Cabinet Office

Progress against the Objectives of the National Cyber Security Strategy – December 2012

This document sets out some of the highlights of work done over the last year in support of the Cyber Strategy.

Objective 1: Tackling cyber crime and making the UK one of the most secure places in the world to do business in cyberspace

- Public-private sector information-sharing 'Hub' pilot successfully completed. Moving to full operational capability in January 2013. Membership will be expanded to include other organisations and sectors, further strengthening the UK's position as a secure place to do business.
- GCHQ , CPNI, and BIS, working with the Office for Cyber Security and Information Assurance produced a guide for industry Chief Executives and board members on the aspects they should attend to if they want safeguard their most valuable assets, such as personal data, online services and intellectual property. Called *Cyber Security Guidance for Business*, this was launched at a meeting of Ministers and chairmen of FTSE 100 companies on 5 Sep 2012.
- CPNI has expanded its scope to include companies not traditionally part of the Critical National Infrastructure.
- BIS produced a Cyber Sector research report into the UK cyber security sector to identify growth potential.
- The National Fraud Authority's *Action Fraud* reporting tool has been enhanced to be the UK's national reporting centre for fraud and financially motivated cyber crime. Over the past 12 months Action Fraud has taken over 46,000 reports from the public of cyber enabled crime. This amounted to attempted levels of fraud of £292 million.
- Capacity and capability of law enforcement cyber crime has expanded rapidly: the Police Central eCrime Unit (PCeU) has trebled in size and developed a framework for Cyber Specials; three new regional policing hubs have been established and the Government has published the Strategic Policing Requirement which covers major cyber incidents; the Serious Organised Crime Agency (SOCA) has increased its cyber capability including new cyber overseas liaison officers and posts dedicated to mainstreaming cyber and digital investigation across the agency.
- The Crown Prosecution Service (CPS) has responded to increased activity amongst the law enforcement community by devoting more resources to prosecuting cyber crime cases. As at the end of September 2012, the Department was prosecuting 29 'live' cyber crime cases.
- The CPS has expanded the content and delivery of its established in-house cyber crime training programme to increase awareness and capability within the organisation. It has developed four new training modules for CPS staff

specifically on cyber crime, covering the topics of cyber stalking, Cybercrime Basic and Cybercrime Intermediate and Indecent Images of Children.

- PCeU has reported that it has already exceeded its four year performance target, preventing £538m of harm in just one year, at a return on investment of £72 harm averted for every pound invested.
- PCeU's Internet Governance Team has ensured the suspension of over 15,000 websites, most associated with either fraudulent or 'pharmacrime' activity. This involved coordination of activity amongst 65 countries.
- SOCA has repatriated over 2.3 million items of compromised card payment details to the financial sector in the UK and internationally since 2011, with an estimated prevention of potential economic loss of over £500 million.
- SOCA led a day of global action (April 2012) to tackle Automated Vending Carts (AVCs) websites selling compromised financial data. Two UK arrests were made, SOCA intelligence assisted the US in seizing data for 26 AVCs and 36 domains. As a result of SOCA Alerts issued, a further 44 AVCs have been taken down, resulting in a major disruption cyber criminals' activities.
- Joint operations between SOCA and PCeU have been initiated to support the design and implementation of the new National Cyber Crime Unit – this will bring together the two units as part of the new National Crime Agency by October 2013. Three individuals were arrested in October 2012 for Conspiracy to Defraud and Money Laundering offences in the first of these operations.
- The National Fraud Authority has worked with industry partners to deliver awareness and behavioural change campaigns such as The Devils in Your Details. This reached over 4 million individuals. Building on this, the NFA have completed an NCSP-funded customer segmentation study to allow effective targeting of cyber security messages and have delivered targeted campaigns on online fraud, reminding people of the increasing threat of cyber crime.
- As part of the UK's continued global support for the Budapest Convention on Cybercrime in March the FCO announced a contribution of £100,000 to support the Council of Europe Global Project on Cybercrime. SOCA continue to work with international partners through dedicated overseas Cyber Liaison officers, their engagement with ICANN and with the Commonwealth Cybercrime Initiative.
- HMRC established a Cyber Crime Team to tackle tax fraud by organised criminals which went live in time to protect the self-assessment filing peak, with 7.65m customers filing online this year. HMRC's enhanced anti phishing capabilities are now leading to interception of 5 major threats a day, while their new cyber team has shut down almost 1000 fraudulent web sites in the last 12 months.

Objective 2: Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace

- GCHQ has invested in new capabilities better to identify and analyse hostile cyber attacks on UK networks, to improve our ability to detect attacks, and to sustain world class cyber capabilities in order to respond.
- The Security Service has developed and enhanced its cyber structures focusing on investigating cyber threats from hostile foreign intelligence agencies and terrorists and working with UK victims.
- The Centre for the Protection of the National Infrastructure helps organisations in the critical national infrastructure to be properly protected. CPNI has promoted the application of 20 critical controls and signposted a range of supporting advice to help organisations work towards effective cyber defence. This provides the technical foundation on which the Cyber Security Guidance for Business Booklet is based.
- CPNI is helping organisations in the critical national infrastructure and beyond to build better systems. It is actively influencing standards, researching vulnerabilities and focusing on the key technologies and systems of cyber infrastructure.
- MOD has established a tri-service Joint Cyber Unit, hosted by GCHQ in Cheltenham. The JCU training and skills requirements have now been established and it is currently developing new tactics, techniques and plans to deliver military capabilities to confront high-end threats.
- Cabinet Office, Security and Intelligence Agencies and other departments and agencies established unprecedented mechanisms for working hand in hand with sponsors and suppliers to the Games in handling and combating cyber threats.
- Government has enhanced and exercised national cyber incident management mechanisms.
- CESG and CPNI launched the Cyber Incident Response pilot to provide organisations with access to companies certified to be able to help them respond effectively to the consequences of cyber security attacks.
- CPNI has commissioned a major research programme with the University of Oxford with the aim of delivering advice, guidance and products aimed at reducing the risk of cyber insider acts.
- To protect core Government systems work has been done across the Public Services Network to create a new security model for the sharing of services including a common and standardised approach to assurance, Single Sign-on through an employee authentication hub, security monitoring, more effective policing of compliance and greater network resilience.

Objective 3: Helping shape an open, vibrant and stable cyberspace that supports open societies

- The UK delivered a successful London Conference on Cyberspace: over 700 participants from over 60 countries, leading to the 'London Agenda'. It worked with Hungary to deliver the follow-up Budapest Conference in October, and now working with South Korea to deliver the Conference in Seoul in 2013.
- The National Cyber Security Programme has allocated £2m per annum for an international Cyber-Security Capacity-Building Centre which will enable industry to back initiatives to tackle cyber crime and improve cyber security across the globe.
- Government and its industry partners delivered a successful Get Safe Online Week – for the first time run in conjunction with the EU and our US and Canadian partners as part of a drive to establish a global Cyber Security Month in October each year.
- The UK worked with NATO and the EU to help develop their emerging cyber strategies, on top of bilateral engagement with a broad range of countries.
- UK Government departments and law enforcement agencies have worked with international partners to encourage more countries to sign up to the Budapest Convention on Cyber Crime and to deepen international cooperation to tackle cybercrime through operational work.
- The UK has played a prominent role in developing internationally discussions on accepted norms of behaviour and Confidence Building Measures in cyberspace, notably at the UN Government Group of Experts and the OSCE.

Objective 4: Building the UK’s cyber security knowledge, skills and capability

- GCHQ launched a scheme to certify the competence of Information Assurance (IA) and Cyber Security professionals in the UK. Over 300 people have been accredited so far through the CESG Certification for IA Professionals scheme.
- The first eight UK universities conducting world class research in the field of cyber security have been awarded “Academic Centre of Excellence in Cyber Security Research” status by GCHQ in partnership with the Research Councils’ Global Uncertainties Programme (RCUK) and the Department for Business Innovation and Skills (BIS)
- GCHQ (in partnership with the Research Councils’ Global Uncertainties Programme (RCUK), (led by the Engineering and Physical Sciences Research Council (EPSRC)), and the Department for Business Innovation and Skills (BIS)have launched the first Research Institute to improve understanding of the science behind the growing Cyber Security threat.
- BIS announced funding for two Centres for Doctoral Training providing 48 PhDs on multidisciplinary cyber topics, in addition to 30 GCHQ sponsored PhDs also funded through the National Cyber Security Programme.
- Government launched a programme to help apprentices enter the cyber security sector through identifying and developing talent in school and university age students and to give opportunities to new recruits into GCHQ and our other Intelligence Agencies.
- Government has brought in changes to the ICT curriculum in order to strengthen computer science teaching in schools.
- In partnership with e-skills, pilot modules and materials (the ‘Behind the Screens’ initiative) have been completed to support the provision of cyber security education at GCSE level.
- Government has worked with Cyber Security Challenge, e-Skills UK and the Institute of Engineering and Technology to identify pathways so that people can move ‘mid-career’ into a cyber security career.
- Government has delivered ‘Protecting Information’ levels 1-3 and ‘Fraud and Corruption’ e-learning packages to the wider public sector.
- Training on cyber for mainstream staff in the Civil Service, law enforcement and the military is being rolled out.

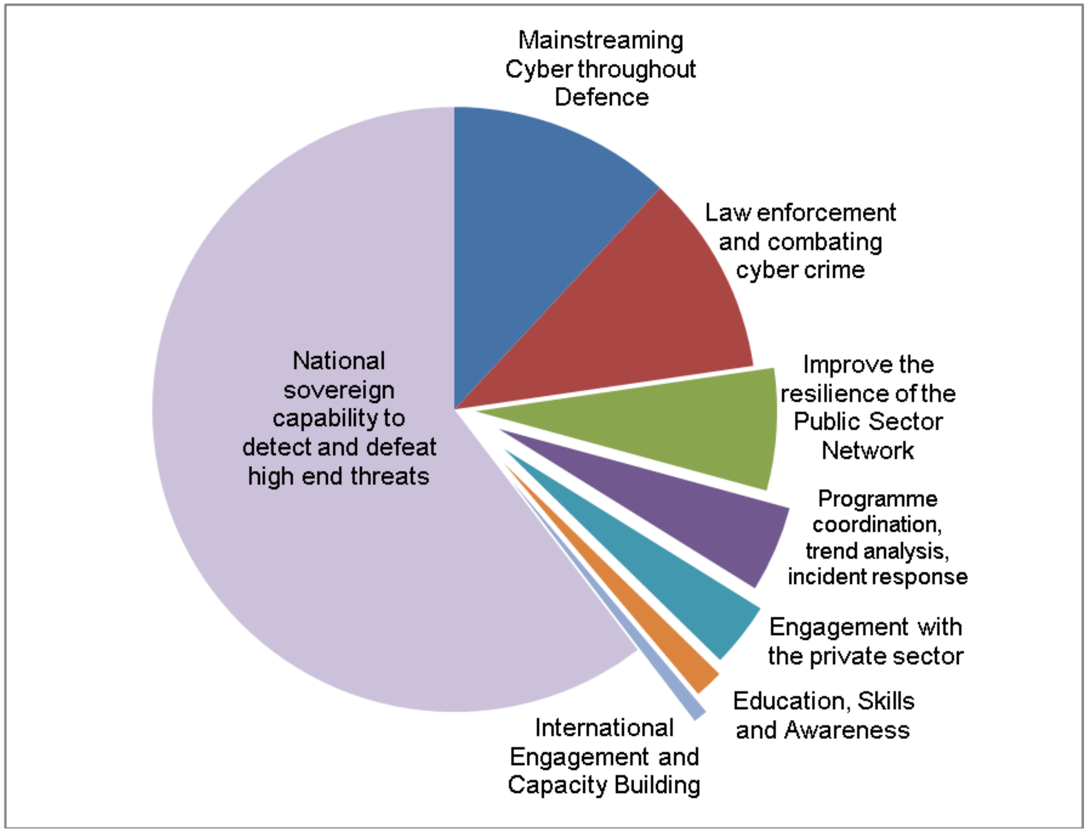
How the National Cyber Security Programme (NCSP) money has been spent:

Outturn and forecast spending in years 1 and 2 of the NCSP is set out below, with lead departments indicated in brackets. These figures do not include spending in support of cyber objectives that is not funded by the NCSP.

Spending has been spread across the breadth of HMG's cyber activities. In some areas, for example, skills and awareness, the bulk of spending will occur in the second half of the Programme as initiatives expand.

We are unable to break down 'sovereign capability' spend in the Intelligence Agencies for reasons of national security, but the capability this buys supports activity across all strands of the Programme.

- National sovereign capability to detect and defeat high end threats (Security & Intelligence Agencies, £157M)
- Mainstreaming Cyber throughout Defence (MOD, £31M)
- Law enforcement and combating Cyber Crime (Home Office, £28M)
- Engagement with the private sector (BIS, £17M)
- Improving the resilience of the Public Sector Network (Cabinet Office, £12M)
- Programme coordination, trend analysis and incident management / response (Cabinet Office, £9M)
- Education, skills and awareness (Cabinet Office, £4M)
- International engagement and capacity building (FCO, £2M)


Mainstreaming Cyber throughout Defence
Law enforcement and combating cyber crime
Improve the resilience of the Public Sector Network
Programme coordination, trend analysis, incident response
Engagement with the private sector
Education, Skills and Awareness
International Engagement and Capacity Building
National sovereign capability to detect and defeat high end threats