to entering the sector.

The CyberFirst bursary programme provides students with £4,000 funding per year.





CyberFirst is a programme to inspire young women to consider a career in cyber security.

We received more than 1,500 applications for 250 places – an increase of **76%** from last year.

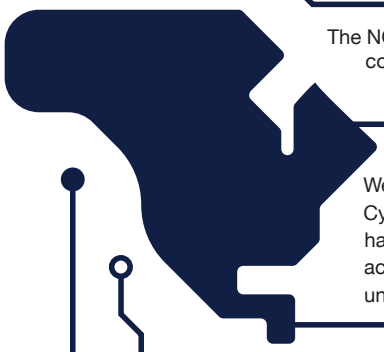
More than **8,000** girls ages 13-15 entered the CyberFirst Girls Competition.

1,060 budding cyber experts aged 14-17 attended our summer courses, introducing young people to cyber security.

44% of this year's attendees were female.

The NCSC have certified Bachelors degrees for the first time this year, with the number of Masters being endorsed rising to 25.

The NCSC sponsored the annual Cambridge2Cambridge competition, testing some of the brightest young minds in UK and US Cyber Security.



We certified **14** Academic Centres of Excellence in Cyber Security Research (ACEs-CSR), including The University of Edinburgh, the first ACEs-CSR in Scotland.

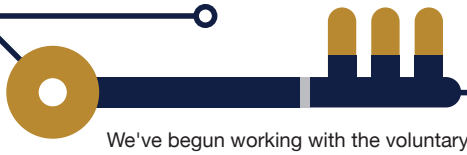
We currently work with 28 CyberInvest partners who have invested **£2.8m** across 30 different British universities up to March 2017.

More than 7,900 Cyber Essential certificates have been issued since June 2014, encouraging basic cyber security measures across UK organisations.

During WannaCry, the NCSC utilised law enforcement's wide-ranging communications channels. This provided invaluable mitigation against the spread of the ransomware.

The Cyber Security Small Business Guide offers small businesses simple, quick and inexpensive steps to improve their resilience.

As more shoppers move online, we worked with the BRC to create a toolkit to help UK retailers increase their cyber resilience.



We've begun working with the voluntary sector to understand its needs and protect them from cyber security threats.

Science and Technology

Cyber Essentials

Our flagship scheme for encouraging UK organisations to implement basic cyber security measures continues to grow. More than 7,900 certificates have been issued since the beginning of the scheme in June 2014, with just over half of them issued since the start of the NCSC. Our new microsite on the NCSC website will soon provide an enhanced experience for all users of the scheme. This includes the development of a brand-new database holding all certificates that will allow customers to validate their supply-chain credentials in one place.

Cyber Security Accelerator

Launched in collaboration with Wayra and DCMS, the cyber security accelerator gives successful applicants access to our world-class experts to allow them to devise cutting-edge products. Based in the Cheltenham Innovation Centre, the first three-month programme ended in March. CyberSmart, one of the beneficiaries of the accelerator, now has an easy to use, cost-effective tool that can be used to help companies apply for Cyber Essentials certification. The success of the first programme has led to the second one running for nine months when it starts this Autumn.

Research Institutes

The NCSC and the EPSRC have expanded the Research Institute programme to develop UK cyber security capability in strategically important areas. As well as securing continuation funding for the existing organisations, we are also establishing a new virtual academic research institute investigating topics relating to hardware-enabled security.

CyberUK conference

As well as creating a talent pipeline for tomorrow's cyber experts, the NCSC also facilitates unprecedented engagement for the existing community through a range of events.

Our flagship event is CyberUK – a three-day conference that takes place annually. This provides a forum to share our strategy and provides industry a chance to meaningfully engage in a shared dialogue to work towards achieving a step change in UK cyber resilience.

Our 2017 conference took place at the Liverpool Arena, and gave a powerful platform for the entire cyber security community. Our event included an all-star line-up of UK and international cyber security experts from government, industry, the CNI and academia.

Taking place only six months after the launch of the NCSC, 94% of delegates said that they had increased their understanding of why the NCSC has been created, our structure, approach and its role in the implementation of the National Cyber Security Strategy.

CyberUK is all about the interaction between government and industry. This year, participants were encouraged to interact and feedback at numerous touchpoints - reflecting the NCSC's commitment to openness, collaboration, supportiveness, creativity and inspiration. The event has helped the NCSC, together with industry to achieve a sense of common purpose and collaboration amongst the nation's cyber security community, bringing together seniors and practitioners alike.

With such good feedback from this year's event, and with 99% of surveyed visitors saying they'll be returning next year, we're delighted to say that in April we'll be hosting CyberUK18 in Manchester.

National Cyber Security Centre
INDUSTRY 100

> One of the major benefits of being part of Industry 100 is working alongside the leading experts in cyber security.
>
> This includes not only those from GCHQ and wider government, but the collaboration with other infosec professionals from Industry.
>
> The work is challenging, engaging and highly rewarding. Knowing that your work is contributing to the cyber reliance of the UK is something that cannot be under estimated. During my tenure, I have improved my knowledge and skills no end.
>
> **Mike from TLM NEXUS**

The NCSC has co-ordinated an unmatched collaboration between public and private sector organisations to reduce the cyber risk to the UK. Through the pioneering Industry 100 initiative, launched by the Chancellor Phillip Hammond, organisations of all sizes and sectors have been invited to work directly with us. We are working with or embedding one hundred external staff into the NCSC, so that industry can directly challenge our thinking, and help us achieve a greater understanding of the cyber security environment, which will benefit both government and industry alike.

The initiative has attracted analysts, network defenders, academics and engagement partners to work alongside us on the issues that matter. Already this year we've had a hugely positive reaction, and Industry 100 includes a variety of organisations from multinationals banks, to regional SMEs in the UK.

For our upcoming year, the NCSC is establishing an oversight board for the organisation which will consist of experts from the heart of UK industry and senior civil servants. Transparency is fundamental to the NCSC, and the panel will help provide the strategic direction of the NCSC as we head into our second year, and we will be inviting members to join before the end of 2017.

> Being at the NCSC means being in the middle of the action; being up to date on all the cyber security challenges and threats facing the UK
>
> **Kirsten from BAE**

working at home and abroad

Cyber attacks know no borders and the NCSC is a truly global organisation.

We bolster our expertise by working with countries all around the world, helping to develop mitigation techniques and sharing information. The NCSC has worked with more than 50 countries across five continents. The year has seen ever closer working relationships with colleagues from the European Union.

Throughout the year, senior NCSC representatives have worked with the international community and promoted our centre's expertise and the role we play in the UK Government. The visits have included influential speeches by our Technical Director Dr Ian Levy at Cyber Week Tel-Aviv and NCSC CEO Ciaran Martin at the EU Cyber Security Conference in Tallinn.

In February 2017, NCSC Director of Operations Paul Chichester signed a Memorandum of Understanding to deepen the UK's cyber defence co-operation with NATO. The Memorandum will enhance collaborative working, information sharing and improve cyber incident prevention, resilience and response capabilities.

This close co-operation is hugely productive. For example, following the visit of Japanese Prime Minister Shinzō Abe we have agreed to deepen co-operation with the nation on cyber security ahead of their hosting of the 2019 Rugby World Cup and 2020 Tokyo Olympics and Paralympics. Our respective experts will share best practice and expertise, including through an exchange of expert visits. The UK's support, built on decades of expertise in managing cyber crime and other malicious cyber activity, will help enhance the Games' security.

Paul Chichester, pictured left, with NATO's Assistant Secretary General Sorin Ducaru

> In line with our Cyber Defence Pledge and Strategic Defence and Security Review commitments, NCSC will use its intelligence capabilities and world-class technical insights to work with NATO and our allies to better protect our networks.
>
> **Paul Chichester on signing the Memorandum of Understanding with NATO**

Devolved Administrations

As well as working with the international community, we are also committed to developing our ties with the Devolved Administrations, Crown Dependencies and British Overseas Territories where appropriate.

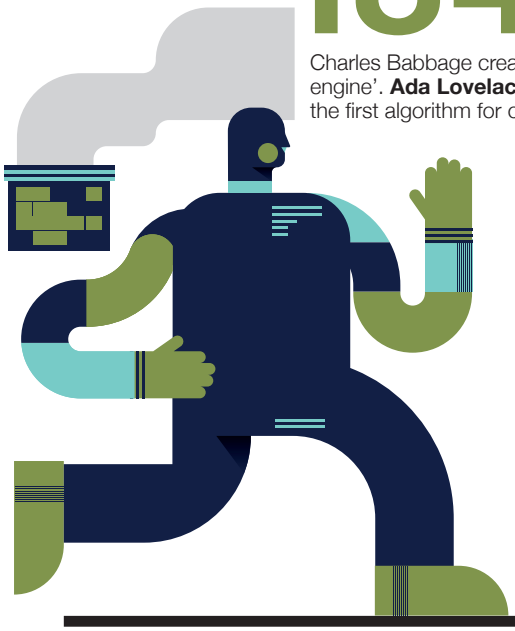
By the end of October, our Chief Executive Ciaran Martin will have visited Scotland, Wales and Northern Ireland to support their initiatives to build cyber security awareness and their adoption of good cyber security practices. During Ciaran's trip to Edinburgh in September, he announced the creation of a permanent NCSC post in Scotland.

Our Operations Director, Paul Chichester, has visited north and south Wales, sharing best practice and working with the Welsh Assembly and cyber security clusters to ensure best cyber practice for government and businesses alike.

The history of cyber

1840s

Charles Babbage creates the 'difference engine'. **Ada Lovelace** assists by creating the first algorithm for computing



Alan Turing writes a paper **On Computable Numbers**, proposing a ***universal computing machine***

Emergency codebook issued to national authorities during the General Strike

Government Code and Cypher School (GC&CS) established with intelligence and security functions

First Typex (UK electromechanical encryption) machine manufactured

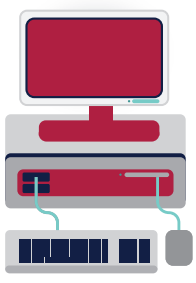
1919 **1926** **1936** **1937**

1988 **1989** **1994** **1997** **1999** **2008**

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

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

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



Commodore 64 ends production. 15,000,000 units sold - the bestselling computer of all time

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

First iPhone (2007) launched followed a year later by Android phones

Colossus

The first **Colossus** computer, the proto-computer, was created for the **Newmanry** section at Bletchley Park

1943

1944

Single national authority for communications security established

1953

World's first transistored computer built at University of Manchester

1960s

Concept of microprocessors is born - leading to the first CPU in 1971

1969

GCHQ incorporates the Communications-Electronic Security Group (CESG) becoming National Technical Authority for all aspects of cryptology

1970

Public key cryptography conceived by James Ellis at GCHQ

1971

Ray Tomlinson emails himself. The first ever email sent over an early version of the internet

1981

Early malware begins to be discovered at scale. A year later, Elk Cloner spreads beyond the lab it was created in

2010

The UK Government puts the Cyber Threat as a tier one risk to national security in the National Cyber Security Strategy

Start of the first UK National Cyber Security Programme

2013

NCA and its National Cyber Crime Unit launched

2014

More devices connected to the internet than people on the planet

CERT-UK, the national computer emergency response team, launched

2016

NCSC created from parts of CPNI, CERT-UK, CESG, GOVCERT, and the Centre for Cyber Assessment

2017

53% of all UK fraud is online - 1.9m offences. British citizens are 20 times more likely to be defrauded at their computer than held up in the street

National Cyber Security Centre
a part of GCHQ

did you find the secret codeword?

Add it to the end of our website address to learn more
www.ncsc.gov.uk/[codeword]