Cabinet Office

Progress against the Objectives of the National Cyber Security Strategy – December 2013

Cabinet Office

Progress against the Objectives of the National Cyber Security Strategy – December 2013

This document sets out highlights of work done over the last year in delivering the UK Cyber Security Strategy.

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

Tackling Cyber Crime:

- As part of the launch of the National Crime Agency (NCA), the National Cyber Crime Unit (NCCU) was established in October 2013. The NCCU brings together the skills and expertise of the precursor units, SOCA Cyber and the Police Central e-Crime Unit, into a world-leading organisation dedicated to fighting the most serious cyber criminals. They are supported by GCHQ, whose capabilities have helped to disrupt sophisticated international cyber crime activity. Recent NCCU activity includes:
    - in the weeks running up to its launch, it helped smash a $500 million worldwide computer scamming ring through a joint operation with the FBI and industry in over 80 countries. More recently, a joint operation between the NCCU, the FBI and other law enforcement partners led to the arrest of 11 people for crimes that were estimated to have caused over $200 million of losses to individuals and businesses;
    - in November 2013, it issued an urgent alert to inform internet users of a risk of infection linked to a mass email spamming event. The emails, that appeared to be sent from banks and financial institutions, were sent to millions of UK customers and contained a piece of ransom ware called ‘Cryptolocker’. The Alert provided guidance and additional links for victims of this attack;
    - it provided a enabled security measures to be put in place and prevented approximately £14 million from potentially being extracted from the swift response to a financial institution whose customer accounts were under threat from a malware infection. The quick response e accounts;
    - and it is also providing specialist support to wider NCA operations, such as the recent arrests in connection with the online trade of illegal substances.
- The Government has been building cyber capacity more widely in the law enforcement community:
    - dedicated cyber units are being established in the nine Regional Organised Crime Units (ROCU). These will be able to investigate cyber crime that crosses the boundaries of the police forces in their area, as well as supporting the work of the NCCU to investigate the most serious cyber crimes;
    - the College of Policing has mainstreamed cyber investigation skills into the training of thousands of UK police officers (detailed under objective 4 below);
    - the NCA is investing in technology that will improve analysis and exploitation of intelligence and assist in investigations into malware, enhancing its ability to respond to cyber crime;

- the Crown Prosecution Service continues to build its ability to mount cyber prosecutions, with notable successes including the prosecution of four Lulzsec computer hackers who were jailed for a total of seven years; and
- the Action Fraud reporting tool is now the central point of contact for reporting online fraud and financially-motivated cyber crime. Members of the public can go to the Action Fraud website (www.actionfraud.police.uk) for advice on how to avoid fraud, or to report an instance where they have been a victim. All reports are forwarded to the National Fraud Intelligence Bureau for assessment and investigation. Between April and August 2013, around 20,000 crime reports per month were fed into the National Fraud Intelligence Bureau by Action Fraud.

- Government departments, including DWP and HMRC, with expert advice from GCHQ, have been working to counter fraud in the provision of their digital services:
  - HMRC provides cyber security advice to its customers on a daily basis via online guidance and Twitter – for example by raising awareness of phishing attacks using fake HMRC emails. Since January 2013, more than 200,000 taxpayers have visited the relevant HMRC web pages;
  - dedicated cyber crime capability in HMRC has provided specialist advice to approximately 20 criminal cases, resulting in an overall Revenue Loss Prevented of more than £40m;
  - anti-phishing capabilities have been developed. HMRC has shut down more than 2,300 fraudulent websites since January 2011, with the average time between detection and “take down” now just 7.5 hours. An enhanced DWP anti-phishing capability has assisted with the identification of websites masquerading as DWP sites;
  - in co-operation with IT suppliers, DWP has been identifying and blocking attempts to access DWP online services from overseas IP addresses. There were some 28,500 attempted visits to the Universal Credit online service in the last 3 months, from 36 different countries; and
  - an innovative new identity assurance service is being developed that will enable people safely and securely to verify their identity to use online services and allow government to be confident that those using online services are who they say they are. The Identity Assurance Programme, developed by the Government Digital Service, has published new cross-government standards for securely delivering online public services; developed a service to provide identity assurance for individuals, and supported pilot projects with industry and other public bodies to test different aspects of the service. The Programme has engaged stakeholders, including privacy and consumer organisations, to develop interoperability standards and a market for identity assurance services, including through membership of the Open Identity Exchange. Contracts with five identity providers have been signed and the first services using identity assurance will go live in early 2014.

- With most serious cyber threats originating overseas, the Government has worked with partners internationally to enhance the global response to cyber crime:
    - the NCCU is working closely with partners from the US, Australia, and Europe to develop effective models for global joint cyber investigations, and is working to enhance capabilities internationally to help tackle cyber crime threats at source;
    - through the United Nations Office of Drugs and Crime (UNODC), the UK has helped lead work on a range of practical co-operative measures to tackle cyber crime, while championing the Budapest Convention as a best practice model for all countries seeking to enhance their national cyber crime fighting capabilities. As of November 2013, 40 states have ratified the Budapest Convention; while a further 11 states had signed the Convention but not ratified it; and
    - the FCO has provided guidance and assistance, including financial support, to cyber crime initiatives in the Commonwealth, UNODC and the Council of Europe.
- All this work has been based on a solid evidence base. The Government conducted a review of all the published evidence on the scale and nature of cyber crime in the UK in order to help better inform our response to this threat. The findings were published by the Home Office alongside the Serious and Organised Crime Strategy in October 2013 (www.gov.uk/government/publications/serious-organised-crime-strategy), highlighting the varied and changing nature of cyber crime. The review also outlines some of the steps being taken continuously to improve our understanding of the scale and nature of the cyber threat.

Secure to do business in cyberspace:

- The Government has worked hard to raise business awareness of cyber security risks and provide practical advice on addressing them, with briefings from Ministers and Intelligence Agency Heads, industry engagement by government departments, and the publication of authoritative guidance.
- More than seven thousand businesses have downloaded the best practice cyber security guidance - ‘10 Steps to Cyber Security’. This was developed by Government during the first year of the strategy, providing UK industry with clear guidance on steps they could take to increase their cyber security. It has since received international recognition with a cyber security innovation award by the globally recognised SANS Institute of America which described the booklet as delivering a ‘big step forward toward a global minimum standard of due care in cyber security”. The World Economic Forum also endorsed the 10 Steps guidance at its annual meeting in Davos in January 2013. In April 2013, the Government published further guidance tailored to the needs of smaller businesses.
- In July, Government in partnership with the audit community launched the Cyber Governance Health Check for FTSE350 companies. The first stage, the Tracker, was delivered in November. This online survey of the governance behaviours of each company was completed by 62% of the FTSE 350 and resulted in individual benchmarking reports for each participating company and an aggregated report, which is

hosted on the Gov.uk website. The next stage, a Diagnostic tool which will build on the Tracker results, will be rolled out by the audit community in 2014.

- The Government has provided additional support and guidance to the largest and most critical companies to help protect critical services from cyber attacks:
    - the Centre for the Protection of National Infrastructure (CPNI) has published a range of cyber security-focused guidance to raise awareness of threat and vulnerability and provide advice on mitigation measures. Topics include spear-phishing, insider threat cases, online reconnaissance, passwords and mobile devices.
    - a Cyber Risk Advisory Service has been developed by CPNI providing in-depth support to senior executives and boards of the UK's most economically important companies and academic institutions. To date the service has engaged with 200 companies. The aim is to improve their understanding of the impact of cyber threat and its effect on long-term performance and competitiveness, and to help them mitigate their organisation's risk exposure to embed good cyber security practice and to improve corporate governance and cyber risk management in UK business.
    - CPNI has been developing new cyber security awareness training courses for senior managers and engineers with responsibility for maintaining industrial control systems. New courses are set to launch in 2014.
- The Cyber Security Information Sharing Partnership (CISP) was launched in March 2013. The collaboration environment allows members of the CISP Community to exchange cyber threat information in real time in a dynamic environment to help protect their organisation and the UK as a whole from cyber threats. The Fusion Cell (comprised of government / industry network defence analysts) examines the information and data feeds and provides enriched contextual cyber threat information and advice to the CISP community. CISP membership has broadened beyond the CNI community to SMEs, small public sector organisations, academia and supply chains. There are now 700 individual members and 250 member organisations.
- In the finance sector, the Bank of England's Financial Policy Committee recommended measures to improve cyber resilience in June. The recent 'Waking Shark II' exercise tested cyber defence and incident handling in the sector. The CISP platform played an integral role in the exercise, enabling participants to share 'real-time' threat information as the scenario developed.
- The Government continues to monitor the cyber threat to UK business. In partnership with PwC, BIS published its annual Cyber Breaches Survey in April 2013. The survey suggested that 93% of large organisations and 87% of small businesses had experienced a cyber security breach in the previous year. However there are also strong indications that cyber security awareness is rising. The recent FT and ICSA boardroom Bellweather survey of FTSE 350 company secretaries indicated that 98% had seen the Government's 10 Steps advice, and two-thirds had actively discussed what it meant for their firms.

Promoting economic growth:

- The Government launched the UK Cyber Exports Strategy in May 2013 to actively support UK cyber export opportunities by helping UK companies to penetrate overseas markets, improve overseas awareness of UK industry capabilities, encourage information sharing to improve competitive positioning and increase awareness of the emerging complexities of export risks.
- The "Cyber Growth Partnership", a joint Government and UK industry collaboration, was created to stimulate domestic and exports growth in cyber security. The group membership includes representatives from government, large companies, SMEs, trade associations and academia. The group is co-chaired by a BIS Minister and BT's CEO. Early successes include the launch of a "cyber supplier to HM Government" scheme, collaboration on priority markets, and an economic growth target for cyber exports.
- More than £500,000 has been made available to UK SMEs via cyber security Innovation Vouchers to improve their cyber security, protect their business ideas and support growth. Administered by the Technology Strategy Board (TSB), innovation vouchers are designed to encourage businesses to draw in expertise from outside their business to enable them to grow and develop. With cyber security proving more popular than any of the other strands of innovation voucher schemes, TSB agreed to further funding and it is anticipated that Government will have committed close to £1 million in cyber voucher support by the time the current call for applications closes on 22 January 2014.
- In November 2013, following industry consultation, the Minister for Universities and Science announced a preferred organisational standard for cyber security to help businesses demonstrate use of best practice. This new profile will be available in March 2014 when businesses will be able to audit themselves against it. Government will use this profile in its own procurement, where relevant and proportionate.

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

Resilience to Cyber Attack:

- The Government is putting in place best practice structures to strengthen resilience to cyber attacks. The design of the new organisation for national cyber incident management, CERT-UK, has been agreed and the Director is in post. Initial operating capability will be achieved early next year. The new CERT will work closely with government, industry, academic and international partners to co-ordinate responses to cyber incidents in the UK and internationally.
- To ensure the critical national infrastructure is resilient to cyber risk:
    - the Government is working with incident response companies and academia to research and publish good practice on how the UK's critical national infrastructure and other economically important businesses can best prevent, detect and recover from targeted cyber intrusions and attacks. Based on real incidents, the first publications and presentations in summer 2013 were well

received by cyber security managers and their network defenders. The latest phase of the research is focused on detecting specific elements of cyber intrusion; a series of briefings and publications are due in early 2014.

- over the last year the Government has held 10 exercises, working with 30 industrial partners and 25 government departments and agencies, to test cyber resilience and response in key sectors including finance, law enforcement, transport, food and water. There has also been liaison with both EU and US exercise discussion and planning groups.

- the Government, under its Trustworthy Cyber CNI research initiative, has been enhancing its understanding of the key technological dependencies that underpin the UK's critical national infrastructure. In 2013 CPNI partnered with the Institute of Engineering and Technology (IET) to research and publish guidance on "Cyber Security and Resilience of the Built Environment" which includes a range of measures to manage the risks. Positive reaction from industry has instigated further IET-led effort in this area.

- protecting the CNI from insider threat (individuals working within a company) has been a focus of work this year for the CPNI. It has also been promoting the role of personnel security in ensuring good cyber security, for example through personnel security risk assessment and development of a clear organisational security culture. Six animations on communicating personnel security messages have also been uploaded to CPNI's YouTube channel in order to raise general awareness. Meanwhile research, conducted in partnership with IBM, i to i research and the Universities of Oxford, Leicester and Cardiff, is developing practical methods to help organisations detect and prevent security insider incidents. The teams have been regularly presenting on their progress to international and industrial forums.

- CNI sector Information Exchanges (IEs), representing over 250 companies, have continued to focus on cyber security issues, complementing the virtual information exchange taking place through the CISP. CPNI held its first annual conference for IE members this year (IE13) focussing on cyber-related issues including threats to SCADA (Supervisory Control and Data Acquisition) and cyber insider threats.
- two Cyber Incident Response (CIR) schemes were formally launched in August 2013 by GCHQ and CPNI. These schemes accredit providers of incident response and clean-up services so that organisations that may be victims of cyber-attack can procure appropriate services with confidence.

- The Government continues to strengthen the protection and resilience of its own IT systems:

  - specialist cyber security advice is provided by GCHQ's CESG, the national technical authority on information assurance. CESG has issued security guidance for use by public sector organisations covering eleven common desktop and mobile platforms including Android, Windows 8, Blackberry 10, iOS, Samsung, Google and OS X. This guidance provides information on how these devices should be provisioned, configured, and deployed to ensure a suitable level of security for remote working.

- CESG's resources are being prioritised to focus on address the highest levels of cyber security risk for the most important national IT networks and systems. This ensures that CESG's unique technical expertise is directed to where it can deliver greatest benefit.

- the Office of the Government Senior Information Risk Owner (OGSIRO) has been created to deliver an appropriate and effective risk management regime for information and cyber security risks for all major Government IT projects and common infrastructure components and services. OGSIRO has issued the Information Risk Directive and oversees the Pan-Government Information Risk Register across Government**.**

- public sector organisations began to move to the Public Services Network (PSN) this year with 13 now fully transitioned. The PSN has published operational security standards and guidance to help address common security problems such as patch management and malware protection and has completed Phase 1 of the building of the new PSN Security Operations Centre.

- through the National Archives, the Programme is providing briefings to Government board and audit committee members. By the end of this financial year, the team will have provided briefings on cyber security to more than 100 board and audit committee members across the public sector, including key departments such as DWP, DfT and Defra.

- DWP has been developing a Threat Intelligence capability that includes: an analytical environment to identify cyber anomalies on its systems; a social media analytical service and an Internet based threat intelligence service. The majority of these services have recently been brought into live service and are already providing insights to DWP online services.

- across Government a new identity assurance service will enable people safely and securely to verify their identity to use online services and allow Government to be confident that those using online services are who they say they are. In two years the Identity Assurance Programme has published new cross-government standards for securely delivering online public services; developed a service to provide identity assurance for individuals and supported several innovative projects with industry and other public bodies to test different aspects of the service. The Government Digital Service has worked with stakeholders worldwide, including privacy and consumer organisations, to develop interoperability standards and a market for identity assurance services, including through membership of the Open Identity Exchange, and established an intensive programme of user research to inform the ongoing development of the service. Contracts with five identity providers have been signed.

Protecting our interests in cyberspace:

- GCHQ has continued to invest in new capabilities and technical infrastructure that increase the Government's ability to defend and protect the UK against increasingly sophisticated threats faced in cyberspace. These capabilities support and inform a wide range of the Government's work on cyber security, including tackling cyber crime and protecting critical national infrastructure. It would not be appropriate to provide specific details of this activity in a public document, but it has been reported to the Intelligence & Security Committee of Parliament.
- The Government has continued to strengthen the cyber security of the armed forces and the military supply chain, and is mainstreaming cyber into Defence planning and operations. Specifically:
    - the Defence Cyber Protection Partnership (DCPP) to improve cyber security within the defence supply chain has been formed with 12 prime defence contractors, and with ADS and techUK who represent small to medium enterprises (SMEs). The DCPP is concentrating on measurements and standards, communication and awareness in the supply chain, and information sharing. To ensure best value for money and coherence with wider work on cyber security standards the partnership is using and building on initiatives that exist across government such as the Cyber Information Sharing Partnership (CISP) and the '10 Steps' guidance: this is being used as a self-assessment tool through the supply chain.
    - the Joint Forces Cyber Group (JFCyG) was stood up in May 2013 to deliver Defence's cyber capability. The group includes the Joint Cyber Units (JCUs) at Cheltenham and Corsham, with the new Joint Cyber Unit (Reserve) which is using innovative approaches to attract skilled cyber security professionals into a 'Cyber Reserve'. JFCyG continues to develop new tactics, techniques and plans to deliver military capabilities to confront high-end threats.
    - recruiting for the Joint Cyber Unit (Reserve) commenced in October 2013 with a high number of applications received in response to the Defence Secretary's announcement in September 2013. The Unit provides support to the Joint Cyber Unit (Corsham), the Joint Cyber Unit (Cheltenham), and tri-service Information Assurance units, and will represent a significant uplift in the number of Reservists employed in cyber and Information Assurance. Its creation allows Defence to draw on individuals' talent, skills and expertise gained from their civilian experience to meet cyber threats.
    - the MOD has continued to mainstream cyber into its research programs. Specifically this year it has invested in cross-government research into cyber standards and best practice, developed test assurance for defence cyber capability and training for our military forces, and sponsored seven cyber-related projects with Defence Science and Technology Laboratories (DSTL).

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

- The UK has made a major contribution to two significant advances in the international cyber agenda. First, a UN Group of Government Experts, in which a UK expert participated, agreed a consensus report in June 2013 on aspects of state behaviour in cyberspace. A key outcome was agreement that international law applies in cyberspace. The agreement has passed through United Nations General Assembly (UNGA) First Committee under a consensus resolution. Second, in December 2013, at the end of nearly two years of negotiations, the 57 participating States in the Organisation for Security and Cooperation in Europe (OSCE) agreed the first set of multilateral confidence building measures in cyberspace. The two documents set a marker for multilateral cooperation on these issues, will contribute significantly to improved understanding and to reducing the risk of conflict in cyberspace, and provide a strong basis for further discussions in 2014.
- In addition, the UK worked closely with the government of South Korea to deliver the successful Seoul Conference on Cyberspace in October 2013 under the theme of Global Prosperity through an Open and Secure Cyberspace – Opportunities, Threats and Co-operation. At the Conference (at which 85 countries were represented), the UK succeeded in communicating a clear statement of its policy positions, particularly the overriding importance of maintaining an open Internet for economic progress, and put forward practical suggestions for how to move this on, maintaining the UK's reputation as a leading international player on cyber.
- The UK has taken a leading global role in increasing the impact, scale and pace of international capacity building efforts, and improving global co-ordination mechanisms around cyber security threats. The UK has established a cyber capacity building fund, which among other initiatives has funded a Global Cyber Security Capacity Centre, now up and running at Oxford University. We are starting to see real world results from this fund, with the arrest in June 2013 of a major global e-fraud network following UK training of partners in South East Asia.
- The Government has been advancing its vision of an open and borderless internet and a multi-stakeholder model of internet governance through multiple international fora:
    - working with EU Member States and the institutions to develop the new EU Cyber Security Strategy launched in February 2013 and endorsed by the EU Council in June 2013. The UK encouraged creation of a Friends of the Presidency to provide Member State oversight of its implementation;
    - working with the European Commission to influence the draft Network and Information Security Directive to reflect the UK position, including undertaking a UK Impact Assessment to gather industry and stakeholder views on the proposed measures in the Directive;
    - through the G8, whose Foreign Ministers' communiqué in April 2013 recognised the central importance of the economic benefits of the internet, endorsed the work of the UN Group of Government Experts (UNGGE) and promoted international cyber security capacity building;

  - with the signing by the Foreign Secretary of the World Economic Forum's 'Principles for Cyber Resilience', engaging the global business community in a conversation about managing cyber risks in a hyper connected world;

  - through the secondment of staff to the NATO Cooperative Cyber Defence Centre of Excellence. The centre is an International Military Organisation located in Tallinn, Estonia. The centre's mission is to enhance capability, cooperation and information sharing among NATO, its member nations and partners in cyber defence;

  - through dialogue and lobbying at the WSIS (World Summit on Information Society) Review meeting at UNESCO in February 2013; at the International Telecommunication Union (ITU) meetings; and at the UN General Assembly; and

  - through strengthening its bilateral partnerships on cyber, continuing to work closely with like-minded countries.

- We are also investing in the future, engaging top international students in the UK on cyber to help ensure that future cadres of global leaders have a good understanding of cyber security issues and that the UK has the international links in place in future to engage with other countries in this field. A new engagement process is starting with Chevening, Commonwealth and Marshall Scholars from Africa, Asia, and America by selecting a number of these students to attend the annual Academic Centres of Excellence in Cyber Security Research Conference in December and to enrol in an international cyber policy course at Cranfield University.
- The UK's international approach is supported by the Multi-stakeholder Advisory Group on Internet Governance (MAGIG). Formed in May 2013, it brings together government departments with representatives from UK industry, civil society and academia to: collaborate on UK inputs to internet governance events; comment on UK government policy on internet governance; and ensure broad understanding within the UK of the Government's approach.

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

Skills and Capability:

- The Government has taken steps to increase and strengthen cyber content at all levels of education:
    - creating a new coding module for use within the Computer Clubs for Girls (an initiative which has previously engaged over 135,000 10-14 year old girls); this covers how algorithms work, alongside coding in a range of programming languages.
    - funding the development of ten modules of cyber security learning and teaching materials at GCSE and A-level (the advanced-level strand within e-skills UK's 'Behind the Screen' initiative). Materials are to be released to schools in January 2014. The A-level materials cover two main areas: including the linkages between changes in technology and the developing requirement for cyber security; and understanding of the causes, aftermath, recovery and lessons learnt relating to a hacking scenario.
    - working with academic partners, through the Trustworthy Software Initiative, to develop teaching materials to prevent security vulnerabilities in the design and development of software. Teaching materials developed and trialled in three universities will be extended with a view to incorporation within software engineering and potentially a range of other undergraduate teaching in 2014/15; Complementing this work, e-skills UK have incorporated information security learning outcomes into the development of their new Software Development for Business degree. This was designed with input from leading employers to ensure its relevance to the needs of today's business, and several universities are expected to first offer this new degree in 2014/15.
    - funding the ongoing Cyber Security Skills Alliance pilot of an employer-sponsored bursary scheme at Masters level.
    - funding a Graduate Prospects' development of an industry profile for cyber security, helping stimulate higher education student interest and raise the profile of cyber security as a new discipline with good career possibilities.

- The Government has also been working with industry and academic partners to increase the availability of cyber skills in the workforce, through apprenticeships and other initiatives:
    - supporting the e-Skills UK 'Cyber Academy' and its employer-led programme of skills activities. Advanced stage activities include the ongoing development of a cyber security Higher Apprenticeship scheme, providing a distinctive new route to cyber security professional work and a viable alternative to the traditional full-time degree route. Ten businesses contributed to the employer definition of appropriate learning outcomes. The new apprenticeship framework developed becomes fundable by the Skills Funding Agency early in 2014. Sixty-seven IT apprentices are already using information security materials and learning outcomes in advance of the launch of a cyber security specific Higher Apprenticeship scheme. e-skills UK estimate 220 young people will be recruited to the scheme in 2014. As part of this work, seven new information security units were created to sit on

the Qualifications and Credit Framework. These cover core topics (security audits, forensic examinations, incident investigation, incident management, information system security testing, risk assessments, and risk management) and are available for any awarding body to incorporate into a qualification (such as the City and Guilds level four Diploma in Information Security Professional Competence) which is the competence qualification within the new apprenticeship framework. Work is continuing to agree a suitable foundation degree to form the apprenticeship's knowledge component.

- other activity underway includes a school outreach programme, aligned with existing e-skills UK education and careers activities. including the launch of the 'Secure Futures' campaign, and a range of activities being trialled such as the delivery by schools of 'collapsed curriculum' days where cyber security becomes a focus for lessons in many subjects, and drawing employers in to enrich pupils' learning.

- the Information Assurance Advisory Council (IAAC) summer 2013 pilot of a national cyber security HE internship scheme. e-skills UK has committed to run a national internship scheme in 2014 as part of its 'Cyber Academy' suite of skills projects and BIS hosted a workshop for various stakeholders to help inform detailed planning.

- CESG's Certified Professional (CCP) scheme, which provides a firm foundation for the UK's emerging cyber security profession by setting a standard for individual accreditation. There are now over 800 professionals who have demonstrated they have the right levels of skills, knowledge and experience to be awarded CCP certification and this number continues to grow. The CCP is now available to the private sector; and

- innovative initiatives to encourage young people to get into cyber careers. Most notably, the Government supports the Cyber Security Challenge, launched in 2010, since then over 10,000 people have registered to take part. A wide range of sponsors (industry as well as government) not only provide the financial backing for the Challenge but also design, develop and help run the competitions themselves. Many of the participants have gone on to pursue careers in the industry as a result of the Challenge.

- The Government has invested in training its own workforce to ensure that the public sector has better general cyber awareness and specific cyber skills:
    - since 2011, the National Archives (TNA) has been delivering training to civil servants in a variety of different roles across a diverse range of public sector organisations. The training comes in a range of different formats, including IAO training workshops, IAO roundtable discussions, SIRO knowledge exchange sessions and management board briefings. This year, TNA have trained 697 public sector staff in information assurance and cyber security (145 SIROs, 344 IAOs and 208 others) in this way.

- TNA have also, with National Fraud Authority (NFA), produced the e-learning course 'Responsible for Information', available on the Civil Service Learning website. Since July 2013 nearly 70,000 central government users have undertaken the course. The course is freely available to the wider public sector and approximately 950 organisations use it to train their staff.

- civil Service Learning have developed a comprehensive training and development programme to develop cyber skills within DWP, which will increase cyber security awareness and capability.

- a range of training has been developed across the police to increase knowledge and understanding of cyber crime and how to investigate it. This includes e-learning packages and classroom courses. The College of Policing has been preparing to roll out these courses to train 5,000 police officers. The four e-learning packages for police officers were rolled out sequentially, starting in April 2013. To date, over 11,000 have been delivered. And the NCA is expanding its own investment in cyber skills, with 2,200 NCA officers being trained to become digital investigators who can work alongside and support existing NCCU specialists;

- the Crown Prosecution Service (CPS) is running Cyber Crime courses including courses on cyber stalking and prohibited sexual images. So far over 1,000 CPS lawyers have completed the training;

- the Security and Intelligence Agencies have launched a new Higher Apprenticeship Scheme to attract motivated and technically-minded people to join the Intelligence Academy. The apprentices will undertake a structured training programme that will equip them with the cyber skills and experience necessary to enable them to build, develop and further advance the Agencies technical capability in the future. The scheme will play a vital role in supporting the Intelligence Services in their ongoing mission to tackle terrorism, organised crime, counter espionage and cyber threats to the UK.

- MOD, through Cranfield University, has launched two part-time postgraduate education aimed specifically at the Defence community, leading to Cyber Masters degrees. 50 MOD personnel are currently undertaking these cyber post-graduate courses. The initial modules were run in September, with students coming from across Defence including Reservists. The intent is to develop an understanding of cyber operations and threats amongst future Defence leaders who can then more effectively manage the threats and opportunities of cyberspace.

- two master-classes have been delivered for senior Defence leaders to give them a clear understanding of the cyber environment and how it impacts on their role. A programme of further events is continuing for mid-career and senior military and civilian officers over the coming year.MOD are further developing a career management strategy to ensure continuing access to talented and experienced cyber specialists. An interim career management solution has been rolled out for cyber mainstream staff in the military, to help recognise, manage, and retain cyber skills to support MOD’s role in defending national security in cyber space.

- MOD have delivered a pilot Cyber Operations Planning Course. A further course is planned in early 2014. The Cyber Reserves Induction Programme is being developed to be delivered in April 2014. 60,000 people have completed the cyber awareness module in Defence, 50 people are currently taking Cyber Post Graduate courses.

Research:

- The Government has provided funds to boost the UK's cyber research capabilities, to keep the UK at the leading edge and help stimulate growth in the UK's cyber security sector.
- Three new Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) at UK universities have been launched (Birmingham, Cambridge, and Newcastle) to recognise and promote the UK's world-class cyber security research capability. This is in addition to the eight existing ACE-CSRs (Bristol, Imperial College, Lancaster, Oxford, Royal Holloway, Southampton, Queens University Belfast, and UCL).
- Two Centres for Doctoral Training in cyber security have been launched, hosted by the University of Oxford and Royal Holloway University of London. These Centres will train PhD students to gain the high-end cyber security skills to tackle current and future cyber challenges. Initially 66 PhDs are planned: 48 sponsored by government and 18 by the Universities and Industry. Further to these, GCHQ has sponsored 22 doctoral studentships at the ACE-CSRs.
- The Research Institute (RI) in the 'Science of Cyber Security' has been running for a year and progress was presented at its first annual conference at the end of October. During its first year the RI has delivered tangible research findings across all four projects which are already demonstrating benefit to industry, and has put in place an advisory group of international experts.
- A second Research Institute has been established, centred at Imperial College London looking at 'Automated Program Analysis and Verification'. This will stimulate innovative cyber research and it is hoped will reduce the vulnerability of software products to cyber attack in the future.
- The Government has announced that a third Research Institute looking at Trustworthy Industrial Control Systems is to be created at Imperial College London. Industrial Control Systems now play a major role in ensuring the correct functioning of significant parts of the UK's Critical National Infrastructure. The Institute will help build capability in finding innovative ways to protect the industrial technologies that support our key services.

Wider awareness:

- The Government has worked with industry partners to deliver awareness and behavioural change campaigns such as The Devils in Your Details. This reached over four million individuals. Building on this, a customer segmentation study has been conducted to allow effective

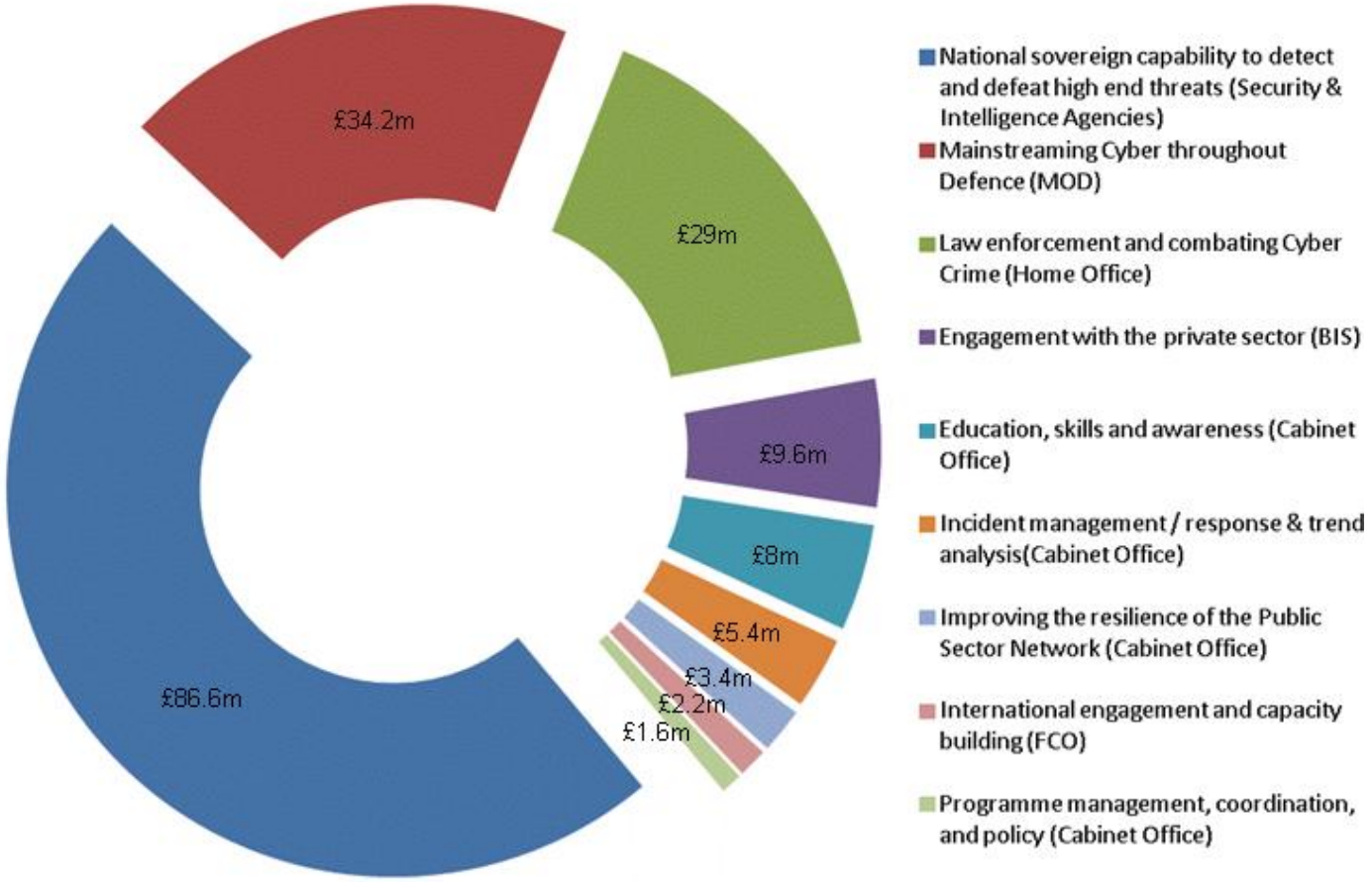
targeting of cyber security messages and have delivered targeted campaigns on online fraud, reminding people of the increasing threat of cyber crime. This analysis has informed the major forthcoming awareness campaign.

- The Government also supports Get Safe Online (GSO), a joint government industry organisation which promotes practical steps for the public and businesses to keep themselves safe online. GSO has run a number of campaigns this year including Valentine's Day; Mobile May: Holiday Fraud: Ticket Scams; Auto scams; Parents Campaign; and a Christmas campaign. These campaigns and GSO's presence in social media have led to increased visits to GSO's website.

Cabinet Office

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

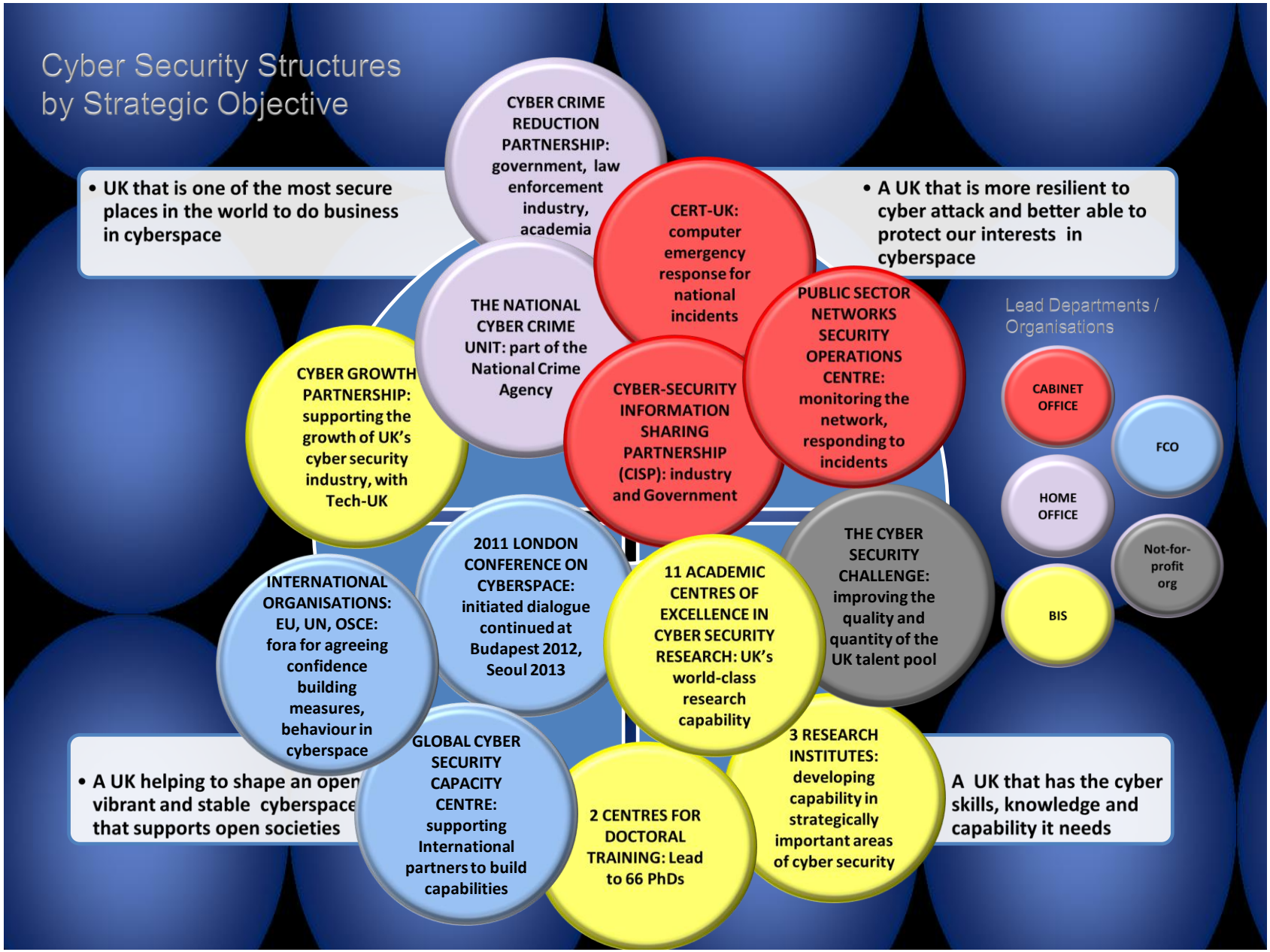
Planned spend for year 3 (FY13/14) of the NCSP is set out below, with lead departments indicated in brackets. These figures do not include spending in support of cyber objectives that is not funded by the NCSP. As shown below, spending has been spread across the breadth of Government's cyber activities. The categories set out below support one another – for example, funding described below as private sector will also bring benefit to law enforcement to the extent it helps prevent cyber crime – but for the purposes of clarity within this document, spend has only been allocated to one category. 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.



Cabinet Office

UK Cyber Security Structures: An Overview of some Key Organisations, by Strategic Objective

1. A UK that that is one of the most secure places in the world to do business in cyberspace	2. UK that is more resilient to cyber attack and better able to protect our interests in cyberspace	3. A UK helping to shape an open, vibrant and stable cyberspace that supports open societies	4. A UK that has the cyber skills, knowledge and capability it needs
The National Cyber Crime Unit (NCCU)	**CERT-UK**	**International Cyber Conferences**	**Academic Centres of Excellence, Centres for Doctoral Training & Research Institutes**
Now live within the new National Crime Agency (NCA), the NCCU began operating in shadow form in spring 2013, bringing together and enhancing capabilities from the Police Central e-Crime Unit and the Serious Organised Crime Agency's cyber team. The NCCU is transforming the way the UK combats the threat from cyber criminals, using its increased operational resources to deliver arrests, disruption and prevention and the NCA's enhanced intelligence picture to proactively pursue criminals.	We are establishing a new National Computer Emergency Response Team (CERT) to improve national co-ordination of cyber incidents and act as a focus point for international sharing of technical information on cyber security. CERT-UK, which will become operational in early 2014, will allow us to bring different strands of our cyber incident response close together, so that we can be as agile as possible in responding to the increasingly complex cyber landscape.	The 2011 London Conference began the international dialogue for building a secure, resilient and trusted digital global environment. It initiated a global conversation on the future of the Internet and establishing norms of behaviour in cyberspace. We are taking forward the London Conference agenda in various ways, in particular through our contribution to the Budapest Cyber Conference in 2012 and again in Seoul in October 2013. The Netherlands will host the next in early 2015.	Recognising and promoting the UK's world-class research capability, GCHQ, BIS and the Engineering and Physical Sciences Research Council (EPSRC) awarded 11 UK Universities "Academic Centre of Excellence in Cyber Security Research" status. Two Centres for Doctoral Training and GCHQ-sponsored studentships will lead to up to 96 PhDs. Three Research Institutes are developing capability in strategic areas of cyber security.
The Cyber Crime Reduction Partnership (CCRP)	**The Cyber Security Information Sharing Partnership (CISP)**	**Global Cyber Security Capacity Centre**	**The Cyber Security Challenge**
The Partnership brings together government, industry, academia and law enforcement agencies to coordinate efforts on reducing cyber crime. This industry engagement group seeks to raise awareness of cyber crime, improve reporting, and help industry become more resilient to the threats. Its work aligns with the Serious and Organised Crime Strategy and the National Cyber Security Strategy. It is co-chaired by the Minister for Security and the Minister of State for Universities and Science.	A secure platform for Industry and Government to share information on threats in cyberspace. Includes a "Fusion Cell" supported by MI5, GCHQ and the NCA along with industry analysts in partnership. They produce an enhanced picture of cyber threats facing the UK for the benefit of all partners. This situational awareness function will feed into the new National CERT when it becomes operational in early 2014. Since CISP launched in March 2013, membership has been extended beyond companies within the Critical National Infrastructure, including to smaller businesses, and supporting delivery of objective 1.	The Global Cyber Security Capacity Centre at Oxford University aims to help other states and organisations across the world to build up their cyber capabilities effectively. Opened in November 2013, the Centre is creating a benchmarking model against which states can measure their cyber security capabilities, identifying global gaps in cyber security capacity and analysing, pooling and sharing information around available and effective resources. This work will help define global priorities and support international partners to increase the scale and effectiveness of efforts against cyber threats.	A not-for-profit organisation which runs national competitions to find talented people for, and raise awareness of, job opportunities in cyber security, improving the quality of the UK cyber security talent pool for employers. Launched in 2010, over 10,000 people have registered. It is sponsored by over 50 organisations including, industry, professional bodies, the the National Cyber Security Programme, and other public sector organisations. The sponsors not only provide the financial backing for the Challenge but also design, develop and help run the competitions.
The Cyber Growth Partnership (CGP)	**Public Services Network (PSN) Security Operations Centre (SOC)**	**Working with International Organisations to promote the UK's objectives in cyberspace**	**Public Awareness**
A joint initiative with techUK, the technology industry representative body representing over 850 large and small UK technology organisations. Central to this partnership is a high level group which is identifying how to support the growth of the UK cyber security industry, with an emphasis on increasing exports.	A hub for monitoring the network, detecting anomalies and responding to incidents, supporting the ongoing transition of public sector organisations onto the PSN. The SOC will issue alerts to PSN users and provide advice on good security practice to help protect the PSN from cyber attacks. As a member of the CISP, it will also support CERT-UK.	These include the EU, Committees in the UN and the Organisation for Security and Cooperation in Europe, where the first regional Confidence Building Measures in cyberspace were agreed. A UK expert joined the UN Group of Government Experts considering international security and state behaviour in cyberspace, which agreed in 2013 that international law applies in cyberspace.	A national campaign to raise public and SME cyber security awareness will launch in January 2014, building on the work of the National Fraud Authority, BIS and Get Safe Online. This will be delivered in partnership with the private sector and will aim at increasing cyber confidence and measurably improving the online safety of consumers and small to medium enterprises.


Cyber Security Structures by Strategic Objective
• UK that is one of the most secure places in the world to do business in cyberspace
• A UK that is more resilient to cyber attack and better able to protect our interests in cyberspace
• A UK helping to shape an open vibrant and stable cyberspace that supports open societies
A UK that has the cyber skills, knowledge and capability it needs
CYBER CRIME REDUCTION PARTNERSHIP: government, law enforcement industry, academia
CERT-UK: computer emergency response for national incidents
THE NATIONAL CYBER CRIME UNIT: part of the National Crime Agency
PUBLIC SECTOR NETWORKS SECURITY OPERATIONS CENTRE: monitoring the network, responding to incidents
CYBER GROWTH PARTNERSHIP: supporting the growth of UK's cyber security industry, with Tech-UK
CYBER-SECURITY INFORMATION SHARING PARTNERSHIP (CISP): industry and Government
2011 LONDON CONFERENCE ON CYBERSPACE: initiated dialogue continued at Budapest 2012, Seoul 2013
INTERNATIONAL ORGANISATIONS: EU, UN, OSCE: fora for agreeing confidence building measures, behaviour in cyberspace
11 ACADEMIC CENTRES OF EXCELLENCE IN CYBER SECURITY RESEARCH: UK's world-class research capability
THE CYBER SECURITY CHALLENGE: improving the quality and quantity of the UK talent pool
GLOBAL CYBER SECURITY CAPACITY CENTRE: supporting International partners to build capabilities
2 CENTRES FOR DOCTORAL TRAINING: Lead to 66 PhDs
3 RESEARCH INSTITUTES: developing capability in strategically important areas of cyber security
Lead Departments / Organisations
CABINET OFFICE
FCO
HOME OFFICE
Not-for-profit org
BIS