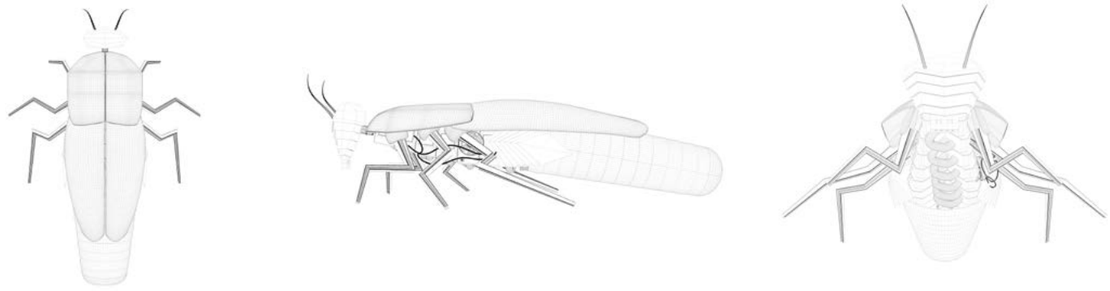
National Cyber Security Centre
a part of GCHQ

Annual Review 2018

Making the UK the safest place to live and work online



Welcome

The National Cyber Security Centre (NCSC) was created in 2016 as part of the Government's five-year National Cyber Security Strategy. Since then, our goal has been to make the UK the safest place to live and work online. This review tells the story of our second year, with interviews, testimonials, images and data that take you behind the scenes at the NCSC. It provides a snapshot of our work over the period 1 September 2017 to 31 August 2018. We hope it helps you understand what we do, and along the way see some of the milestones we have reached in our second year.

We have also produced a digital report where you can see this year's events come to life at:

ncsc.gov.uk/annual-review-2018

National Cyber Security Centre
a part of GCHQ

Ministerial Foreword

We have every reason to be proud of the UK's position at the forefront of the global digital revolution. Our collective ability to embrace cyberspace is already driving our country's prosperity and enhancing our national security. We have one of the highest levels of internet access and usage in the developed world, and our digital industries are growing faster than any other part of the economy. At the same time, the threat from criminals, hacktivists and nation states continues to increase and evolve. It is easier and cheaper than ever before for those who want to do us harm to access the tools, exploits and services they need to launch attacks. That is why cyber security remains a top priority for this government and for me personally, as the Minister responsible for improving the security and resilience of the UK, including protecting our critical national infrastructure.

We launched our National Cyber Security Strategy in 2016 to set the direction and ambition for our investment and efforts. Because as the digital revolution touches every part of our society, we wanted to ensure that our response was comprehensive. To defend our people, to deter our adversaries and to develop the capabilities we need to ensure the UK remains the safest place to live and work online. Our strategy is supported by significant investment – £1.9bn – to drive the transformation we need to respond at the scale and pace required.

We have made good progress since we launched the strategy. At the heart of our response was the formation of the National Cyber Security Centre, which brings together our best intelligence and expertise to be our single centre of excellence. This Annual Review recognises the transformational impact of the National Cyber Security Centre over the last year. As well as providing greater insight into the nature of the threats we face, the National Cyber Security Centre's successes include a pioneering Active Cyber Defence programme, delivered with industry to block attacks on a scale of millions per month, and the development of a world-leading incident management response capability, made possible through key partnerships with law enforcement and the wider cyber security community. It has also reached out internationally to strengthen global cyber defences and our collective ability to deter and disrupt malicious actors, and continues to inspire the next generation of cyber security experts and entrepreneurs.

There are many more achievements to celebrate in this Annual Review. Everyone at the National Cyber Security Centre, and its numerous partners in the public, private and voluntary sectors, should take great pride in this work. How we set up the National Cyber Security Centre reflects the single, clear message that underpins our strategy, that while we can lead the way, we cannot solve these problems alone. We need not just a whole of government but a whole of society approach to tackle cyber security.

The future remains stubbornly difficult to predict. But we do know that the next 12 months will continue to challenge and surprise us. We have built solid foundations to ensure that we can remain resilient in an ever changing world. Key to our success will be how we take on longer-term, strategic challenges, whether that is affecting behaviour change, developing the right skills set among UK professionals, or deepening our collaborative partnerships in the UK and internationally. Because whatever the future holds, we will need to continue to work together to protect our economic and individual freedoms.

Rt Hon David Lidington CBE MP
Minister for the Cabinet Office and the Chancellor of the Duchy of Lancaster

Contents

2017

3 Oct	1ST ANNIVERSARY OF THE NCSC CELEBRATED
11 Oct	SMALL BUSINESS GUIDE PUBLISHED
23 Oct	SECURING ELECTIONS FOR EU MEMBER STATES SUMMIT HELD AT NCSC HEADQUARTERS

2018

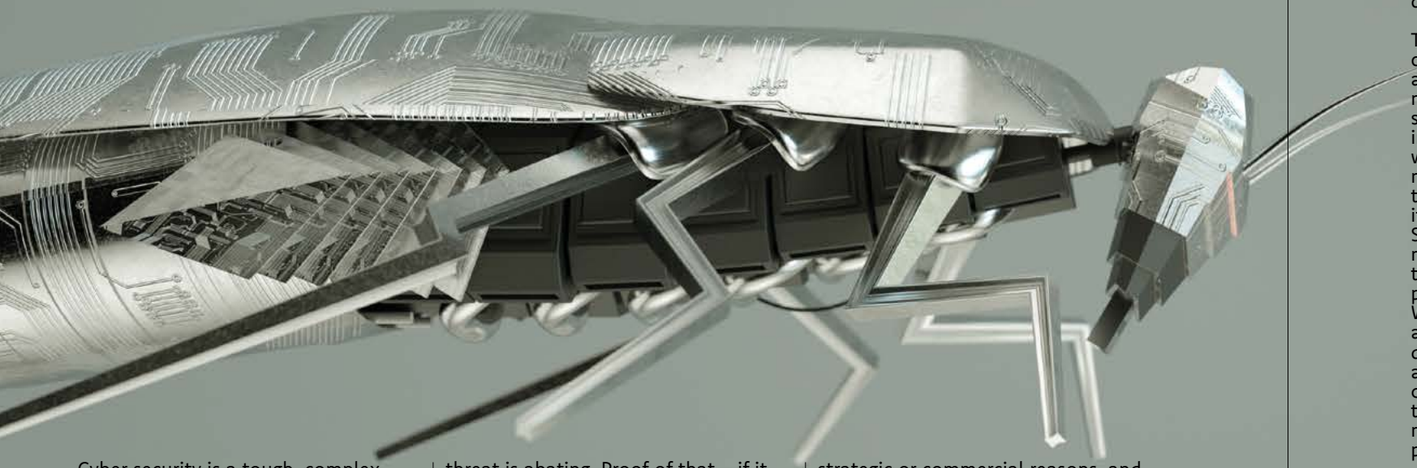
5 Feb	ACTIVE CYBER DEFENCE: ONE YEAR ON REPORT PUBLISHED
1 Mar	CHARITY SECTOR THREAT ASSESSMENT AND SMALL CHARITY GUIDE PUBLISHED
19 Mar	CYBERFIRST GIRLS COMPETITION FINAL TOOK PLACE IN MANCHESTER
10–12 Apr	CYBERUK 2018 HOSTED IN MANCHESTER
10 Apr	CYBER THREAT TO UK BUSINESS JOINT REPORT WITH NATIONAL CRIME AGENCY PUBLISHED
16 Apr	U.S-UK TECHNICAL ALERT ISSUED ON RUSSIAN MALICIOUS ACTIVITY
18 Apr	PRIME MINISTERS OF THE UK, CANADA, NEW ZEALAND AND AUSTRALIA MET AT THE NCSC AS PART OF THE COMMONWEALTH SUMMIT
3 May	GUIDANCE FOR LOCAL AUTHORITIES AHEAD OF LOCAL ELECTIONS PUBLISHED
9 May	NETWORKS AND INFORMATION SYSTEMS DIRECTIVE CAME INTO EFFECT
25 May	GENERAL DATA PROTECTION REGULATION CAME INTO FORCE
25 June	THE NCSC'S CEO AND THE MINISTER FOR THE CABINET OFFICE GAVE EVIDENCE ON THE CYBER SECURITY OF THE UK'S CRITICAL NATIONAL INFRASTRUCTURE TO THE JOINT COMMITTEE ON THE NATIONAL SECURITY STRATEGY
27 June	NINE START-UPS GRADUATED FROM THE NCSC CYBER ACCELERATOR
Jul–Aug	HELD CYBERFIRST SUMMER COURSES FOR YOUNG PEOPLE ACROSS THE UK
19 Jul	CYBER THREAT TO LEGAL SECTOR REPORT PUBLISHED
22 Aug	THREE NEW ACADEMIC CENTRES OF EXCELLENCE IN CYBER SECURITY RESEARCH ANNOUNCED

Timeline

This covers the period 1 September 2017 to 31 August 2018

- Handled **557** incidents
- Removed **138,398** unique phishing sites
- Produced **214** threat assessments
- Produced **145,000** physical items for **170** customer departments through the UK Key Production Authority
- Produced **134** pieces of guidance and **95** blogs
- Had **1.9 million** visitors to our website
- Awarded more than **8,900** Cyber Essentials certificates
- Added **2,361** new members onto our Cyber Security Information Sharing Partnership
- Engaged with **1,968** students on our CyberFirst courses
- Challenged **4,500** girls in the 2018 CyberFirst Girls Competition
- Delivered cyber security awareness sessions to more than **1,000** charities
- Welcomed visiting delegations from **54** countries
- Hosted more than **80** stakeholder events

CEO Overview



Cyber security is a tough, complex challenge. But the UK is making significant progress in strengthening our defences against those who seek to harm us online. This matters as we look to an ever more digital future for our prosperity.

In this report – GCHQ's National Cyber Security Centre's second Annual Review – we set out:

- the latest overview of the threats we face;
- the progress we've made in meeting them, including some world-leading initiatives to rectify some of the systemic security weaknesses of the modern Internet;
- the cyber security challenges facing families, businesses, critical network owners and government, and what they can do to meet them; and
- our plans for the future.

Although the UK is making significant progress in improving our cyber security, that does not mean that we are getting everything right, or that the threat is abating. Proof of that – if it were needed – is that in the two years of our existence the NCSC has dealt with well over 1,000 cyber security incidents.

The majority of these incidents were, we believe, perpetrated from within nation states in some way hostile to the UK. They were undertaken by groups of computer hackers directed, sponsored or tolerated by the governments of those countries. These groups constitute the most acute and direct cyber threat to our national security. I remain in little doubt we will be tested to the full, as a centre, and as a nation, by a major incident at some point in the years ahead, what we would call a Category 1 attack.

Although there have been several very significant incidents, thus far, the UK has avoided a Category 1 – most of our foremost international partners have not. But even if this continues, we must be alert to the constant threat from countries who will attack critically important national networks to steal information for strategic or commercial reasons, and give themselves a starting point – 'prepositioning' – for a significant attack in the future.

That's why earlier this year, along with the Government of the United States, the NCSC published evidence of Russian pre-positioning on some of our critical sectors, along with detailed technical guidance to business on how to get rid of it from our networks.

That landmark publication – not just calling out unacceptable behaviour but providing the tools to clean it up – was one example of how we've been moving in the right direction over the past year. It built on other, similar publications where we have drawn on an array of technical data – some classified, some not – and published transparent, technically authoritative guidance on it. These attacks have come from a range of states, as well as many non-state sources. There is much, much more to the cyber security threat to the UK than just Russia.

This practical guidance really matters, because victims of cyber crime tend to be less concerned with the identity of the attacker than the impact on their lives and wellbeing, and what they can do to contain the damage.

Indeed, whilst nation state activity is the most acute threat, low-sophistication but high-volume cyber crime is the most chronic one, dealt with at scale by our first-rate partners in law enforcement, led by the National Crime Agency (NCA).

Whilst these incidents individually are of less strategic significance, cumulatively they amount to a strategic threat to our prosperity by undermining our confidence in the digital economy.

That is why our world-leading active cyber defence (ACD) initiative – using automation to reduce some of the most common weaknesses in cyber security defences – is one of our most important pieces of work. The Internet was not designed with security in mind and, from a security perspective, there are significant flaws in the way it operates. In the 2016 National Cyber Security Strategy, the Government made a major strategic decision to try to redress some of those structural problems through the ACD programme. We were the first in the world to attempt this, reducing the damage done by large scale but basic cyber attacks, freeing up our world-class operatives to focus on the most potent threats. Our aim is to take away as much of the harm from as many people as we can, as often as we can.

In February this year, our Technical Director, Dr. Ian Levy, published a groundbreaking paper setting out the results of the first year of the programme. The latest results show that since the programme started, the proportion of phishing sites in the world that are hosted in the UK has fallen from 5.3 per cent to 2.4 per cent. This, and other impressive results, means we are going to roll out existing measures further, and expand the programme over the next few years.

The ACD programme shows what government can do directly to improve cyber security. But getting ahead of the problem involves equipping every organisation, however large or small, with the tools they need to protect themselves as best they can. Getting the right cyber security capabilities for an organisation starts with a better understanding of the risks. No one is asking British citizens and businesses to have cyber defence capabilities akin to those of a nation state. They just need to be good enough to fend off what an organisation can reasonably assess to be the risks it faces. Defences also need to be good enough to contain attacks that do get through, as some inevitably will.

Therefore, understanding how cyber attacks work is vital to get ahead of the problem. That's why we've started publishing guidance to boards on the types of questions they can ask their cyber security teams about how they are managing risk. More will follow, with the aim of helping leaders understand enough technical detail to make the right decisions. These are the sorts of practical steps companies can take to make the marginal improvements that will deter some attacks, make some others less likely to succeed, and lessen the impact of attacks that get through. This was launched with support from the CBI – an example of government and industry partnership at its best.

Through our work on incidents over the past year in particular, we have become acutely conscious of the role the supply chain plays in leaving organisations vulnerable to compromise. As the next generation of technology evolves, supply chain risk becomes an ever more important challenge. Meeting it, particularly in the telecommunications sector as the age of 5G approaches, is a top priority for the NCSC, supporting the lead of the Secretary of State for Digital, Culture, Media and Sport, and his department. That's a key challenge for our experts who lead on our programme to protect the nation's most critically important networks, alongside their work on our social security payments systems, the new generation of civil nuclear reactors, our systems to protect our national defence secrets, and the payments and clearing networks that underpin the UK's world-leading financial system.

Finally – for us, heading in the right direction means becoming a truly national centre, reflecting, and being present in, the communities we serve. We remain very proud of our work on skills in schools, particularly our CyberFirst Girls Competition which this year attracted more than 4,500 highly talented 12 and 13-year-old female students with an interest in cyber security. Although just over half of the NCSC's senior leadership are female, there remains a mountain to climb within government service and nationally to harness the power of all sections of the population and end the serious underrepresentation of all minority groups within the profession.

We will also continue to expand our footprint geographically. We held our first ever CyberFirst event in Northern Ireland this summer; we have a permanent member of staff based in Scotland, and Glasgow will host our flagship CYBERUK event in 2019; Cardiff University's success in becoming one of our most recent Academic Centres of Excellence in Cyber Security Research means all four parts of the UK now host one of these centres. And like the rest of GCHQ, we maintain presence in London, Cheltenham, Bude and Scarborough, and we will look to expand our presence in Manchester in the coming years.

This expansion of our national footprint will help us further make a mark on UK cyber security at every level. There is a real opportunity here – there are already signs that other countries' admiration for what the UK is doing in cyber security could secure a competitive advantage for the country in our digital future. As GCHQ begins its second century of service to the UK, it is an exciting time for its newest part, the NCSC.

So let me conclude by paying tribute to our exceptional teams, as well as to our partners in the security and law enforcement communities, within wider government, in industry and other organisations nationally and abroad. Moving forward on all fronts – using world-class data and skills from GCHQ and our partners at home and abroad; publishing clear, technically authoritative guidance to individuals and businesses; fixing some of the underlying security problems inherent in modern technology; and enhancing and diversifying our skills base – are vital for our third year and for our mission to help make the UK the safest place to live and work online.

Ciaran Martin,
CEO of the National Cyber Security Centre

1. Countering the Threat

At the NCSC, we take a proactive approach to securing the UK's online defences at home and collaborating with our allies overseas. Instead of waiting for an attack, we anticipate problems and find solutions to prevent them doing harm.

Active Cyber Defence

Active Cyber Defence (ACD) is a collection of services that aim to protect the UK from the high-volume commodity attacks that affect people's everyday lives. These attacks involve using tools and techniques openly available on the internet that are relatively simple to use.

We have developed and tested our ACD services on government with great success. Our longer-term goal is to encourage solutions like these to be adopted across other sectors in the UK.

1

Web Check

Spotting website weaknesses

Web Check is a service that enables UK public sector bodies to scan their websites for common vulnerabilities. To help these bodies identify potential weak spots, Web Check generates an easy-to-understand report showing what needs fixing and how to fix it.

This year, every local authority in England, Scotland and Wales, and almost all in Northern Ireland have signed up to Web Check.

2

Protective DNS

Protecting the Government from malicious websites

The Protective Domain Name System (DNS) blocks malicious sites from being accessed by public bodies.

The aim of the service is not just to block harmful sites, but to notify the public bodies about any issues so they can fix them. It is currently being used by more than 200 public sector organisations across the UK. The DNS service has now detected and blocked attempts to access over 30 million malicious websites.

3

Takedown Service

Taking down malicious content

We know that people are more likely to click on a link if it appears to come from the UK Government. The Takedown Service aims to prevent cyber criminals impersonating the Government online.

In the past year, we have worked with Netcraft to remove phishing sites that were being used to impersonate the UK Government and notify internet mail providers that are sending malware to unsuspecting members of the public using the UK Government brand. Over the past year, the month-by-month volume of each of these threats has fallen, suggesting that criminals are using the UK Government brand less and hosting fewer of their malicious sites in the UK.

4

Mail Check

Blocking fake emails

Cyber attackers spoof email addresses to trick victims into opening their phishing emails as this makes it easier for them to commit identity fraud and theft. Mail Check enables an organisation to authenticate the email they send so that a receiver can determine if it is genuine or fake. As people don't receive the fake emails, they don't have to make judgments about which attachments to open and which links to click on.

Using the Domain-based Message Authentication Protocol (DMARC) as part of this solution, Mail Check has already prevented a huge number of fake emails getting through. And the number of messages spoofing protected UK Government domains has fallen, suggesting that our work is deterring criminals from spoofing the Government.

Protecting Government Domains

We started Mail Check in 2017. Soon after, cyber criminals responded by spoofing sites that look like UK Government domains but in fact do not exist. For example, instead of using tax.service.gov.uk, they attempted to use tax-service.gov.uk. As the address does not exist, this means there is no record and as a result it will not get blocked.

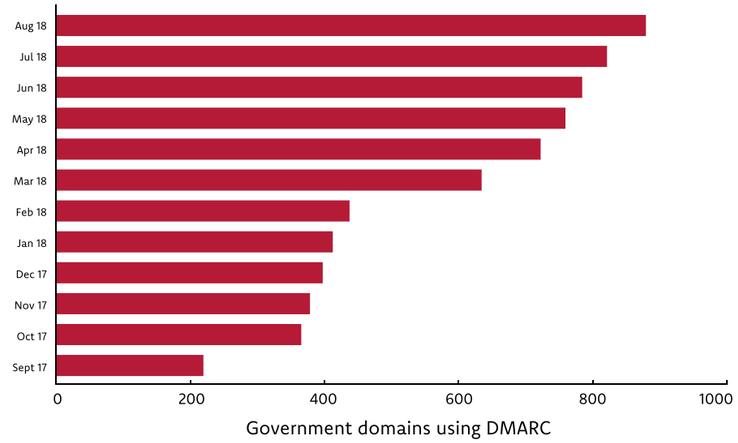
Working in partnership with government and technical experts, we developed a solution, Synthetic DMARC, and used Cyber Security Information Sharing Partnership (CiSP) to keep gov.uk domain administrators informed.

After a few months we saw a significant drop in the abuse of these fake domains. We are now blocking emails spoofing tax-service.gov.uk, and anything else that spoofers create which ends in gov.uk.

UK share of visible global phishing attacks dropped from 5.3% (June 2016) to 2.4% (July 2018)

Availability time for sites spoofing government brands down from 42 hours (2016) to 10 hours median (2018)

Mail Check



Takedown Service

Over the last 12 months, the service removed

138,398

phishing sites hosted in the UK

and a further

14,116

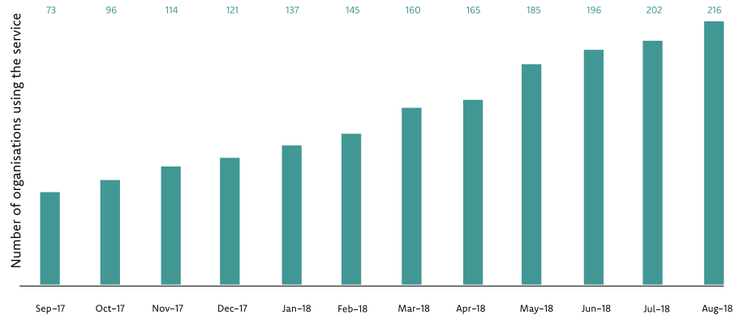
worldwide spoofing the UK Government

Protective DNS

Average of

10,975

unique malicious domains blocked every month

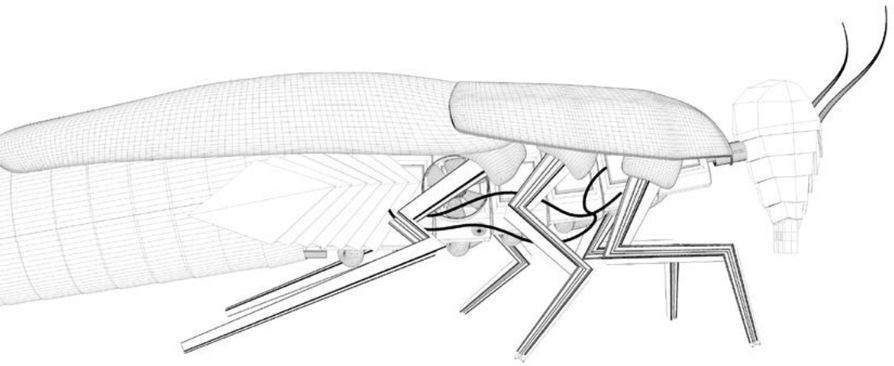


Web Check

We have identified

2,372

urgent findings that have been fixed



What Next for Active Cyber Defence?

The cyber threat is always evolving so we need to continue to build a pipeline of ACD services that can deal with them. These include a service that reports on the condition of an organisation's infrastructure, a service that helps vulnerability researchers to report bugs in government websites, and an online package containing cyber exercises that help organisations prepare for an incident.

To improve information sharing with the cyber security industry, we are continuing to develop a suite of services which automate the processing and sharing of information and events. We have already launched a pilot that shares indicators of compromise with one of the UK's leading internet service providers. This gives their customers better protection automatically at no extra cost.

As part of the ACD programme, the NCSC has started to deliver a pilot host-based capability to central government. This involves deploying software that analyses device data to understand and detect threats that target the Government's IT systems. The service complements an organisation's existing cyber security and has now been successfully deployed to 14,500 government devices. The number of devices enrolled will increase significantly in the coming months. By using the data this generates, we were able to issue our first Threat Surface reports, help early adopters understand the attacks they face, and detect targeted cyber attacks against government systems.

We pilot our ACD tools with the public sector first and, where relevant, demonstrate the benefits to other sectors. This year, we are working with a range of companies and departments to understand how we can help different sectors. We are also encouraging a range of technology providers to offer similar services to their customers so that together we can ensure that cyber crime doesn't pay.

"You don't need to beat cyber crime – and it would be unrealistic to think we could. But we do want to make it as hard as possible and that means making it as unprofitable and risky as we can for cyber criminals to act in the UK."

Dr. Ian Levy, Technical Director, NCSC

International Partnerships

The NCSC's international partnerships help us share information and combat common cyber threats. In our second year, we had the honour of hosting four Heads of Government during the Commonwealth Heads of Government Meeting in April.

We have welcomed delegations from 54 countries across six continents, and we have visited 18 countries for bilateral meetings and public engagements.

In partnership with the rest of government, we have furthered our cooperation overseas, and we aim to expand our reach in 2019.

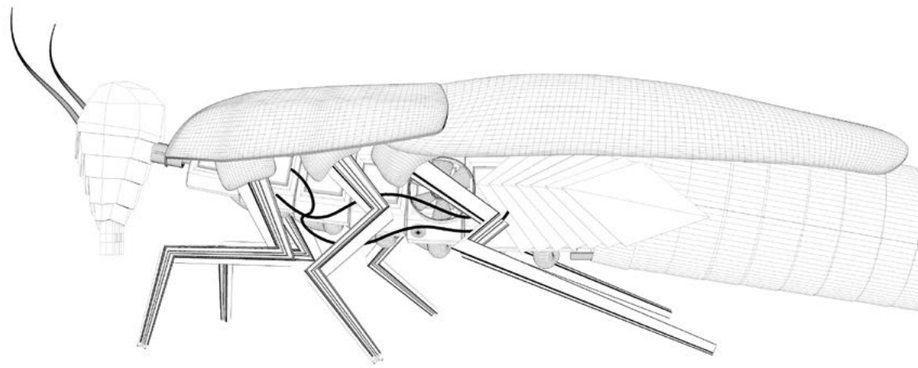
Five Eyes Partnerships

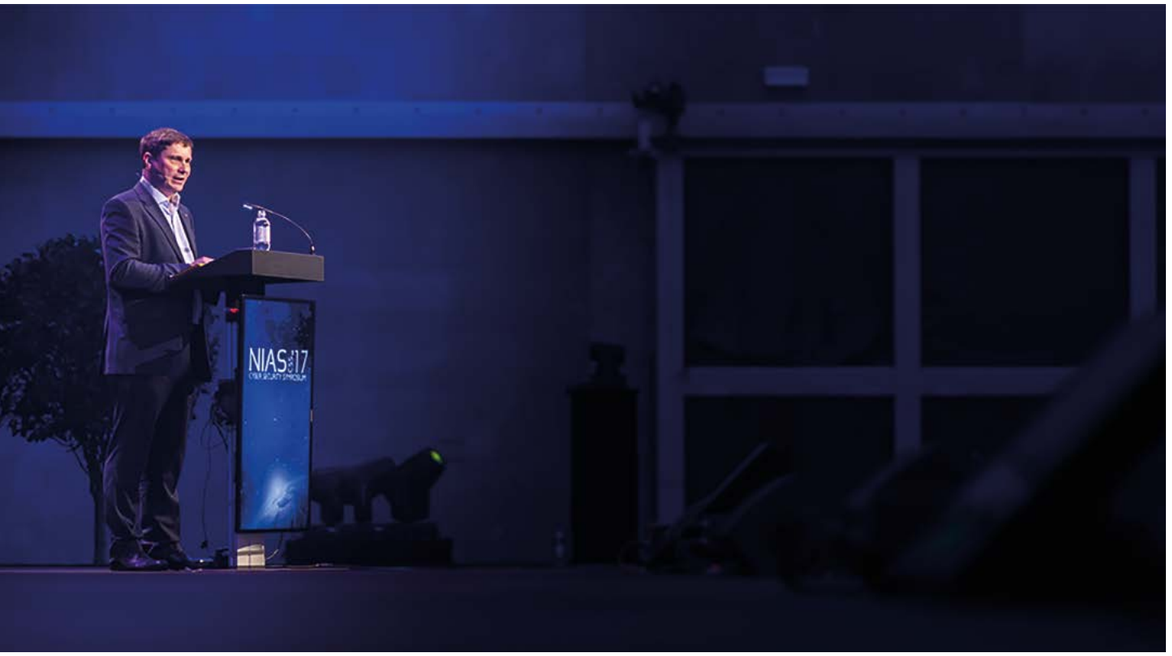
The Five Eyes intelligence alliance comprises Australia, Canada, New Zealand, the United Kingdom and the United States. The alliance – now nearly eight decades old – remains at the heart of our international partnerships.

With the United States, the cornerstone remains the relationship between GCHQ and the National Security Agency but we are working closely with other U.S. agencies. The U.S. Department of Homeland Security and the Federal Bureau of Investigation, with whom we released the joint Technical Alert in April 2018 about malicious cyber activity carried out by the Russian Government, are becoming more and more important to UK cyber security.

New Zealand has a thriving National Cyber Security Centre within their Government Communications Security Bureau. And over the past year, our colleagues in Canada and Australia have announced the creation of their equivalent cyber security organisations.

We are very proud of the work we all do together and as we expand our collaboration on threat sharing, joint operations and beyond, our organisations will become closer still, to the mutual benefit of all.





Keynote speech by NCSC Director of Operations Paul Chichester at NATO's annual cyber security summit

Cyber Defence Cooperation with NATO

Building on the Memorandum of Understanding signed in 2017, the NCSC worked with NATO to deepen our shared understanding of the cyber threat.

We have shared information and taken the steps we need to take to strengthen our cyber defences and to deter and respond to malicious cyber activity.

In a keynote speech at NATO's annual cyber security summit in October 2017, the NCSC's Director of Operations Paul Chichester emphasised the UK's support to NATO operations and encouraged members of the Alliance to embrace their role as lead responders to global attacks from state and non-state actors, who could harm our democracies and critical infrastructure.

European Security Cooperation

As the next phase of the UK's relationship with the rest of Europe takes shape, our ongoing collaboration to tackle common cyber threats will help protect our shared values of freedom, democracy and prosperity.

Protecting the Integrity of Elections

Electoral security is one of the areas in which we are working closely with our European counterparts. In October 2017, the NCSC hosted approximately 50 delegates from across the EU to discuss how to tackle interference in the electoral process and strengthen the collective response to the threat.

The summit helped initiate the creation of a new guide to securing elections across Europe and beyond. Co-led by Estonia and the Czech Republic, the NCSC made a significant contribution to the product which was published in July, six months before the next round of European Parliament elections.

European Conferences

In September 2017, NCSC CEO Ciaran Martin set out the importance of continued international cooperation in cyber security in his keynote address at a major conference held in Tallinn during the Estonian Presidency of the EU Council. A few weeks later he was part of the Prime Minister's delegation to Estonia, where she attended the EU Digital Summit.

Ciaran Martin further reinforced the UK message of unconditional commitment to European security at the Munich Security Conference in 2018, a global forum for security policy, shortly before the Prime Minister set out her vision for post-Brexit European security cooperation.

Visit to NCSC headquarters by four Heads of Government

The NCSC Hosts Four Prime Ministers During Commonwealth Summit

A commitment to improve international cyber security was made during a visit to the NCSC headquarters by four Heads of Government in April 2018.

GCHQ Director Jeremy Fleming hosted the UK Prime Minister alongside prime ministers from New Zealand, Canada, and Australia, where the leaders were also briefed by Ciaran Martin.

The visit was part of the biennial Commonwealth Heads of Government Meeting, in which Ciaran Martin addressed the Foreign Ministers of all 53 member countries and discussed common threats and what the Commonwealth could do together to combat those threats.

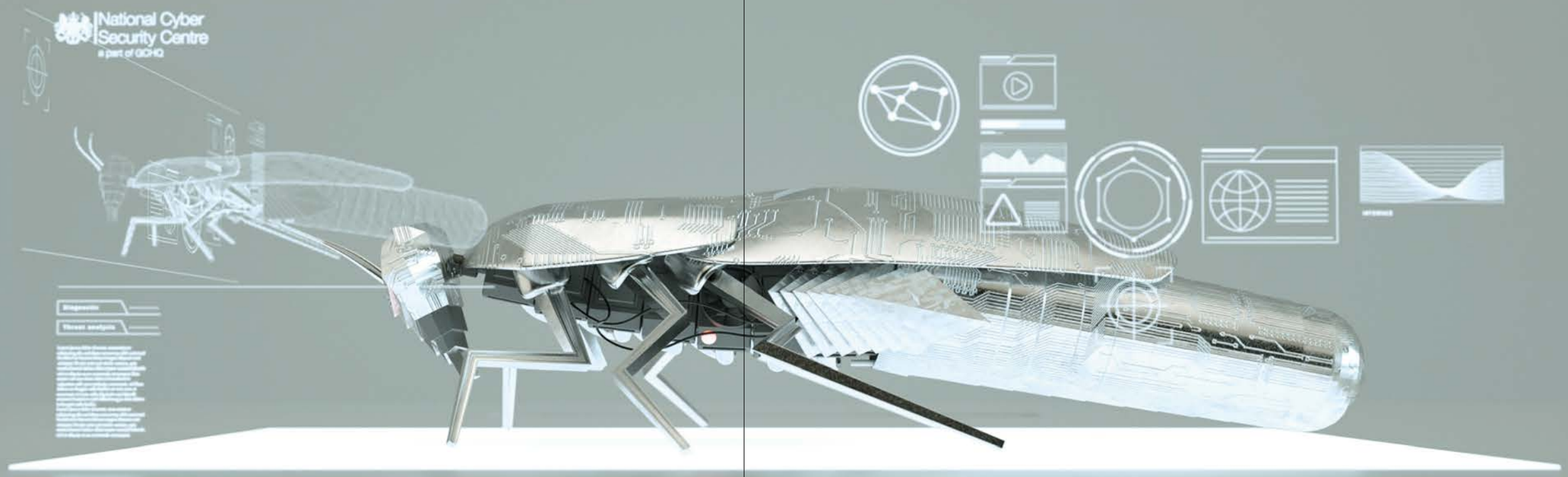
The summit culminated in the UK Prime Minister's announcement of an investment of up to £15 million[1] over the next three years to help the Commonwealth strengthen its cyber security capabilities.

"Cyber security affects us all as online crime does not respect international borders. I have called on Commonwealth leaders to take action and to work collectively to tackle this threat. Our package of funding will enable members to review their cyber security capability and deliver the stability and resilience that we all need to stay safe online and grow our digital economies."

Rt Hon. Theresa May, UK Prime Minister

[1]https://www.gov.uk/government/news/uk-commits-to-a-safer-commonwealth-in-cyber-space

2 Behind the Scenes of an Incident



This special report offers a never before seen glimpse behind the curtain of the UK's strongest asset against cyber attacks. Members of the NCSC's world-class incident management team explain the methodology we have used to defend against more than 1,000 cyber incidents – a rate of more than 10 per week.

Behind the Scenes of an Incident

At the NCSC, we are committed to being open and transparent – even to the point of now sharing the methodology we use to defend against cyber threats.

It is well known that the NCSC coordinates defences to support UK victims, but the tactics our experts deploy are much less understood. This is partly due to the covert nature of some of the intelligence agencies they can draw on, and partly because the NCSC promises confidentiality to the companies who work with us.

Meeting the Team

Two years ago, the level of the cyber threat was well known to the UK Government. Since then, the level of the threat has become unavoidable to every UK citizen. Attackers devise new ways to harm businesses and individuals all over the world, and cyber attacks are rarely out of the headlines.

NCSC Director of Operations Paul Chichester has overall command of the team that coordinates our work against ongoing cyber attacks. Facing more than 1,000 incidents in two years – **including 557 in the last 12 months** – may have been more than some may have expected, but it did not shock Paul.

He reflected: "Cyber attacks are a major danger – the volume and range are huge, but they are on a trajectory that hasn't surprised us.

"There are a wide range of nation state and criminal actors targeting every country. The number of sophisticated actors is increasing, and cyber attacks are seen as a good way of pursuing criminal and national interests. Our job is to make the UK the hardest target possible."

The NCSC's Head of Incident Management Adrian said: "The team operates out of GCHQ's main office in Cheltenham and, since April 2017, the NCSC's London headquarters, Nova South.

"The most prominent attack we have faced so far was WannaCry, which threatened to do unprecedented damage to the NHS in May 2017. But most attempted compromises are never even known to the public and many are mitigated by our incident management team working closely with the victim organisation – and I'm proud of the work we do."

So, what happens when an attack does get through?

Learning About an Incident

The front line of the incident management team includes handlers like Jill, coordinators like Rachel and reporters like Jamie.

"In the past two years, we've had 2,011 reports – or 'tippers', as we call them," Rachel said. "Around half were designated as requiring further enhanced investigation.

"New incidents are raised as a 'ticket' with our Defence Watch Officers (DWOs), who all come from an intelligence, law enforcement or military background. They are able to determine whether it meets our criteria as a 'significant' incident.

Jill added: "We become aware of incidents in a variety of ways. As well as companies contacting us directly, we hear about incidents from international partners and law enforcement colleagues.

"It's really important for us to work closely with law enforcement. Their support is invaluable, and they work with us to pursue the adversaries behind the attacks and ensure protection advice gets out to companies, in particular smaller ones at a local level."

Jamie explained: "Many calls we don't progress relate to individuals rather than organisations. While those attacks can still be significant, they are taken forward by Action Fraud, so we redirect those people to them.

Job Descriptions

Incident handlers
manage and respond to incidents, engage with victims and where necessary support coordinators on significant incidents.

Incident coordinators
manage and coordinate cross-government response to significant incidents and engage with victims.

Incident reporters
produce professional products on incidents to ensure all relevant government partners and agencies are updated on developments.

New Incident Categorisation System

C1 attacks are national emergencies, causing sustained disruption of essential services, leading to severe economic or social consequences – or to a loss of life.

C2 attacks can have a serious impact on a large portion of the population, economy or government.

C3 attacks can have a serious impact on a large organisation or wider government.

C4 attacks could threaten a medium-sized organisation.

C5 attacks include threats to a small organisation.

C6 attacks on individuals, the response would be led by law enforcement agencies, such as the local police force.

"If a tipper has been classed as 'significant' by the DWO, it's elevated to an 'incident' and a handler is assigned to it."

New Categorisation Framework

To ensure the appropriate handler manages an incident, it must first be assigned an attack category. Since January 2018, the UK's cyber community has implemented a new incident categorisation framework.

The new approach fully aligns the NCSC's work with law enforcement agencies to defend against the growing threat, with incident responders now classifying attacks into six specific categories (C1-6) rather than the previous three. The new system ranges from targeting the Government and critical national infrastructure through to individual citizens.

Paul explained: "We wanted to have a more coherent process with industry and law enforcement, so developed a new, truly national system.
"The initial evidence is that it has been extremely effective in helping us direct our resource against the attacks we can best support against.

"At the moment our model is unique, but we know that world leaders and other countries are looking to copy it."

Speaking about the new system, Mike Hulett, Head of Operations at the National Crime Agency's National Cyber Crime Unit (NCCU), said: "We, and others in law enforcement, have worked closely with the NCSC to deliver a consistent and effective response to cyber incidents that affect the UK.

"Our collective understanding of the evolving threat to the UK is improving, but to improve further we encourage all those businesses and organisations which suffer a cyber attack to report them.

"Timely reporting of incidents allows the NCA and NCSC to decide upon and deliver the most effective response."

Once an incident is put onto the system with a specific category, it is allocated an incident handler.

The Language of Espionage

A peculiar aspect that arises at this stage is the language of espionage. All C1-3 incidents are given an operational code name – or 'cryptonym' – that is used as the sole reference during top secret discussions.

"The operation naming process probably isn't as exciting as some might think!" Jamie explained. "Some people think there are 'in jokes' or hidden meanings, but actually the system randomly creates 10 options to choose from.

"You choose something memorable, but it has to be suitable. The names are used across the world, so we also have to make sure it doesn't translate to anything unfortunate."

The sharing of information is of paramount importance. Every morning a daily 'team campfire' is held to look at the last 24 hours and what is next. For C1-3s, a cross-NCSC Tactical Leadership Group (TLG) is immediately set up to share the facts among our colleagues in GCHQ and the law enforcement community.

At this meeting, the team agrees its understanding of the technical issues, sets out clear objectives and ascertains how to provide the best possible support to the victim.

Cyber security is a team sport, and it is also

On 13 June 2018, Dixons Carphone plc announced that a review of its systems and data had shown unauthorised access to certain data held by the company.

A Dixons Carphone spokesperson said:

"Our experience engaging with the NCSC following the discovery that some of our customers' data had been subject to unauthorised access has been beneficial.

"The NCSC has been supportive and provided valuable advice which has helped both shape our response and ensure that we are taking all appropriate steps to ensure the security of our customers' data."

vital that information is shared to other affected areas of government. The TLG findings are fed into a cross-Whitehall Strategic Leadership Group (SLG). A single incident can be of interest to multiple departments, so representatives are brought into the meetings to discuss the attack and identify the next actions to take.

Supporting the Victim

Simultaneously, the NCSC works with the victim organisation to ensure they have appropriate defences in place. An important part of business continuity and disaster recovery planning is identifying a supplier of incident response services in advance of any serious attack.

Rachel explained: "The first thing a handler will ask a potential victim is 'Do you have a Cyber Incident Response (CIR) company? We can still work with them if they don't, but it will often influence how effectively they can investigate and mitigate against the attack."

Jamie added: "If the company is happy to share information, we will set up a trilateral group between ourselves, the victim and their CIR company to investigate. If it's appropriate, we can enrich any information we receive with intelligence we have, and we work with a range of partners to further develop our understanding.

"It's really helpful if companies allow us access to their system logs to look for indicators of compromise (IOCs), and we look for known scripts from actors we already track. By knowing who is behind the attack, we are better able to understand intent and reduce the damage."

If an incident has been detected by the NCSC but is not known to the company, it falls to the incident handlers to pick up the phone and explain what has happened.
Jill said: "That's not always easy – we get a lot of people hanging up! They might think it's just someone on the inside or don't realise the seriousness, so sometimes we need to have persuasive skills as well as technical knowledge.

"To help with that there's a contact validation form on our website that individuals can use to confirm the identity of a member of the NCSC who has contacted them. We explain what we think is happening and try to get them to investigate so they can give us more information. We try to work with them to identify what's happening and help them to fix it."

For the most significant incidents, the NCSC deploys boots on the ground and sends an incident response team to the victim to offer hands-on support.

Jamie added: "We can provide direct support and advice to victims, and help to understand the nature and extent of a compromise. "That response enables us to review the logs on a computer to locate the attack. It can be done by either looking through the victim's physical system or taking a digital image of the system to the NCSC labs."

Public Engagement

When a major incident hits, it is also vital that the public are kept informed. The NCSC has a range of sector engagement teams and full-time communications staff who are embedded in every stage of an incident – including a 24/7 media duty service.

NCSC Director of Communications Nicky Hudson said: "Getting our messaging right during an incident is absolutely vital. The old saying of 'a lie can get halfway around the world before the truth gets its boots on' is particularly true in cyber security – and particularly dangerous.

"Cyber attacks obviously don't adhere to international boundaries or time zones. Incidents often break during the night, and we need to make sure harmful myths are corrected.

"If a company has publicly acknowledged a breach and it affects a large number of people, we work with technical colleagues to get the right advice out quickly which people can act on."

The result is around 1,000 words of easy-to-understand, actionable advice published on the NCSC website within 24 hours of an incident. The NCSC website receives around 180,000 visitors per month, and is soon to be revamped to help users find relevant advice.

"I raise my glass to the UK for what they have done with NCSC – galvanising public and private interests with that bold statement of becoming the safest place to live and do business online. And the results speak for themselves – it has been amazing."

Dave Hogue, U.S. National Security Agency

Aftermath and Evaluation

An incident stops being 'active' once the breach is sealed and no further realistic assistance can be given. However, that is not the end of the NCSC's work to learn lessons and share findings that will help to make the country safer.

While completely confidential, intelligence gained from incidents goes into mapping the broader threat landscape and leads to significant breakthroughs in broader UK intelligence operations.

Paul said: "By having those who track and respond to threats in the same team, it helps us to better understand who is targeting us, investigate them and share our findings.

"That can lead to public attribution – as we've seen more than ever this year. NCSC assessments were behind attributing WannaCry to the North Korean Lazarus Group and NotPetya to the Russian state.

"When we concluded the Russian state was almost certainly responsible for NotPetya, it was announced in a joint attribution with the United States of America. By standing shoulder-to-shoulder with international partners, we have been able to show that foreign state aggression will not be tolerated."

Every single incident is comprehensively evaluated by coordinators, who diligently identify both successes and lessons learned.

Adrian explained: "There wasn't an NCSC before 2016 and we always said we are trying to create something completely new.

"That learning has not ended now we are up and running – we are still always looking to evolve and improve."

Mitigation, not Prevention

There is no silver bullet that will defeat cyber attacks, but work can be done to reduce the harm they cause. Post-event work also includes outreach work to support the victim and proactively warn companies who could suffer similar attacks.

Paul added: "We always ask them three things: Do you know who could target you? Do you know your critical assets? And do you have a comprehensive response plan?

"Answering those three questions isn't going to stop all of the damage, but every organisation should know what to do in the first 36 hours of an attack."

"We understand that defending from cyber attacks can feel daunting. The attacks we face change every day, and as with any response process, every time we work on an incident we learn from it – and share those learnings as widely as possible."

The NCSC has been clear that cyber attacks will take place for the foreseeable future and it is a matter of when and not if a 'category one' attack will occur.

But thanks to the expertise and agility of our incident management team, the UK has one of the best lines of defence in the world to help the country thrive in the digital age.

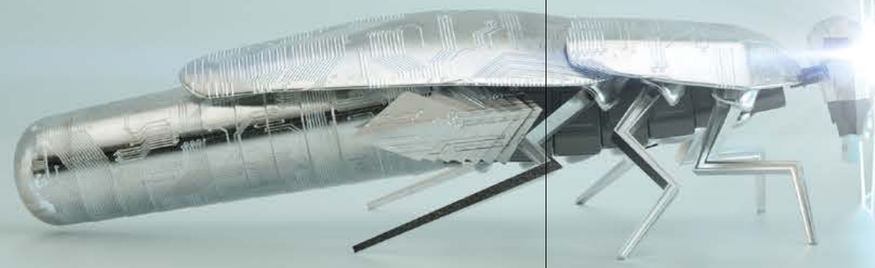
Mythbusting

While the NotPetya attack was ongoing, worldwide media reported early international assessments that it was ransomware.

The NCSC detected it was actually wiper malware masquerading as ransomware, and the communications team quickly acted to ensure people stopped treating the attack as something it wasn't – which could have caused financial damage without retrieving any data.

Director of Communications Nicky Hudson said: "We quickly published an updated statement on our website, phoned journalists and tweeted to get the message out as quickly and clearly as possible. That worked and helped to focus people's actions on the real threat rather than paying a ransom for something that doesn't exist."

3 Building the UK's Defences



The NCSC serves every part of the UK. In our second year, we have worked to strengthen our regional partnerships, deepen our local understanding and expand our reach across the country.

We seek to make sure that every corner of the UK is as well prepared as it can be for whatever incidents may hit us. We are working closely with partners in England and the devolved administrations where we have advised critical sectors including water, energy and health, and advised on the implementation of the Network and Information Systems (NIS) Directive. These partnerships are vital as they help to protect our essential services.

Working Across the UK

Central Government

Alongside HMRC, the Home Office, the Department for Work and Pensions, the Ministry of Defence, and the Foreign and Commonwealth Office, the NCSC is a key stakeholder in the Transforming Government Security Programme. This initiative transforms the way that the Government addresses its most challenging security problems. As part of this, we delivered training for the new Senior Security Advisors, who are the focal points for security in government, to ensure they are equipped to deliver the right advice on cyber security.

Regional Organised Crime Units

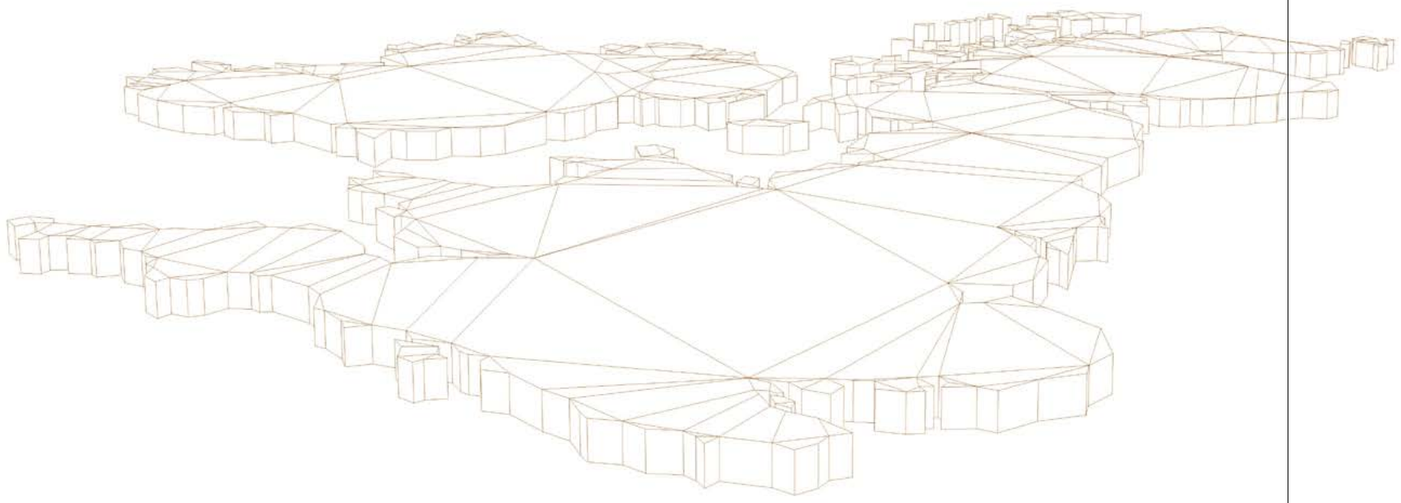
Regional Organised Crime Units (ROCUs) are trusted partners of the NCSC that form the Cyber PROTECT Network. The national policing network of Cyber PROTECT officers aims to raise awareness of the threats posed by cyber crime and provide advice to organisations and individuals on how to protect themselves. The Network is made up of over 60 officers and staff who provide communities with specialist policing capabilities for cyber security. Cyber PROTECT is a critical route for the NCSC to get its message into – and a source of feedback from – local communities. The PROTECT network coordinator and engagement lead are both seconded into NCSC to embed this partnership fully.

Devolved Administrations

We continue to help the UK's devolved administrations raise cyber resilience across all sectors. We promote the adoption of ACD, CiSP and CyberFirst; provide bespoke technical consultancy; and present at cyber security events. We have helped to deliver a secure platform for devolved benefits in Scotland; supported the Welsh Government with their plans to raise cyber resilience within their 22 local authorities; and supported the Northern Ireland administration with workshops designed to link their incident management process to the national framework.

Digital Government Lofts

Digital Government Lofts are events where NCSC experts brief representatives from other areas of government and the public sector to improve regional engagement. The Lofts take place across the country and, this year, they were held in Shipley, Glasgow, Bristol, Cardiff and London, with up to 80 people attending each event.



Events in London and Cheltenham

We have hosted more than 80 stakeholder events at our London headquarters and at GCHQ in Cheltenham. These have ranged from regular Information Exchanges with representatives from critical national infrastructure sectors to CyberFirst activities, international visits, and training events.

"The National Cyber Security Centre has offered vital expertise and support to our work to develop a set of action plans that will help make Scotland a world leading nation in cyber resilience."

Representative of the Cyber Resilience Unit, Scottish Government

"Our close working relationship with the NCSC is invaluable on our journey to design and build the brand new technology platform to support the devolution of social security benefits to Scotland. The safe and secure transition of those benefits is of paramount importance and our early engagement with the NCSC, as the national technical authority for cyber security, demonstrates our commitment to the principle of 'secure by design'."

Representative of the Social Security Directorate, Scottish Government

"The NCSC provides ROCUs with up to date information and services which we can then disseminate to SMEs and the general public."

Representative from the Southern Wales ROCU

"Our engagement with NCSC this year has continued in several valuable areas, from successful take-up of Active Cyber Defence in the Welsh public sector, to raising awareness of the threat and support on managing incidents at several events funded by Welsh Government, to supporting the growth of cyber skills in Wales through CyberFirst courses at Cardiff Metropolitan University."

Representative of the Welsh Government

"The inaugural Northern Ireland CyberFirst Defenders course was a major success. It was a really collaborative effort and we were very pleased with the engaging way of involving the pupils."

"We are certain that this is the beginning of a long-term strategic plan which will encourage more young people to join the profession. NCSC staff were particularly helpful in providing definitive advice and guidance on policy and strategy for password management."

Strategy Officer, Digital Shared Services, Northern Ireland administration

Protecting Critical National Infrastructure

The UK's critical national infrastructure (CNI) supports nearly every aspect of our daily life. Our CNI is becoming increasingly digital, which brings real benefits, but also raises cyber security risks. To combat these threats, we work with thousands of systems and hundreds of organisations across the UK.

Over the past year, we have supported many of these organisations to secure their systems. In the transport sector, our advice has helped to secure the next generation of vehicles. In the energy sector, our experts have helped design the security of a new sustainable national grid.

In the telecoms sector, our work with the Department for Digital, Culture, Media and Sport (DCMS) has helped pave the way to faster 5G networks. And as we enter the 'Great British Space Age', we are helping to design four new UK spaceports to help an already successful industry reach for the stars.

Mapping Critical Systems

The NCSC has been working with lead government departments and industry to develop a process which identifies the systems that are critical to our CNI, including dependencies between the sectors. We have mapped the critical systems that are vital to the everyday operation of the CNI. By better understanding the interconnectedness of the various sectors, we can improve their resilience.

As it continues to develop, this work will provide an overarching view of our CNI, enabling industry and government to concentrate their cyber security efforts where they will have the most impact.

Protecting the Nation's Energy

The NCSC has undertaken a range of work within the energy sector. We brought together participants from the oil and gas sector, cyber security industry, the Department for Business, Energy & Industrial Strategy (BEIS) and the Oil & Gas Authority to conduct a threat and vulnerability survey of the sector. This resulted in a number of vulnerabilities being identified which will lead to improvements based on our advice.

Exercising Capability in Europe

The NCSC both contributed to the development of and participated in the European Union Agency for Network and Information Security Cyber Europe 2018 exercise for the aviation sector. The exercise drew participants from 30 countries and enabled each to test their national incident response procedures as well as their ability to coordinate with European partners in the event of a widespread cyber incident. It involved sending out over 23,000 'injects' – updates that drive the direction of an exercise – with the UK receiving approximately 470. This enabled the NCSC and the Department for Transport (DfT) to validate their procedures and identify areas for development in their response.

"The NCSC is a valuable partner for the Bank of England in developing the next generation of the Real-Time Gross Settlement service; a high value settlement system which lies at the heart of the UK's financial system. The NCSC is providing guidance at both a technical and strategic level to help the bank design a system that will meet the changing needs of the public and support innovation in the payments industry while maintaining security and resilience at the heart of the service."

Victoria Cleland, Executive Director, Banking, Payments and Financial Resilience, the Bank of England

Civil Nuclear Exercise

We supported BEIS on the planning and delivery of a technical exercise in Estonia for the UK's civil nuclear sector. The NCSC acted as part of the 'red team', testing the 15 participants in their ability to understand and defend against a range of cyber threats.

The NCSC continues to work with BEIS, other government departments and industry partners to extend the number and types of technical exercises available to operators in their sectors.

"This provided a very rich scenario which taxed us across a broad range of technical abilities in many cyber security topics."

Gavin, Nuclear Decommissioning Authority

Securing the Air

We have continued working with NATS, the main air navigation service provider in the UK, to review the cyber security of their air traffic control and management system. A series of rigorous technical reviews looked at their existing and new systems and made recommendations for improvements which NATS agreed. The new systems will also be compatible with changes being made across Europe over the next 20 years as part of the Single European Sky ATM Research project.

Working with the Regulators

NIS Directive

This year has seen the UK regulations implementing the EU NIS Directive come into force, resulting in companies being designated as Operators of Essential Services (OES) and Digital Service Providers (DSP). The NCSC has two formal roles under NIS: to act as the UK's Cyber Incident Security Response Team (CSIRT); and to be the UK's single point of contact. As the CSIRT, our role is to provide 24/7 incident support and assistance to OESs and DSPs on cyber matters.

We have also produced guidance and developed a framework which supports the assessment of the level of cyber security achieved by OES in relation to NIS requirements. While the NCSC has no regulatory role in NIS, we are supporting new NIS regulators to develop their staffs' skills and provide guidance on the threat that different industries face. We are working with industry and the regulators to ensure that the implementation of this directive leads to better standards of cyber security.

GDPR

In May, the General Data Protection Regulation (GDPR) came into force alongside the new Data Protection Act 2018, placing a comprehensive set of new obligations on public and private sector organisations to protect all the personal data that they collect and process.

The NCSC has partnered with the Information Commissioner's Office (ICO) to develop a set of GDPR security outcomes. This guidance provides an overview of what the GDPR says about security and describes a set of security-related outcomes that all organisations processing personal data should seek to achieve.

National Security

The national security sector faces unique threats as it processes the UK's most sensitive data and runs its most sensitive systems. The NCSC is working hard to support them. Far from being limited to securing the defence sector, the NCSC's robust encryption systems help ensure the UK Government stays secure today and in the future.

Securing Britain's Secrets

From the rise in mobile working to the emergence of quantum computing, the national defence landscape is changing all the time. In response, we have developed secure systems that our government partners and allies can trust. These solutions ensure government missions achieve their outcomes.

Joint Crypt Key

The Joint Crypt Key Programme (JCKP) helps the UK keep its secrets secret, share information effectively and ensure that it is available when and where required.

Working in collaboration with the Ministry of Defence (MOD), JCKP helps us work with foreign partners and keeps our key distribution technologies up to date. Now, two years into a 10-year plan, JCKP has helped the UK maintain its standing as a world leader in cryptographic key services.

UK Key Production Authority

The UK Key Production Authority (UKKPA) is a critical part of the NCSC's cryptography defences. UKKPA generates, distributes and accounts for cryptographic key material for government, industry and our allies overseas to support secure encrypted communications.

UKKPA Facts

- 170 customers across government, industry and law enforcement
- Alongside the U.S, we are one of only two suppliers of key material to NATO
- Annually we process approximately 3,800 orders for key material, equating to 145,000 physical items, such as CDs and data tokens
- We support the MOD, intelligence agencies, and other government departments in their requirements for allied electronic key received from the U.S. and other partners.

Government Missions

The NCSC works with the defence sector and UK intelligence agencies to help preserve the national security of the UK. Our encryption expertise enables the NCSC to protect the UK's national defences in a range of ways.

Securing Secret Communications

The NCSC has continued to support the Cabinet Office's FOXHOUND programme to deliver a secure IT and communications network (known as Rosa) across central government. Rosa offers the UK Government and its partners a single, secure platform for working up to and at the SECRET classification.

This year, the first phase of bespoke mobile phones that use our unique technology was deployed to users, and we are working with the Rosa operations centre to ensure a smooth transition to the new system. The effective partnership between the NCSC and the Cabinet Office Government Security Group is delivering a single security solution to dozens of departments and thousands of users. Our cyber security experience means we are perfectly placed to secure the UK Government's latest technology.

Protecting Our NATO Allies

We work with NATO to help protect their communications infrastructure. Our expertise in cryptography and security helps support NATO defence efforts and ensures our armed forces get the protection they need.

Defending Defence

The NCSC continues to support the Defending Defence Programme, which was established in 2014 with the aim to make the defence sector a more difficult target for those that threaten our national security.

Strategic Deterrent

To help the MOD protect the UK's most sensitive capabilities, we provide support with incident and threat reporting, advice on cyber security policy and training to identify supply chain vulnerabilities.

Joint Strike Fighter

The NCSC supported the MOD to ensure the secure delivery of the new F-35B fighter planes. We produced cryptographic key management that enables the MOD to operate the aircraft wherever and whenever they are needed. We tested the aircraft to ensure that it met national TEMPEST standards, which ensure that military equipment does not unintentionally emit sensitive information. We also provided guidance to secure the international ground systems and provided technical expertise to mitigate the threat to the supply chain that supports the aircraft throughout its life.

Securing the Defence Supply Chain

We worked with the MOD through the Defence Cyber Protect Partnership to build better cyber security into their contracting and procurement processes. We also provided defence industry suppliers with threat briefings to help them identify vulnerabilities in their supply chains. Our work helps protect national security customers and helps ensure that their systems are not compromised.

Working with Industry

We cannot do any of this alone. Our industry partners provide a vital service to keep our communications secure.

The Sovereign Enabling Framework

The Sovereign Enabling Framework allows companies to work with us on cryptographic key projects such as the JCKP. We designed this framework to ensure that companies working with us have a good understanding of cryptographic key and to demonstrate the behaviours we need to protect the UK.

In its second year, we are pleased to welcome two businesses onto the framework, joining the original six companies. With their support, we have sustained and developed the skills, capacity and capabilities of the UK's cryptographic key industry.

Exporting Crypt Overseas

This year, the NCSC made the biggest change to information security export licensing in over a decade. Working in partnership with the Department for International Trade and industry bodies, we released our Open General Export Licence (OGEL) for information security items.

The new licence removes a large administrative burden for businesses and introduces a simpler, lighter touch process for the faster export of low risk cryptographic goods from the UK. This enables UK firms to compete on a more equal playing field with the U.S.

The Wassenaar Arrangement

The NCSC provides cryptography and cyber security expertise into the UK's representation at The Wassenaar Arrangement. The Arrangement is a body of technical experts from 42 states who provide guidance on arms control. During the 2017 negotiations, the NCSC contributed to the redrafting of the controls text for intrusion software tools.

The outcome provides greater clarity of the control text and provides some exemptions where the described products are used by the cyber security industry. The NCSC's contribution was a significant factor in achieving the progress to date. We also provided technical contribution to new areas where controls might be relaxed or tightened.

"The NCSC has provided significant ongoing cyber security support within the F-35 mission support environment. The NCSC has been a critical contributor to F-35 system connectivity and UK network security, enabling Defence Equipment and Support to understand and mitigate risk while ensuring that security policies and international collaborations remain robust to the cyber threat."

Caroline Dyer, Programme Manager, Ministry of Defence

Supporting our Citizens and Economy

The NCSC is committed to helping everyone stay safe online – from the smallest organisations to the biggest global brands. We have begun in-depth research to inform the content that we deliver to our varied audiences. We have listened to users and will be incorporating their feedback into the launch of our new website. The new website will have a focus on protecting individuals and families, businesses, charities, and government.

We aim to expand and develop our offer across the UK. We are developing a toolkit to help boards better understand the cyber threat and mitigate risks. And we are working with our Industry 100 partners to create innovative new ways to raise the level of cyber security across the UK.

Enterprise and Organisations

Small and Medium-Sized Enterprises

Small and medium-sized enterprises (SMEs) account for 99% of all private sector businesses. With fewer resources than larger companies, it is crucial that we do all we can to help these businesses keep themselves safe. That's why we produced our Small Business Guide and distributed copies around the country through the annual business engagement event, the Small Business Saturday Bus Tour.

We partnered with various trade bodies to ensure we are tailoring our products to meet the needs of SMEs. We also participated in the Prince's Trust Business Emergency Resilience Group's 'Would You Be Ready' campaign to ensure that businesses are as resilient as they can be.

We have also developed links with regional organisations such as the North West Business Leadership Team. This has led to direct engagement with universities, local authorities and business leaders in the region.

Legal

Legal services hold some of their clients' most sensitive information and they are increasingly subject to cyber attacks. That's why we produced The Cyber Threat to UK Legal Sector Report. In partnership with The Law Society and our Industry 100 legal partners, the report helps law firms understand current cyber security threats and the risks to the legal sector, and includes guidance firms can use to secure their cyber defences.

Charities

We work with the charity sector to ensure their good work can carry on without interruption from cyber threats. As part of an awareness-raising campaign, the NCSC released the first ever threat assessment for UK charities. The report showed that charities were under attack but few people in the sector were aware of the significance of the threat.

To combat the threat, we released our Cyber Security: Small Charity Guide. In partnership with the Charity Commission and leading charitable bodies, the guide aims to help charities understand the risks and offers advice to reduce them. We collaborated with The Foundation for Social Improvement to bring the guide to life by delivering cyber security awareness sessions to more than 1,000 charities across the UK.

The NCSC is working with the National Association for Voluntary and Community Action to develop a range of training materials for their 200 members to deliver to the 145,000 charities and voluntary groups they represent. This is a unique campaign that ensures that the work of these vital organisations is protected. We pride ourselves on being able to help safeguard those charities who safeguard others.

Retail

Our work with our retail partners ensures the sector remains resilient to potential attacks. In 2017, the retail sector contributed £194 billion to the UK economy.[2] And as the largest single employer in the UK, it is vital that we help keep it safe.

To do this, we produced the Retail Cyber Security Toolkit in partnership with the British Retail Consortium. The toolkit has now been downloaded and shared thousands of times, helping to make online shopping safer.

Education

We worked with Universities UK to raise awareness of cyber security among university leaders. We also partnered with the Department for Education to produce cyber security guidance for schools.

Sport

We have developed relationships with major UK sports organisations, helping the FA prepare for the 2018 FIFA World Cup and incorporating cyber security into the plans for the 2022 Commonwealth Games. Our work helps sports organisations understand that reducing the cyber threat really is a team sport.

[2]http://researchbriefings.files.parliament.uk/documents/SN06186/SN06186.pdf

Individuals and Families

Despite the scale of the cyber threat today, vital protective actions are still routinely left at individuals' discretion. We support a number of initiatives which help people to take the right protective action.

To encourage lasting and meaningful change, the NCSC is working with other government departments on strategic communications and initiatives that build on the success of the UK Government's current behaviour change campaign, Cyber Aware. This is based on the technical advice of the NCSC and promotes simple measures that people can adopt to stay secure online.

"As data controllers, law firms handle significant volumes of confidential and sensitive information and client monies as part of their daily work. The Law Society sees The Cyber Threat to UK Legal Sector Report as as a positive step to help our members spot vulnerabilities and put relevant safeguards and protections in place."

Christina Blacklaws, President, The Law Society

"The small charities guide is really useful because it uses simple language, it is practical and it doesn't shroud everything in a mist of expertise. It just gives you some very simple steps that you can take to make your charity more secure."

Pauline Broomhead, CEO of Foundation for Social Improvement

"For the British Retail Consortium and our members, cyber security is at the very heart of our work and an area where relationships with the NCSC are vital. We look forward to continuing our ground-breaking work into the future."

James, British Retail Consortium

The NCSC Online

The NCSC's digital output has become an integral part of how we provide advice and guidance.

This year, more than 1.9 million people have visited our website, and our Twitter and LinkedIn channels now reach more than 80,000 people. Our content has allowed the NCSC to start conversations, raise awareness and increase understanding across the cyber security landscape.

As the NCSC develops, so must our digital presence. To deliver an improved website, we have responded to feedback and focused on giving users a much-improved journey through the site with more intuitive navigation.

Our goal is to deliver a digital platform that helps users not only understand the importance of cyber security, but also how they can protect themselves at work and at home. This platform will also be a base for new digital services in the future.

CiSP

The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a confidential and dynamic environment.

The benefits of CiSP include giving members a secure environment to engage with industry and government counterparts, supplying early warning of cyber threats, and helping members learn from their experiences and successes of other users.

Since its launch, CiSP has grown to 10,569 users across 22 sectors and produced 20,270 pieces of content.

Bug Bounty

The NCSC works with vendors to help mitigate critical security issues before they cause real harm. This includes vulnerabilities in major software products. As testament to our skills, the NCSC was named as one of Microsoft's top five Bounty Hunters in the first quarter of 2018. NCSC's expertise helps keep government, businesses and individuals safe and provides support for a range of good causes as all the bounties we win are awarded to charity.

CYBERUK 2018

CYBERUK is the UK Government's flagship cyber security event. CYBERUK is all about promoting a national conversation around cyber security and building a community that works together.

We were delighted to bring CYBERUK 2018 to Manchester, a city synonymous with innovation, creativity and technology.

Over the three days in April, we had engaging speakers, thought provoking topics and a plethora of talent in attendance. We were committed to putting diversity at the heart of CYBERUK 2018.

This meant ensuring that we had diversity of thought in the programme, and provided a positive learning environment for all participants.

The conference brought together 2,500 delegates with combined expertise across multiple disciplines and professions. The event offered a wealth of content on the technical aspects of developing and implementing cyber security in the face of complex problems and threats.

We are pleased to announce that CYBERUK 2019 will be held in Glasgow.

Highlights

- **2,500** delegates
- **210** speakers
- **48** track and stream sessions
- **26** 'Spotlight stage' lightning talks
- **15** workshops
- **105** sponsors and exhibitors
- Dragons' Den style 'Cyber Den'
- Live cyber incident exercise
- Provided sign language interpreters for hearing-impaired delegates
- **94%** of delegates rated the content of the conference as 'excellent' or 'good'
- **88%** of delegates rated our commitment to diversity positively

"CYBERUK is a tremendous conference. You get to meet a lot of interesting people in areas I wouldn't normally be exposed to. It is a great community. The partnership with the people who are in attendance and who are here speaking has really evolved a lot and the initiatives, the competitions and the outreach to the community has been really amazing to watch."

Katie Moussouris, Founder, Luta Securia

Industry 100

The NCSC's Industry 100 initiative brings together public and private sector talent to generate innovative ideas and collaborate on some of the latest cyber security challenges across a wide range of NCSC placements.

Since the programme began, we have been pleased to welcome 132 professionals from 60 organisations who have come together to enhance the cyber security of the UK.

Contributors have included representatives from sectors including legal, finance, aerospace, telecoms, academia, IT, oil and gas, nuclear and engineering.

"Industry 100 allows us to draw on the best and brightest in industry – to test and to challenge the Government's thinking as we take this project forward."

Rt Hon. Philip Hammond, Chancellor of the Exchequer

How Does Industry 100 Work?

1

Industry 100 secondees will work across a wide range of bespoke short-term placements at the NCSC normally on a part-time basis.

2

Participating organisations are expected to continue to pay salaries for Industry 100 secondees, in order to maintain independence.

3

There are exciting and challenging opportunities in all areas, including security engineering, communications and finance.

4

Some roles are also available for secondees who are not based at our offices.

Find out more:
www.ncsc.gov.uk/industry-100

"I'm proud to be part of the Industry 100 programme as I am at the forefront of developing cyber security skills across the UK. My role as a Cyber Security Educator is to build upon the work of the CyberFirst programme and increase its proliferation and participation."

Zeshan, Technical Evangelist at CompTIA and Cyber Security Educator at the NCSC

"Industry 100 has enabled me to research the most pressing and emerging issues in cyber and security affairs, something that has been invaluable for both King's College London and my own academic studies. The flexible working hours at the NCSC are very convenient, allowing me to balance my work with my continuing academic studies."

Rob, master's student at King's College London and CNI Assessor at the NCSC

4. Cyber Capability for the Future

The NCSC strives to identify new ways to build the UK's talent pipeline, promote innovation, and develop the UK's cyber security research. Our investment in skills helps the UK remain a world leader in cyber security by developing the talent we have and attracting the best and brightest people to the industry. To ensure a secure, resilient and prosperous economy, organisations must have access to the cyber security skills they need, which is why the NCSC is working closely with the Department for Digital, Culture, Media and Sport (DCMS) to close the cyber skills gap.

People

The NCSC's single greatest asset is our people. At a time of rapid change in our industry, we are helping students of all ages develop the skills they need to grow to work across the UK and have a rewarding and interesting career in cyber security.

CyberFirst

The CyberFirst programme aims to identify and nurture exceptional young talent, engaging students from all backgrounds and every region.

CyberFirst Bursaries

The CyberFirst Bursary project continues to grow, and in autumn 2018 more than 500 students will have joined the initiative. Each student receives £4,000 a year and a minimum of eight weeks' paid cyber security work experience or training each summer with industry or government.

CyberFirst Degree Apprenticeships

In September 2017, we ran a recruitment exercise for our brand new Cyber Security Degree Level Apprenticeship which will see young people working within the NCSC's parent organisation, GCHQ. Successful applicants will start a degree apprenticeship, learning everything from code to emerging technologies, with a potential full-time role upon graduation.

The apprenticeships give students exposure to some of the most cutting-edge technologies and practical insights into the innovative ways we use them. In our first year, we have already made over 100 offers of an apprenticeship and were pleased to welcome our first intake in September 2018. We hope this programme will open up a career in cyber security for a wide range of people – not just those who choose to go to university.

CyberFirst Courses

This year, we held CyberFirst courses in Edinburgh, Belfast, Cardiff and Southampton as well as 23 free, week-long summer courses at universities across the UK.

"Looking back over my time in the scheme, I consider myself lucky to have been a part of such a great project. Not only has my cyber outlook been enhanced but my career aspirations changed completely!"

Lauren, CyberFirst Bursary student

"The competition has taught me and my team-mates a lot about coding and I think I'd now like to do computing for GCSEs."

Annarose, St Catherine's College, CyberFirst Girls Competition finalist from Northern Ireland

CyberFirst Girls Competition

Women make up only 11% of the global cyber security workforce.[3] Through the CyberFirst Girls Competition, we are working to increase the number of young women in the cyber industry.

This year's CyberFirst Girls Competition attracted over 4,500 girls aged 12-13. The finalists overcame 170 challenges of varying difficulty and the top ten teams qualified for a head-to-head final in Manchester. As part of their prize, all the finalists were then invited to Buckingham Palace to meet His Royal Highness The Duke Of York.

In 2019, we are hoping to build on this year's success by expanding the CyberFirst Girls Competition to over 1,000 schools.

2018 Winners: The Computifuls from The Piggott School

[3]https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

Launch of the Cyber Schools Hub in Gloucestershire

Cyber Schools Hubs

At the NCSC, we are also taking strides to reduce the UK's digital skills gap. Currently, only one in nine students chooses to take a GCSE in Computer Science. Initiatives like our Cyber Schools Hubs aim to change that by encouraging pupils to choose a career in the cyber sector.

Launched in spring, our two pilot Cyber Schools Hubs in Gloucestershire have provided the opportunity to over 17,000 children to engage in events, code clubs, and fun ways to learn about cyber security. At one school, we held an event that took inspiration from the popular BBC TV show Dragons' Den to inspire students and increase their awareness of cyber security.

The initiative has been incredibly popular, and we have encouraged participating schools to share what they have learnt with nearby schools. The Hubs are an example of how we are extending a hand to local communities and supporting projects that build our national strengths.

"What a morning it was! As someone working in the cyber and technology industry and a father of two kids who will be making their own career choices in the coming years, I came away feeling inspired, enlightened and also somewhat humbled by the experience."

Richard, company director and dragon at the school event

Certified Degrees

We believe that all UK students should have access to a high-quality education in cyber security. Assessing everything from the instructor to the facilities, NCSC-certified degree programmes have helped hundreds of students choose the right cyber security degree course for them. Since the initiative began, we have certified 24 master's degrees, three integrated master's degrees and two bachelor's degrees.

This year, analysis by the Higher Education Standards Authority shows that UK students with a certified master's degree have higher employment rates and higher salaries than students on non-certified master's degrees. We were particularly pleased to see an increase in applications from post-92 universities as well as more universities from all around the UK.

"There has been a definite increase in the number of applicants, which has more than trebled since gaining certified status."

Representative of University of South Wales

Cyber Security Body of Knowledge

Through the Cyber Security Body of Knowledge (CyBOK) project, we are identifying and defining the key knowledge areas required by those working in cyber security.

After public consultation and having taken on board a great deal of feedback, the project took its first big steps this year with the launch of the first two of the 19 identified knowledge areas: 'Cryptography' and 'Software Security'. We aim to have launched all 19 knowledge areas by the end of July 2019.

CyberFirst Girls Competition finalists in action

Research

We worked with external partners to support programmes that put the UK at the forefront of cyber security research. This gives us access to world-class experts and helps the NCSC to discover new ways to keep the UK's information safe.

Academic Centres of Excellence in Cyber Security Research

Universities which are recognised by the NCSC and the Engineering and Physical Sciences Research Council (EPSRC) as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR) have been assessed as producing world-leading, impactful cyber security research.

When the ACE-CSR programme was launched, only eight universities were successful at the assessment panel. After the most recent assessments in 2018, 17 universities have now been recognised. This is testament to the universities' growing support for cyber security research. In return, the ACEs-CSR get the chance to build their profile, receive international recognition and showcase the UK's research capabilities on the global stage.

Research Institutes

Research Institutes help us to develop cyber security capability in strategically important areas.

In the past year, all our Institutes have increased expertise in every research area while deepening their relationships with industry. The Institutes also successfully attracted match funding to complement the funds received from government. In November 2017, we saw the launch of the Research Institute in Secure Hardware and Embedded Systems at Queen's University Belfast, which will announce its first funded projects in December 2018.

The results have been outstanding. A start-up from Imperial College London, whose work focuses on the automated testing of graphics, has been acquired by Google. Middlesex University's work on the verification of security protocols uses physics to develop a cryptosystem that is immune to quantum computer attacks. And the University of Glasgow, the University of Birmingham and the University of Bristol are all measuring the impact of the EU NIS Directive.

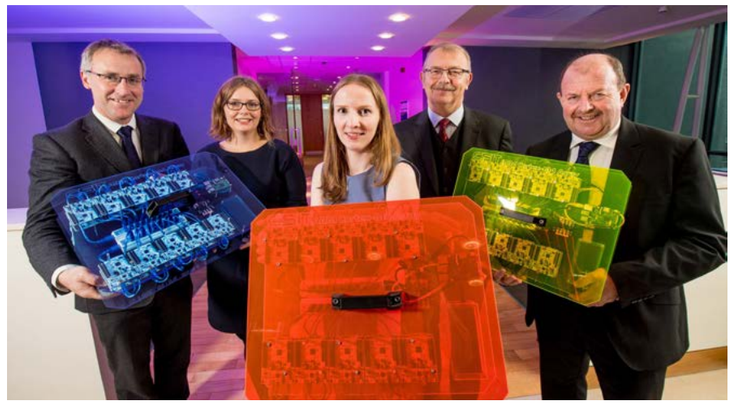
The Initiate Portfolio

An important part of the NCSC's work is to anticipate how cyber security will evolve and discover new ways to keep the UK's information safe. One of the ways we do this is through the Initiate Portfolio which brings together the technical expertise of the NCSC with the latest industry practices and academic research.

The Portfolio includes a range of projects, from developing the next generation of cryptographic devices to finding new ways to reduce data loss. As just one example, we led a research project to investigate vulnerabilities in medical devices that use Wi-Fi or Bluetooth. This has enabled government departments to manage the risk and help staff use these devices. Future projects include developing common standards for devices connected to the Internet of Things.

With funding from the MOD, UK intelligence agencies, the Cabinet Office and the Foreign and Commonwealth Office, the NCSC will continue to help the Government harness innovation, utilise ground-breaking new technologies and keep our information secure.

Launch of the Research Institute in Secure Hardware and Embedded Systems, Queen's University Belfast



Doctoral Studentship Programme

The NCSC's sponsored Doctoral Studentships Programme helps increase the number of UK nationals undertaking cyber security research, which will make a real difference to the UK's security.

The students often make discoveries, for example, vulnerabilities in products or standards, which are then reported to the manufacturer or the appropriate authority. The programme also offers students the opportunity to undertake work placements within the NCSC and has led to several students successfully applying for subsequent employment with the NCSC.

Quality

Organisations need confidence that the people, products and services that help them manage their risk will improve their security, not undermine it. Working with our external assurance partners, we operate a number of commercial initiatives that give organisations the evidence to help them differentiate the good from the bad.

Cyber Essentials

Helping guard against the most common, internet-based cyber threats, the Cyber Essentials programme is available to all UK organisations, of any size and sector, that want to demonstrate their commitment to cyber security. Over the past year, we have more than doubled the number of certificates issued, with the award of over 8,900 new certificates. This brings the total to 15,826 since the initiative began in 2014. We are currently reviewing the programme to make sure it is as effective and affordable as possible.

Certified Cyber Security Consultancy

The Certified Cyber Security Consultancy gives customers independent, expert cyber security advice from a pool of certified professional service providers. The initiative certifies organisations through a robust process of evidence assessment and interview, to provide bespoke cyber security services that meet the NCSC's demanding standards.

Currently there are 23 organisations across the UK who have achieved certification by demonstrating that the services they deliver meet the NCSC's standards for high quality cyber security advice in the areas of risk management, risk assessment, security architecture, and audit and review.

Innovation

Innovation takes new thinking and insights and turns them into the things we need to live and do business in cyberspace. We work with DCMS to create an ecosystem that will transform ideas into real world solutions. This brings our experts together with small businesses to help solve the cyber security challenges we face today. At the heart of this is the NCSC's Cyber Accelerator.

Cyber Accelerator

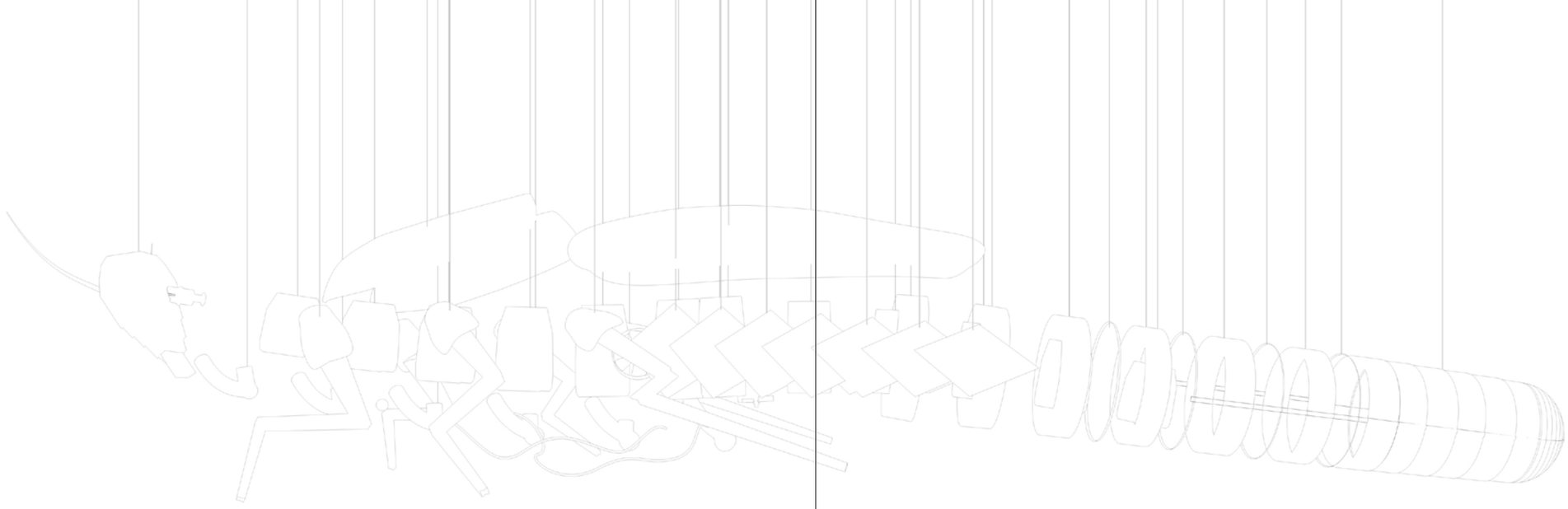
Aiming to nurture innovation in cyber security, the NCSC's nine-month Cyber Accelerator saw nine companies develop products and services that will enhance the UK's cyber defences.

This included a service to solve the problem of age verification and parental consent for young people in online transactions, and another that connects Internet of Things devices with end-to-end authenticated, encrypted security.

In the past 18 months, the first two cohorts raised more than £20 million in funding, created 19 UK jobs and won 15 trials and contracts worth over £3 million. We're now recruiting for a third cohort to start in late 2018.

"The opportunity to be part of the NCSC Cyber Accelerator programme afforded Trust Elevate unprecedented access to cyber security experts, support and guidance, which was and continues to be instrumental in accelerating our growth and reach."

Dr. Rachel O'Connell, CEO of Trust Elevate



CyberFirst Courses

Venue	Course
University of Birmingham	Defenders, Futures and Advanced
Cardiff Metropolitan University	Adventurers, Defenders, Futures and Advanced
Cleeve School	Adventurers
Dean Close School	Adventurers
University of Gloucestershire	Adventurers
Imperial College London	Defenders, Futures and Advanced
Lancaster University	Defenders, Futures and Advanced
Manchester High School for Girls	Adventurers
NCSC headquarters	Adventurers
Newcastle University	Defenders, Futures and Advanced
Newent Community School	Adventurers, Defenders, Futures and Advanced
Nottingham University	Adventurers
Queen's University Belfast	Adventurers
Royal Holloway, University of London	Futures
University of Southampton	Adventurers
The University of Stirling	Adventurers
University of Warwick	Adventurers, Defenders, Futures and Advanced
University of the West of Scotland	Defenders, Futures and Advanced

To find out more, visit:
www.ncsc.gov.uk/information/cyberfirst-courses

Innovation

Cyber Accelerator – Cheltenham Innovation Centre

Research Institutes - Host Universities

Research Institute in Science of Cyber Security (RISCS) – University College London
Research Institute in Verified Trustworthy Software Systems (RIVeTSS) - Imperial College London
Research Institute in Trustworthy Inter-Connected Cyber-Physical Systems (RITICS) - Imperial College London
Research Institute in Secure Hardware and Embedded Systems (RISE) - Queen's University Belfast

Academic Centres of Excellence in Cyber Security Research

University of Birmingham
University of Bristol
University of Cambridge
Cardiff University
University of Edinburgh
Imperial College London
University of Kent
King's College London
Lancaster University
Newcastle University
University of Oxford
Queen's University Belfast
Royal Holloway, University of London
University of Southampton
University of Surrey
University College London
University of Warwick

NCSC-Certified Degree Providers

Abertay University
University of Birmingham
University of Bradford
Cranfield University
De Montfort University
Edinburgh Napier University
Imperial College London
University of Kent
Kingston University
Lancaster University
University of Oxford
Oxford Brookes University
Queen's University Belfast
Royal Holloway, University of London
University of Southampton
University of South Wales
University of Surrey
University College London
University of Warwick
University of the West of England
University of York

100 Years of the Cyber Mission

The NCSC's parent organisation, GCHQ, will be 100 years old in 2019. Founded as the Government Code & Cypher School in 1919, before changing its name to Government Communications Headquarters (GCHQ) in 1946 – and it has been keeping Britain safe ever since.

1919
Government Code and Cypher School (GC&CS) is established with intelligence and security functions

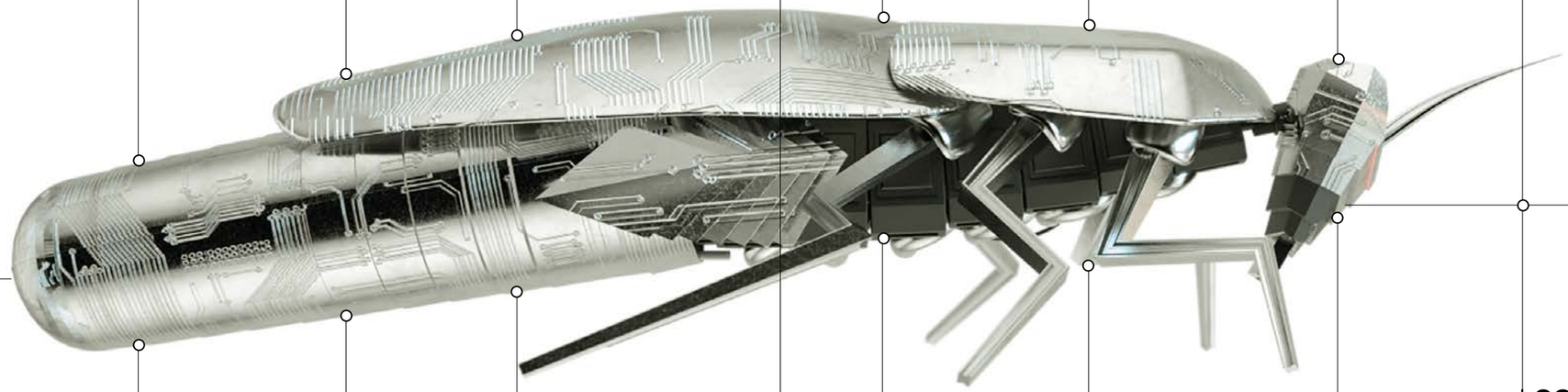
1926
An emergency codebook is issued to national authorities during the General Strike

1936
Alan Turing writes a paper **On Computable Numbers**, proposing a universal computing machine

1943
The first **Colossus** computer, the proto-computer, was created for the Newmanry section at Bletchley Park

1944
Single national authority for communications security is established

1946
First use of computers to generate cryptographic-material



1950s
Alvis, the first machine of the electronic era, is created and remains the workhorse for secure communications for over 30 years

1969
GCHQ incorporates the **Communications-Electronic Security Group** (CESG) becoming National Technical Authority for all aspects of cryptology

1970
Public Key Cryptography is conceived by James Ellis at GCHQ

1981
Early malware begins to be discovered at scale. A year later, **Elk Cloner** spreads beyond the lab it was created in

1988
The Morris Worm computer virus is distributed via the internet, resulting in the creation of the first Computer Emergency Response Team (CERT) in the U.S.

1989
The concept of the World Wide Web is created by Sir Tim Berners-Lee

1996
The **BRENT** Secure Telephone is introduced to provide secure communications across the whole of government

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

2010
The National Cyber Security programme of £860 million is announced to deliver the **'National Cyber Security Strategy 2011-2016'**

2013
The National Crime Agency and its National Cyber Crime Unit is launched

2014
CERT-UK, the national computer emergency response team, is launched

2015
The **'National Security Strategy 2016– 2021'** is launched, confirming cyber as a top-tier threat to the UK's economic and national security

2016
The NCSC is created as a 'one-stop shop' for cyber security, uniting separate parts of government that had a role in this area, within GCHQ

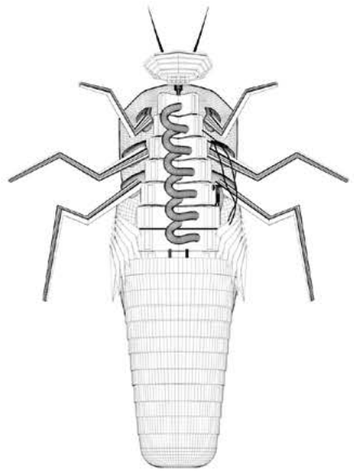
2017
The NCSC led the UK response to the global outbreak of Wannacry ransomware

2018
The NCSC dealt with its first 1,000 cyber incidents – a rate of more than 10 per week

GCHQ commences celebrations for its 100th anniversary and launches its second puzzle book to mark the occasion

2019
GCHQ's centenary events include an exhibition at the Science Museum exploring the science behind keeping the country safe, which opens in summer 2019; and the publication of its first authorised history in autumn 2019


National Cyber Security Centre
a part of GCHQ
Calendar
2017-2018



Can you find the secret codeword?
Visit ncsc.gov.uk/annual-review-2018

To find out more visit:

ncsc.gov.uk

@NCSC

National Cyber Security Centre

Designed and created by
Agent Marketing Ltd.
agentmarketing.co.uk