CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Anna-Maria Osula

National Cyber Security Organisation: United Kingdom

Tallinn 2015

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre, NATO, any agency or any government. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Italy

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the USA

Upcoming in 2015

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of November 2014.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

UNITED KINGDOM

By Anna-Maria Osula
Researcher, NATO CCD COE

Table of Contents

1. Introduction: information society in the United Kingdom

1.1. Infrastructure availability and take-up

The citizens and enterprises of the UK have good access to the internet. Since 2005, 100% of the UK's population have lived in areas served by fixed broadband, and with 34.11% of total take-up of fixed broadband, the UK is ranked 6th in the EU. According to 2013 statistics, 87% of all UK households and 95% of enterprises have a broadband connection, which rank, respectively, 2nd and 11th best in the EU.[1] Similarly, mobile broadband take-up is comparatively high with 88.89 subscriptions per 100 people.

Almost 100% of the fixed broadband lines have a service quality of at least 2 Mbps while only 1% of the fixed broadband lines have 100 Mbps as a service quality. The UK leads the EU in providing a baseline internet connectivity of 2 Mbps, but has subsequently failed to keep pace with other EU members when greater broadband speeds are considered, where the UK ranks 14th and 23rd, respectively, when internet penetration is measured at speeds up to 30 Mbps and 100 Mbps.

In 2013, 88% of households had internet access at home and 87% of the individuals were regular internet users (6th in the EU). According to another study, 83% of UK's population is online,[2] and a strong majority of the internet users (93%) are very or fairly confident using the internet.[3]

1.2. E-government and private sector e-services

1.2.1. E-government

The UK has seen e-governance as a priority already since 1999, when the national goal was set to have the possibility of 'all dealings with government being deliverable electronically by 2008'.[4] In 2010, the availability of e-governance services to citizens and enterprises was close to 100%, whereas citizens' use of these services[5] has remained static since 2010 with only 48% of all individuals engaging such services. However, the use of e-government services by enterprises has reached 91% in 2013, although the UK still ranks 14th in the EU overall.

Today the UK's approach follows a concrete strategy with the end goal of all government services becoming 'digital by default', meaning that government digital services should be so 'straightforward and convenient that all those who can use them will choose to do so whilst those who can't are not excluded'.[6] One of the biggest steps in this direction has been the issuing of the Digital by Default Service Standard[7] as part of the

[1] Unless explicitly stated otherwise, the statistics in this section are taken from the EU Digital Agenda Scoreboard: EU Digital Agenda, 'Country Ranking Table, On A Thematic Group Of Indicators — Digital Agenda Scoreboard', 2014 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators>. Information in this chapter was checked for accuracy as of November 2014.

[2] For more information, read: UK Cabinet Office, *Digital Landscape Research - GOV.UK*, 2012 <https://www.gov.uk/government/publications/digital-landscape-research/digital-landscape-research>.

[3] UK Cabinet Office, *Digital Britain 2: Putting Users at the Heart of Government's Digital Services*, 2013 <http://www.nao.org.uk/wp-content/uploads/2013/07/10123-001-Digital-Britain-2-Book.pdf>.

[4] UK Cabinet Office, *Modernising Government*, 1999 <http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm>.

[5] The most popular public services in 2013 were applying for a student loan, booking a practical driving test and searching for a job through a government service. Source: *Digital Britain 2* (n 3).

[6] UK Cabinet Office, *Government Digital Strategy - GOV.UK*, 2013 <https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy>.

[7] UK Cabinet Office, *Digital by Default Service Standard — Government Service Design Manual* <https://www.gov.uk/service-manual/digital-by-default>.

Government Service Design Manual[8] that, as from April 2014, guides and facilitates the end-to-end service redesign of all transactional governmental services with over 100,000 transactions per year.[9] With the focus on saving users' time and the government's money,[10] the strategy foresees moving all 650 transactional services and information about government services onto one single platform, GOV.UK.[11]

1.2.2. E-commerce and private sector e-services

In 2013, the e-commerce indicators for individuals ordering goods or services online in UK were among the highest in the EU, as are the indicators for individuals selling online and the general turnover from e-commerce. In 2013, 82% of UK enterprises had their own website, but only 24% of the enterprises chose to send or receive e-invoices in a format suitable for automatic processing.[12]

In conclusion, it can be said that the UK has a high take up and availability of mobile and fixed broadband connection nationwide and that individuals are actively using e-commerce. However, statistical data shows that there is room for development and increased education regarding the use of e-services within and among businesses, as well as individuals using e-government services. The UK is targeting these shortcomings with nation-wide programmes and strategies, aiming at systematically rendering all Government services 'digital by default.' Also, with the estimated cost of the average cyber-security breach falling between £600,000 and £1.15m for large businesses and £65,000 and £115,000 for smaller ones, the government has strong incentives to improve protection for businesses and making the UK more resilient to cyber attacks and crime.[13]

2. Strategic national cyber security objectives

2.1. National cyber security foundation

Following the threat of cyber attacks mentioned in the National Security Strategy of 2008,[14] the UK Cabinet Office adopted its first cyber security strategy in 2009, focusing on the safety, security, and resilience in cyber space and how to positively exploit the opportunities it presents.[15]

In 2010, the UK National Security Council considered 'hostile attacks upon the UK cyber space by other states and large scale cybercrime' as one of the highest national security risks, taking into account both the likelihood and impact of possible attacks.[16] This is a higher categorisation than the threat of nuclear attack, and elevates cyber threats to the same level of risk as international terrorism, major accidents or natural hazards, and

[8] UK Cabinet Office, *Government Service Design Manual* <https://www.gov.uk/service-manual>.

[9] *Government Digital Strategy* (n 6).

[10] It is estimated 'that moving services from offline to digital channels will save between £1.7 and £1.8 billion a year.' ibid.

[11] 'GOV.UK' <https://www.gov.uk/>.

[12] ibid.; EU Digital Agenda Scoreboard (n 1) (eBusiness).

[13] UK Government, *Information security breaches survey 2014* <https://www.gov.uk/government/publications/information-security-breaches-survey-2014>.

[14] UK Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an Interdependent World* (The Stationery Office, 2008), <http://books.google.com/books?hl=en&lr=&id=Oe8E2Vkb3YQC&oi=fnd&pg=PA3&dq=%22power+blocs+has+been+replaced+by%22+%22the+connections%22+%22new+opportunities+for%22+%22the+United+Kingdom+directly.%22+%22crime,+pandemics+and+%EF%AC%82ooding%22+%22strategy,+CONTEST,%22+%22to+understand+them+better,+act+early%22+&ots=2fuVeJg41H&sig=Vjax57NGOceFzr812D0mHUX22m8>.

[15] UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (London: Stationery Office Books : [distributor] Stationery Office Books, 2009).

[16] David Cameron, Great Britain and Cabinet Office, *A Strong Britain in an Age of Uncertainty the National Security Strategy* ([Norwich]: Stationery Office, 2010) <http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf>.

international military crises.[17] The UK national security strategy underlines the influence that cyber threats exert over the day-to-day life of the government, private citizens and individuals, as access to the internet is already seen as 'woven into the fabric of our society' and 'a right rather than a privilege'.[18]

Together with the national security strategy, the UK Strategic Defence and Security Review was published putting significant emphasis on cyber security. It established a four-year National Cyber Security Programme (NCSP) that included a £650 million pool of investment[19] to strengthen the government's response to cyber threats and allocating the funds among key government entities with vital roles in cyber security.[20] In 2013, an extra £210 million investment over 2015-2016 was announced in support of the UK's continued priorities in protecting its interests in cyber space, as well as raising awareness and skills and standards.[21]

The national cyber security strategy was renewed in 2011 when the UK Cabinet Office put forward the strategic vision for UK cyber security in 2015 together with concrete objectives and necessary actions, assignment of roles and responsibilities, and main principles.[22] Namely, the strategy includes an implementation section that details the Government's way forward and the specific actions to be undertaken (some of them with firm deadlines and identified lead organisations) to reach the defined objectives.[23] The strategy also includes an obligation to report back on fulfilling the NCSP priorities in 2012[24] and a similar review was undertaken in 2013,[25] resulting in two published review documents: *Progress against the Objectives of the National Cyber Security Strategy –December 2013*[26] and *The National Cyber Security Strategy: Our Forward Plans – December 2013*[27]. The latter includes a list of core goals for 2014. The current lead Minister for cyber security is the Minister for the Cabinet Office and Paymaster General, Francis Maude MP.[28]

The national cyber security strategy is supplemented and supported by a number of other national strategies. Examples include the National Information Assurance Strategy 2007,[29] the Association of Chief Police Officers' (ACPO) e-crime Strategy 2009,[30] the National Cyber Crime Strategy 2010[31], the National Security Strategy 2010,

[17] UK House of Commons, Home Affairs Committee, *E-Crime, Fifth Report of Session 2013–14*, 2013 <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf>.

[18] *A Strong Britain in an Age of Uncertainty the National Security Strategy* (n 16).

[19] 'The £650 million has been allocated to the NCSP over the period 2011-2015, of which 14% (£90 million) has been allocated to the Ministry of Defence, and 59% to the Single Intelligence Account. (The Cabinet Office, Home Office, Business Innovation and Skills and Government ICT account for the remainder.)', read more: House of Commons and Defence Committee, *Defence and Cyber-Security: Sixth Report of Session 2012-13, Vol. 1: Report, Together with Formal Minutes, Oral and Written Evidence* (The Stationery Office, 2013), <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf>.

[20] UK Government, *Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review.* (London: HM Government, 2010) <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf>.

[21] UK Treasury, *Spending Round 2013* (London: Stationery Office, 2013).

[22] UK Cabinet Office, *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>.

[23] ibid.

[24] ibid.

[25] 'Cyber Security Strategy: Progress so Far - GOV.UK' <https://www.gov.uk/government/collections/cyber-security-strategy-progress-so-far--2>.

[26] UK Cabinet Office, *Progress Against the Objectives of the National Cyber Security Strategy - December 2013*, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265384/Progress_Against_the_Objectives_of_the_National_Cyber_Security_Strategy_December_2013.pdf>.

[27] UK Cabinet Office, *The National Cyber Security Strategy Our Forward Plans - December 2013*, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf>.

[28] 'The Rt Hon Francis Maude MP - GOV.UK' <https://www.gov.uk/government/people/francis-maude>.

[29] UK Cabinet Office, *A National Information Assurance Strategy*, 2007 <http://www.eurim.org.uk/activities/ig/idg/NationalInformationAssuranceStrategy.pdf>.

[30] Association of Chief Police Officer of England, Wales & Northern Ireland, *The ACPO e-crime strategy,* 2009 < http://www.acpo.police.uk/documents/crime/2009/200908CRIECS01.pdf>.

[31] UK Home Department, *Cyber Crime Strategy* (London: Stationery Office, 2010).

Government ICT Strategy 2011[32] and its strategic implementation plan[33] together with the 4 sub-strategies: Greening Government ICT Strategy 2011,[34] End User Device strategy 2011,[35] Government Cloud Strategy 2011,[36] ICT Capability Strategy 2011,[37] Counter Terrorism Strategy 2011,[38] MoD Information Strategy 2011,[39] Government Digital Strategy 2013,[40] National Risk Register of Civil Emergencies 2013,[41] and Serious and Organised Crime Strategy 2013.[42]

2.2. Cyber security strategy objectives

The *UK National Cyber Security Strategy 2011* puts forward a vision for the UK in 2015 'to derive huge economic and social value from a vibrant, resilient and security cyber space, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society'. One of the objectives of the UK 2011 Cyber Security Strategy is to make the UK more resilient to cyber attacks and to be better able to protect the nation's interests in cyberspace.

The strategy emphasises that the Government's powers have limits in acting in this arena, and therefore close collaboration with industry and academia is required. The strategy also includes four principal objectives:

1) 'The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace;
2) The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace
3) The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies;
4) The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives'.[43]

In 2014, the main topics under the UK cyber security policy are:

a) 'Building cyber security capacity internationally,
b) Identifying and analysing threats and strengthening our networks, [44]

[32] UK Cabinet Office, *Government ICT Strategy*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf>.

[33] UK Government, *Government ICT Strategy - Strategic Implementation Plan*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266169/govt-ict-sip.pdf>.

[34] UK Government, *Greening Government : ICT Strategy* (2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/155098/greening-government-ict-strategy.pdf>.

[35] UK Government, *Government End User Device Strategy*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/175618/government-end-user-device-strategy_0.pdf>.

[36] UK Cabinet Office, *Government Cloud Strategy*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266216/government-cloud-strategy.odt>.

[37] UK Government, *Government ICT Capability Strategy*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266328/government-ict-capability-strategy.pdf>.

[38] UK Government, *The United Kingdom's Strategy for Countering Terrorism* (Norwich: TSO, 2011).

[39] UK Ministry of Defence, *MOD Information Strategy 2011*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27388/mod_information_strat2011.pdf>.

[40] *Government Digital Strategy* (n 6).

[41] UK Cabinet Office, *National Risk Register of Civil Emergencies*, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf>.

[42] UK Government, *Serious and Organised Crime Strategy* (London: Stationery Office, 2013).

[43] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).

c) Setting up a National Cyber Crime Unit,
d) Improving cyber skills, education and professional opportunities,
e) Promoting economic growth in the cyber security sector,
f) Working with industry on minimum standards and principles,
g) Establishing a cyber security information sharing partnership, and
h) Providing cyber security advice for businesses and the public'.[45]

3. National organisational structure for cyber security and cyber defence

In the UK, the majority of organisational reforms regarding cyber security were undertaken after the adoption of the 2009 national cyber security strategy (NCSS).[46] The 2009 NCSS advocated a 'coherent approach' and created new national entities to deal with cyber security. However, later years have witnessed alterations of parts of these organisational structures, and the 2011 NCSS cautions that allocations of certain responsibilities to specific departments 'are provisional and can be adjusted if experience suggests that a different mix of inputs will produce better results'.[47] This indicates certain 'fluidity' of the governmental organisation of cyber security, where a variety of government entities function in a multi-layered and still evolving system of coordination and hierarchy. Given the Government's active role as a policy-maker and the priority of national security in the UK, the roles and responsibilities will probably be subject to further scrutiny, and additional developments are to be expected before the optimum disposition of agencies and bodies is established.[48]

For clarity, the chapter has divided the organisational structure into three work streams, even if in reality these domains may not be so easily differentiated. Principle work streams and their leading entities – Policy coordination and setting strategic priorities (Cabinet Office, OCSIA), national security intelligence (GCHQ), and cyber defence (MOD) – will be first introduced with a short summary before detailing their and other involved entities' work.

3.1. Policy coordination and setting strategic priorities

The cross-government coordination and strategic guidance over cyber security is the overall responsibility of the Cabinet Office. Cyber security is the mandate of the National Security Secretariat within the Cabinet Office which supports the National Security Council and the Prime Minister in the full range of national security issues across Government. Within the National Security Secretariat the central coordinating body for cyber security is the Office of Cyber Security & Information Assurance (OCSIA), which supports the Minister for the Cabinet Office and the National Security Council in determining priorities for securing cyberspace. The unit provides strategic direction and coordinates action relating to cyber security and information assurance in the UK, being also the owner and manager of the cross-governmental National Cyber Security Programme (NCSP). The National Security Secretariat's other entities that are dealing more specifically with the domain of national security and intelligence in the context of cyber security are described in subchapter 3.2.

Historically, ministerial responsibility and accountability for cyber security was vested in the Home Office, but was shifted to the Cabinet Office for greater clarity. The Home Office continues to deal with issues related to the use of cyber space for criminality and includes the Office for Security and Counter-Terrorism focusing on

[44] There are also many initiatives launched outside these key entities, such as the across-Government initiative to increase the security of Government's own computer networks (the new Public Sector Network). More information can be found at: *The National Cyber Security Strategy Our Forward Plans* (n 27).
[45] *Keeping the UK Safe in Cyber Space - Policy - GOV.UK.*
[46] *Cyber Security Strategy of the United Kingdom* (n 15).
[47] ibid.
[48] Julian Richards, *A Guide to National Security: Threats, Responses and Strategies*, Oxford University Press, 2012, p 112.

the terrorist-related use of cyber space. Nevertheless, concerns remain over the complex division of responsibilities given the increasing overlap of cyber security responsibilities among the numerous ministries and agencies of the Home Office, the Foreign and Commonwealth Office, and Cabinet Office.[49]

3.1.1. Office of Cyber Security and Information Assurance (OCSIA)

As noted above, OCSIA, as part of the Cabinet Office, supports both the Minister of the Cabinet Office, who also chairs the National Cyber Security Programme Board, and the National Security Council in determining national strategic priorities related to cyber security and information assurance, and has 'ownership' over the NCSP, including the allocation of funding. The unit's other tasks include: supporting education, awareness, training and education; working with private sector partners on exchanging information and promoting best practice; improving and maintaining the UK's information and cyber security technical capability and operational architecture; working with the Office of the Government Chief Information Officer (OGCIO) to ensure the resilience and security of government ICT infrastructures; and engaging with international partners in improving the security of cyberspace and information security.

OCISA works with other lead government departments and agencies such as the Home Office, Ministry of Defence (MOD), Government Communications Headquarters (GCHQ), the Communications-Electronics Security Department (CESG), the Centre for the Protection of National Infrastructure (CPNI), the Foreign & Commonwealth Office (FCO) and the Department for Business, Innovation & Skills (BIS).[50]

3.1.2. National Cyber Security Programme (NCSP)

The idea of a cross-government cyber security programme introduced in 2009[51] was further outlined in the National Defence and Security Review 2010 that established the NCSP, a four-year investment programme providing additional funding to the UK's cyber security and defence entities. The NCSP established a number of new cyber security agencies and listed several initiatives to be undertaken in close cooperation with the private sector, focusing on:

a) Overhauling the UK's approach to tackling cybercrime, creating a single point of contact for the public and private sector to report cybercrime;

b) Addressing deficiencies in detecting and defending against cyber attacks, including, as the basis of the UK's activities in cyber space, improving the ability to deliver cyber products and services and enhancing investments in national intelligence capabilities.

c) Streamlining the Ministry of Defence's cyber security, including the integration of cyber activities across the spectrum of defence operations under a newly created Defence Cyber Operations Group;

d) Addressing shortcomings in the critical cyber infrastructure, ensuring online public services are secure and giving support to key UK industries and those critical networks owned and operated by the private sector;

e) Sponsoring long term security research, improving education and skills, and working closely with the private sector and academic partners to maintain excellence and raise awareness;

f) Continuing to build cyber security alliances (including a comprehensive UK-US Memorandum of Understanding for enabling the countries to share information and plan and conduct operations

[49] E.g. on the issues of oversight over the GCHQ, UK Intelligence and Security Committee, *Intelligence and Security Committee Annual Report 2011-2012*. (London: Stationery Office, 2012), quoting 'Oral Evidence – Foreign Secretary, 26 January 2012'.
[50] UK Cabinet Office,*Office of Cyber Security and Information Assurance* <https://www.gov.uk/government/policy-teams/office-of-cyber-security-and-information-assurance>.
[51] *Cyber Security Strategy of the United Kingdom* (n 15).

jointly) to ensure capacity building with partners and shape international political and technical standards.[52]

All of these activities were brought together and further outlined in the 2011 NCSS that also introduced the NCSP's investment for 2011 to 2015. The NCSP funding is clearly steered towards intelligence and information assurance (59%), while the rest is divided by Home Office/Cyber Crime (10%), Government ICT/online services (10%), MoD (14%), Cabinet Office/coordination an operational threat (5%) and Department for Business, Innovation and Skills/working with the private sector (2%).[53]

3.2. National security and intelligence

The National Security Secretariat (NCS) is within the Cabinet Office, responsible for coordination on security and intelligence issues of strategic importance across government, including cyber security. As part of the NCS, the Joint Intelligence Organisation produces independent all-source assessments on issues of national security and foreign policy importance. While supporting the work of the National Security Council and the Joint Intelligence Committee respectively, these entities provide advice to the Prime Minister and other senior ministers.[54]

Under the umbrella of and in close cooperation with the NCSP, intelligence agencies have a prominent role in tackling cyber threats.[55] Government Communications Headquarters (GCHQ) is central to this effort, offering or hosting strategic analyses of the threats, operational CS capabilities and cyber incident management. GCHQ and its supporting entities are outlined below.

3.2.1. Government Communications Headquarters (GCHQ)

Central to national security and intelligence efforts is GCHQ, with approximately 5300 staff[56] at Cheltenham; it receives over half of the NCSP's estimated £650 million budget in order to enhance the UK's capabilities in detecting and countering cyber attacks.[57] GCHQ works in close cooperation with the National Security Council, UK Armed Forces serving abroad, and with partners in the intelligence community, Security Service (MI5), Secret Intelligence Service (MI6) and other government departments.[58] GCHQ also hosts the MOD's Joint Cyber Unit (Cheltenham) (see subsection 3.3.1.1.).

Nearly all of GCHQ's work has a cyber-related element and the organisation's claim to the lion's share of NCSP funding has helped GCHQ develop a number of cyber security projects: expanding its work on protective cyber security advice and information assurance; improving detection and analysis of cyber attacks (including cybercrime); strengthening intelligence operations in cyberspace; as well as improving co-operation with international allies and partners.[59]

As part of GCHQ, the Cyber Defence Operations team – formerly the Network Defence Intelligence and Security Team – has significantly improved the UK's protective coverage from cyber attacks through increased detection

[52] *Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review* (n 20).
[53] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[54] *National Security and Intelligence - GOV.UK* <https://www.gov.uk/government/organisations/national-security>. However, it must be noted, that the relationship between these entities seems not to be clear cut either, as suggested by a study that looked at maximising the effectiveness of the central national security and intelligence structures. *See* UK Government, *Supporting the National Security Council (NSC): The central national security and intelligence machinery* <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61948/Recommendations_Suppporting_20the_20National_20Security_20Council_The_20central_20national_20security_20and_20intelligence_20machinery.pdf>>.
[55] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[56] Figure as of March 2011. *Intelligence and Security Committee Annual Report 2011-2012* (n 49).
UK Government, Cabinet Office.
[57] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[58] 'GCHQ Webpage' <http://www.gchq.gov.uk/who_we_are/Pages/Welcome-to-GCHQ.aspx>.
[59] *Intelligence and Security Committee Annual Report 2011-2012* (n 49).

and analysis, leading to a better understanding of the vulnerabilities being exploited, while attributing attacks to their source has helped develop counter-measures and, in turn, improved the efficacy of security advice offered by CESG and others.[60] Between 2009 and 2011, the number of GCHQ staff employed in the field of network defence and analysis of cyber attacks increased by almost one-third.[61]

Other agencies have also gone through reforms in order to better tackle the threats posed by and within the cyber space. For example, MI5 has decided to 'merge its work on counter-espionage, counter-intelligence, counter-proliferation, cyber and protective security into a new branch' with the aim of tackling the threat from foreign states[62] even though it is suggested that the majority of cyber attacks continue to be criminal.[63] In addition, 'its protective security work has been broadened beyond the Critical National Infrastructure to include other priority areas of the UK private sector.'[64]

3.2.1.1. Cyber Security Operations Centre (CSOC)

The Cyber Security Operations Centre (CSOC) was created to monitor and co-ordinate incident response and share with businesses and the public information and advice on attacks against UK networks and users.[65] The centre is a multi-agency body that consists of representatives of the government and key stakeholders, and reports to an inter-departmental oversight board. It is hosted by GCHQ in Cheltenham that allows the centre to be in close cooperation with the GCHQ's Information Assurance arm – the National Technical Authority for Information Assurance (CESG, formerly the Communications-Electronics Security Group).[66] The centre is likely to be stood down once the CERT UK and Centre for Cyber Assessments are established.[67]

3.2.1.2. National Technical Authority for Information Assurance (CESG)

CESG GCHQ's Information Assurance arm, is also based in Cheltenham. It is one of the principal players in technical aspects of information security in government, focusing on the 'defence, or security, of computers and networks: ensuring that the barriers against cyber attacks are strong, that vulnerabilities are reduced and that networks are monitored so that attacks can be spotted'.[68] CESG's multiple activities are carried out in partnership with industry and academia, as well as using insights into threats from the work of our colleagues in the Centre for Protection of National Infrastructure (CPNI), MI5 and Secret Intelligence Service (MI6).[69]

3.2.1.3. Computer Emergency Response Team (CERT-UK)

CESG will also be running the Computer Emergency Response Team (CERT-UK), operational since 2014, catering to the public sector organisations by providing warnings, alerts and assistance in resolving serious IT incidents.[70] The design for the new organisation for national cyber incident management has been agreed and the entity is planned to work closely with the government, industry, academic and international partners to co-

[60] *Intelligence and Security Committee Annual Report 2011-2012* (n 49).
[61] ibid.
[62] UK Intelligence and Security Committee, *Intelligence and Security Committee of Parliament Annual Report 2012-2013*, quoting the 'Letter from the Security Service, 4 December 2012.'
[63] Intelligence and Security Committee of Parliament Annual Report 2012-2013 (n 62).
[64] *Intelligence and Security Committee Annual Report 2011-2012* (n 49).
[65] *Cyber Security Strategy of the United Kingdom* (n 15).
[66] ibid.
[67] UK Ministry of Defence, *Cyber Primer*, 2013, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf>.
[68] *Intelligence and Security Committee Annual Report 2011-2012* (n 49).
[69] National Technical Authority for Information Assurance (CESG) website, <http://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx>.
[70] GovCertUK Webpage <http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx>.

ordinate responses to cyber incidents in the UK and internationally.[71] In addition, CERT-UK will deliver an expanded exercise programme in an effort to test the preparedness of critical information infrastructure against the potential impact of a destructive cyber attack.[72] It will also provide a permanent home for the Cyber Security Information Sharing Partnership (CISP) team and taking on responsibility for running the dedicated CISP online collaboration environment.[73]

CISP was launched in March 2013[74] and is one of the principal UK mechanisms for reaching out to the private sector regarding cyber threats and effective risk management practices. Following these goals, the collaborative environment allows members of the CISP community to exchange cyber threat information in real time and receive enriched, contextually relevant cyber threat information and advice from the Fusion Cell, which is comprised of government and industry network defence analysts. Despite its short history, the CISP already involves over 250 large firms and major organisations; the 2014 target is to raise this number to 500 by the end of the year.[75]

CISP has also been employed in government cyber security exercises. During 2012 and 2013, the UK Government held 10 exercises, working with industrial partners and government departments as well as agencies, to test cyber resilience and response in key sectors including finance, law enforcement, transport, food and water.[76] For instance, the 'Waking Shark II' exercise tested cyber defence and incident handling in the banking sector. [77] The CISP platform played an integral role in the exercise, enabling participants to share 'real-time' threat information during the development of the scenario.[78]

3.3. Military cyber defence

The workstream of military cyber defence is run by the UK Ministry of Defence (MOD) that deals with the military use of cyber space, including defence policy and doctrine. Since the UK does not have a specific cyber defence strategy and neither the 2011 National Strategy for Defence[79] nor the MOD Defence Plan 2010-2014[80] explicitly mention cyber as a priority or a threat, MOD's cyber policy follows the guiding principles of the UK Cyber Security Strategy and is, where appropriate, co-ordinated with OCSIA and Other Government Departments (OGDs) to ensure harmonious departmental approaches.[81]

3.3.1. Ministry of Defence (MOD)

MOD's guidance in cyber defence derives from the Strategic Defence and Security Review 2010 (SDSR) that stated that a UK Defence cyber capability would be established as part of the transformative cross-government approach. SDSR tasked the MOD to 'provide a cadre of experts to support our own and allied cyber operations to secure our vital networks and to guide the development of new cyber capabilities'.[82] The 2011 UK Cyber

[71] *Progress Against the Objectives of the National Cyber Security Strategy* (n 26).
[72] *The National Cyber Security Strategy Our Forward Plans* (n 27).
[73] CISP, CERT-UK webpage <https://www.cert.gov.uk/cisp/>.
[74] 'Cyber Security Information Sharing Partnership - Speeches - GOV.UK' <https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme>.
[75] *The National Cyber Security Strategy Our Forward Plans* (n 27).
[76] *Progress Against the Objectives of the National Cyber Security Strategy* (n 26).
[77] Bank of England, *Publications | News Releases | News Release - Bank of England Publishes Report into Cyber-Resilience Exercise* <http://www.bankofengland.co.uk/publications/Pages/news/2014/030.aspx>.
[78] *Progress Against the Objectives of the National Cyber Security Strategy* (n 26).
[79] UK Ministry of Defence, *The Strategy for Defence*, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27398/stategy_for_defence_oct2011.pdf>.
[80] UK Ministry of Defence, *Defence Plan 2010-2014*, 2010 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27163/Defence_Plan_2010_2014.pdf>.
[81] UK House of Commons Defence Committee, *Defence and Cyber-Security*, *Written Evidence*, 2012, <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/1881.pdf>.
[82] *Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review* (n 20).

Security Strategy identified MOD as the government lead for 'ensuring that the UK has the capability to protect our interests in cyberspace [by] improving our ability to detect threats in cyberspace [and] expanding our capability to deter and disrupt attacks on the UK', and assigned from April 2012 the newly created Joint Forces Command as the lead for the development and integration of defence cyber capabilities.[83]

In order to make sure that the MOD meets the priorities set out by Government, it has formulated the classified Defence Strategic Direction (2011) from the SDSR 2010 as a guideline for the annual defence planning and resource allocation, while concurrently working closely with the National Security Council and the Cabinet Office.[84] Since the internal structure and division of responsibilities for cyber security in the MOD and the Armed Forces have been a target of critique by the UK Parliament, the MOD has aimed to clarify the lines of command and control more clearly.[85]

Finally, it needs to be underlined that the MoD has no jurisdiction to develop policy or otherwise related to the protection of Critical National Infrastructure, and only maintains an advisory role to the official competencies of the CPNI, OGAs and Agencies.[86]

3.3.2. Armed Forces

The UK Armed Forces envision cyber as a 'joint field issue across the entirety of Defence … that must be integrated within all areas of planning, preparation and budgeting' and to that end, the Chief of Defence Staff has decided to bring together 'all the operational command of Cyber units under Joint Forces Command to ensure a consistent and holistic approach to Cyber in operations and Defence business'.[87]

According to the Defence and Cyber Security report, the Minister for the Armed Forces will act as a focal point for delivery of this objective, and the funding allocated from the NCSP (£90 million) will be used by the Defence Cyber Security Programme (DCSP) to 'improve the broader transformation as to how the MoD approaches cyber operations'.[88] The DCSP is divided to four major work streams, being supported by a number of cross cutting activities[89], and led at two-star level within Defence:

> 'a) Mainstreaming Cyber – which seeks to establish cyber operations as part of the mainstream of departmental planning and operations; backed by appropriate training, education and awareness.
> b) Defence Cyber Operations Group (DCOG) – which considers the role, structure and organisation of the DCOG; together with the specialist skills and training required for personnel within the group (see subchapter 3.3.1.2.).
> c) Cyber Capability – which builds the necessary capabilities to undertake cyber operations.
> d) Cyber Future Force – which designs the cyber component of the Future Force 2020 providing the longer term vision backed by a programme of experimentation and development.'[90]

After the depletion of the DCSP, much of the defensive work will continue within the Defence Cyber Programme (DCP) which will 'deliver coherent defensive workstreams within the MOD'.[91]

[83] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[84] *Defence and Cyber-Security, Written Evidence* (n 81).
[85] UK House of Commons Defence Committee, *House of Commons - Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13 - Defence Committee*, 2013 <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm>.
[86] ibid.
[87] ibid.
[88] *Defence and Cyber-Security, Written Evidence* (n 81).
[89] 'Including programme governance and management, cross OGD working, and engagement with Allies', read more at: *Defence and Cyber-Security, Written Evidence* (n 81).
[90] ibid.

According to the Intelligence and Security Committee 2013 report, the MOD has developed a 'joint doctrine on cyber operations, which sets out how cyber activities integrate into military operations and the legal framework within which they could be used'.[92] As of January 2013, the MOD has appointed Commander of Joint Forces Command (JFC) as the Defence Authority for Cyber to develop and maintain the department's cyber capability, as well as plan and prepare for all cyber operations. On a day-to-day basis this authority is delegated to Chief of Defence Intelligence (CDI), although 'Head Office is still responsible for formulating cyber policy, delivered through the Deputy Chief of Defence Staff for Military Strategy and Operations (DCDS (MSO)).[93] CDI, on behalf of the Commander of JFC, "commands all cyber operations, with cyber defence delivered by the Information Systems and Services (ISS) organisation'[94] Command and control within the cyber domain will be outlined further by the soon to be adopted Chief of the Defence Staff Directive on Cyber.[95]

The Senior Responsible Owner (SRO) of the Defence Cyber Security Programme (DCSP) has also been appointed and this post is responsible for ensuring the success of the programme in its stated aims and objectives.[96] Furthermore, it is the intent of Commander JFC to set up a Joint Forces Cyber Group (JFCyG) to oversee the operational function of the Joint Cyber Units, Joint Information Assurance Units and the Cyber Reserve, believing that 'this line of Command and Control gives /…/ the necessary chain of command, while retaining the flexibility and agility required to deal with the threats and opportunities emanating from cyber.'[97] The JFCyG also 'heralds the formation of specialist units in cyberspace for MOD, frequently using existing resources and to be centrally managed in consultation with single-Services and civilian manning agencies.[98] Despite these developments, the UK House of Commons Security and Defence Committee has residual concerns about the clarity over which individual command responsibilities are extended to the MOD's part of the spectrum.[99]

The UK has openly discussed the existence of two Joint Cyber Units. The Joint Cyber Unit (Corsham) aims to proactively and reactively defend MoD networks 24/7 against cyber attacks, whereas the Joint Cyber Unit (Cheltenham), hosted by GCHQ, will reach full operational capability by 2015 and 'will have the role of developing new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace.'[100]

In 2013, the MOD has announced the creation of the Joint Cyber Reserve, which initiated a large-scale recruitment campaign directed at attracting the UK's cyber professionals in a reserve capacity to bolster the cyber capability of the regular UK armed forces.[101] The reservists[102] provide support to the Joint Cyber Unit (Corsham), the Joint Cyber Unit (Cheltenham) and the tri-service information assurance units located across the MOD, and are part of the defence budget's increasing investment in high-end capabilities such as cyber, intelligence, and surveillance assets.[103]

[91] *Cyber Primer* (n 67).
[92] Intelligence and Security Committee of Parliament Annual Report 2012-2013 (n 62).
[93] UK Ministry of Defence, *How Defence Works*, version 4.1 30 September 2014, available at. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360143/20140930_24153_How_Defence_Works.pdf>.
[94] ibid.
[95] Intelligence and Security Committee of Parliament Annual Report 2012-2013 (n 62).
[96] ibid.
[97] *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).
[98] *Cyber Primer* (n 67).
[99] UK House of Commons Defence Committee, *Defence and Cyber-Security Commons Debate on 4 Mar 2014*, 2014 <http://www.theyworkforyou.com>.
[100] UK Ministry of Defence, *Supplementary Written Evidence from the Ministry of Defence* <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm>.
[101] UK Ministry of Defence and Joint Forces Command, *New Cyber Reserve Unit Created - News Stories - GOV.UK*' <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit>.
[102] See more on recruitment: *Working for JFC - Joint Forces Command - GOV.UK* <https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment>.
[103] UK Ministry of Defence and Joint Forces Command.

The 2013 initiative 'Defence Cyber Protection Partnership' (DCPP), uniting CPNI, MOD and nine companies, supplements the current cyber defence efforts by tackling the emerging threat to the 'UK defence supply chain by increasing awareness of cyber risks, sharing threat intelligence, and defining risk-driven approaches to applying cyber security standards'.[104] Nevertheless, the security of the MOD's supply chain and industrial base have been recently questioned, especially concerning the lack of clarity on 'efforts to improve the technical processes involved, identification of adequate resources, and provision of training to address the human aspects of good cyber defence'.[105] The MOD is committed to solving these issues.[106]

In addition to the priority of being able to defend the UK against attacks in cyber space, the Intelligence and Security Committee has concluded that 'there are also significant opportunities which should be exploited in the interests of UK national security' such as 'active defence; exploitation; disruption; information operations; and military effects', adding that they must, however, 'be closely linked to cyber 'defence' [where] the lessons learned from one can feed into planning for the other'.[107]

One of the avenues of enhancing the military capabilities of the UK Armed Forces is seen as being through international cooperation.[108] To that end, there is a tri-lateral Memorandum of Understanding in place with the UK's close allies the USA and Australia with the aim to work collaboratively on cyber, 'drawing from each other's specific experiences and allowing each nation to draw on best practices'.[109]

3.3.3. Defence Cyber Operations Group (DCOG)

With the goal to transform the UK's cyber capabilities and becoming more flexible, advanced, and suitable for the battlespace, the UK Defence Cyber Operations Group (DCOG) was established as a major part of the DCSP, and is planned to become fully operational by March 2015.[110] As part of the transformative cross-government approach, the DCOG 'will provide a cadre of experts to support our own and allied cyber operations to secure our vital networks and to guide the development of new cyber capabilities' as well as 'bring together existing expertise from across Defence, including the Armed Forces and our science and technology community'.[111] The DCOG aims to 'provide Defence with a significantly more focused approach to cyber',[112] ensuring that the UK will 'plan, train, exercise and operate in a way which integrates our activities in both cyber and physical space' and is responsible for 'developing, testing and validating cyber capabilities as a complement to traditional military capabilities'.[113] Consequently, the DCOG will work closely with other government departments, industry and international partners.[114] The DCOG is 'a federation of the cyber units across defence',[115] and will include the Joint Cyber Unit hosted by GCHQ at Cheltenham[116] as well as the GOSCC and presumably its attached Joint Cyber Unit at Corsham.[117]

The UK Parliament has criticised the initiative claiming that the 'unifying role of the DCOG is more illusory than real' and there is an overlap of the tasks of GOSCC and Information Services and Systems, asking for further

[104] *Defence Partnership Tackles Cyber Security Risks - News Stories - GOV.UK* <https://www.gov.uk/government/news/defence-partnership-tackles-cyber-security-risks>.
[105] UK House of Commons Defence Committee, *House of Commons - Defence and Cyber-Security - Defence Committee; 2 MoD Networks, Assets and Capabilities*, 2013 <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm>.
[106] *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).
[107] Intelligence and Security Committee of Parliament Annual Report 2012-2013 (n 62).
[108] *Defence and Cyber-Security, 2 MoD Networks, Assets and Capabilities* (n 105).
[109] *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).
[110] *Supplementary Written Evidence from the Ministry of Defence* (n 100).
[111] *Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review* (n 20).
[112] *Defence and Cyber-Security, Written Evidence* (n 81) 3.
[113] *Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review* (n 20).
[114] ibid.
[115] *Supplementary Written Evidence from the Ministry of Defence* (n 100).
[116] *Defence and Cyber-Security, Written Evidence* (n 81) 3.
[117] *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).

clarification of the roles of Chief Information Officer and the Joint Forces Commander.[118] The Government has clarified that 'the recent agreement of the Defence Board to establish a 3* Defence Chief Information Officer (CIO) will strengthen and centralise the Department's leadership and accountability for information systems in both the military and business environments' and that Information Operating Model together with the creation of additional cyber specific posts will facilitate progress in the management and delivery of ICT.[119]

3.3.4. Global Operations and Security Control Centre (GOSCC)

Comprehensive management and cyber defence for all the UK Armed Forces' and MOD's communications networks including theatre networks, is provided by the new Global Operations and Security Control Centre (GOSCC), located at MOD Corsham.[120] GOSCC operates around the clock and monitors over 200,000 devices across defence networks worldwide, ready to provide an immediate response and to function as incident command and co-ordination.[121] The centre has also the capabilities to undertake forensic analysis of the attacks and 'give possible indications of future vulnerabilities, attack vectors, and as best as can be done—attribution of source'.[122] In addition, the centre will make use of the Joint Cyber Unit (Cheltenham) that is embedded within the GOSCC and 'develop and use a range of new techniques, including proactive measures, to disrupt threats to … information security.'[123] Around 200 people work in the GOSCC, a mix of military, MoD civilian and contractor personnel from major industry partners.[124]

3.4. Resilience of critical national infrastructure

Approximately 80% of the UK's critical national infrastructure (CNI) is privately owned. The UK does not have a single policy or an act of Parliament to deal with CNI. There exists specific legislation for different CNI sectors, but it is fragmented, rather than following a common approach. Even though the government is the lead regulator and policy-maker of the CNI security,[125] it is the private entities who own the UK's CNI that are responsible for financing and putting into action selective measures, leaving the government without a direct operational security role or cost.[126] The full list of CNI sites is confidential.

Under the Trustworthy Cyber CNI research initiative, the government has been improving its understanding of the key technological dependencies that underpin the UK's critical national infrastructure.[127] Two Cyber Incident Response (CIR) schemes were launched in August 2013 by GCHQ and CPNI.[128] The government confirms the existence of a clear set of National Incident Management procedures which are regularly exercised, including with Ministerial participation.[129] Regarding a possible attack against the MOD's and the Armed Forces' networks, assets and capabilities, the Government states that there are a 'number of business continuity and contingency plans to ensure … [being] able to continue to fulfil our role, should any number or combination of events occur' are planned and exercised, and that '[cyber] is being integrated fully into /…/

[118] *Defence and Cyber-Security, 2 MoD Networks, Assets and Capabilities* (n 105).
[119] *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).
[120] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[121] *Defence and Cyber-Security, Written Evidence* (n 81) 4.
[122] ibid.
[123] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[124] *Supplementary Written Evidence from the Ministry of Defence* (n 100).
[125] Responsibility for the CPNI policy remains with Other Governmental Agencies and Agencies. Stated in: *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).
[126] Alex Carmichael, *UK Critical National Infrastructure* <http://www.coess.eu/_Uploads/dbsAttachedFiles/Intervention_Alex_Carmichael.pdf>.
[127] *Progress Against the Objectives of the National Cyber Security Strategy* (n 26).
[128] ibid.
[129] *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13* (n 85).

contingency operation planning process'.[130] However, no further information on this or contingency plans for CNI are publicly available.

As a parallel initiative, the UK Government monitors the most significant emergencies that the United Kingdom and its citizens could face through the confidential National Risk Assessment (NRA). This assessment is supplemented by the publicly available report 'National Risk Register of Civil Emergencies 2013'[131] that reflects the latest iteration of the National Risk Assessment,[132] which includes 'cyber attacks against infrastructure' and 'cyber attacks resulting in the breach of data confidentiality' as possible examples of malicious attacks.

There are also examples of initiatives aimed at raising awareness on cyber threats across different essential services, such as a recent summit bringing together regulators from the financial, water, energy, communications and transport sectors with ministers and senior officials from the security and intelligence agencies to discuss cooperation and partnership opportunities aimed at addressing cyber threats to critical infrastructure.[133] The subsequent joint communique[134] expressed the agreement on undertaking further activities in that regard, such as:[135]

a) exercises to test procedures and resilience;
b) the adoption of security standards[136] and auditing against best practice (e.g. Ten Steps to Cyber Security); and[137]
c) information sharing through initiatives such as the CISP (Cyber Security Information Sharing Partnership).

UK governmental entities are also looking into the possible risks related to the foreign involvement in the Critical National Infrastructure and the implications for national security concluding that the 'National Security Council should ensure that there are effective procedures and powers in place, and clear lines of responsibility when it comes to investment in the CNI'.[138]

3.4.1. Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI), created in 2007, facilitates public-private partnership efforts in the UK as the central governmental body working directly with the network of key industries and companies that own much of the state's critical infrastructure. CPNI provides security advice on 'physical security, personnel security and cyber security/information assurance'[139] and aims to reduce the

[130] ibid.
[131] *National Risk Register of Civil Emergencies* (n 41).
[132] *CPNI in Context* <http://www.cpni.gov.uk/about/context/>.
[133] *Government and Regulators Meet to Combat Cyber Threats to Essential Services - Press Releases - GOV.UK* <https://www.gov.uk/government/news/government-and-regulators-meet-to-combat-cyber-threats-to-essential-services>.
[134] UK Government, *Joint Communique from the 'Strengthening the Cyber Security of Our Essential Services* Event' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284085/Communique_-_Strengthening_the_Cyber_Security_of_Our_Essential_Services.pdf>.
[135] *Government and Regulators Meet to Combat Cyber Threats to Essential Services* (n 133).
[136] An example of such an initiative is: UK Department for Business, Innovation and Skills, *Cyber Security Organisational Standards, A Call for Views and Evidence*, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf>.
[137] For this and other materials on UK guidance for business, see: *Cyber Security Guidance for Business - Publications - GOV.UK* <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility>.
[138] UK Intelligence and Security Committee, *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security* (London: Stationery Office, 2013). See also the *Huawei Cyber Security Evaluation Centre: Review by the National Security Adviser*, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266487/HCSEC_Review_Executive_Summary_FINAL.PDF>.
[139] *About CPNI* <http://www.cpni.gov.uk/about/>.

vulnerability of national infrastructure to terrorism and other threats such as espionage, including threats deriving from cyberspace.[140]

CPNI prioritises to whom the organisation gives advice through various mechanisms such as a 'sector approach for national infrastructure, a criticality scale and CONTEST Protect's seven current themes for counter terrorism.'[141] CPNI has also been developing new cyber security awareness training courses for senior managers and engineers, to be launched in 2014.[142]

3.4.2. Department for Business Innovation and Skills

The Department for Business Innovation and Skills (BIS) focuses on industrial and economic policy, and regulatory policy, particularly in the telecommunications sector[143] and includes a new Cyber Infrastructure Team providing strategic leadership and regulatory oversight.[144] Other interesting BIS initiatives include developing an 'industry-led organisational standard for cyber security'[145] and running the 'Cyber Governance Health Check' programme that offers significant insight into the cyber governance of the UK's highest-performing businesses.[146]

[140] *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (n 22).
[141] About CPNI (n 139).
[142] *Progress Against the Objectives of the National Cyber Security Strategy* (n 26).
[143] 'Department for Business, Innovation & Skills - GOV.UK' <https://www.gov.uk/government/organisations/department-for-business-innovation-skills>.
[144] *Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review* (n 20).
[145] *The National Cyber Security Strategy Our Forward Plans* (n 27).
[146] UK Home Department, FTSE 350 Cyber Governance Health Check Tracker Report, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf>.

References

‘About CPNI’ <http://www.cpni.gov.uk/about/>.

‘Bank of England | Publications | News Releases | News Release - Bank of England Publishes Report into Cyber-Resilience Exercise’ <http://www.bankofengland.co.uk/publications/Pages/news/2014/030.aspx>.

‘Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard, Broadband - Mobile (supply and Take-Up), UK’ <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={%22indicator-group%22:%22mobile%22,%22ref-area%22:%22UK%22,%22time-period%22:%222013%22}>.

‘CPNI in Context’ <http://www.cpni.gov.uk/about/context/>.

‘Cyber Security Guidance for Business - Publications - GOV.UK’ <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility>.

‘Cyber Security Information Sharing Partnership - Speeches - GOV.UK’ <https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme>.

‘Cyber Security Strategy: Progress so Far - GOV.UK’ <https://www.gov.uk/government/collections/cyber-security-strategy-progress-so-far--2>.

‘Defence Partnership Tackles Cyber Security Risks - News Stories - GOV.UK’ <https://www.gov.uk/government/news/defence-partnership-tackles-cyber-security-risks>.

‘Department for Business, Innovation & Skills - GOV.UK’ <https://www.gov.uk/government/organisations/department-for-business-innovation-skills>.

‘Digital by Default Service Standard — Government Service Design Manual’ <https://www.gov.uk/service-manual/digital-by-default>.

‘GCHQ Webpage’ <http://www.gchq.gov.uk/who_we_are/Pages/Welcome-to-GCHQ.aspx>.

‘GOV.UK’ <https://www.gov.uk/>.

‘GovCertUK Webpage’ <http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx>.

‘Government and Regulators Meet to Combat Cyber Threats to Essential Services - Press Releases - GOV.UK’ <https://www.gov.uk/government/news/government-and-regulators-meet-to-combat-cyber-threats-to-essential-services>.

‘Government Service Design Manual’ <https://www.gov.uk/service-manual>.

‘Information security breaches survey 2014‘ <https://www.gov.uk/government/publications/information-security-breaches-survey-2014>.

‘National Security and Intelligence - GOV.UK’ <https://www.gov.uk/government/organisations/national-security>.

‘The Rt Hon Francis Maude MP - GOV.UK’ <https://www.gov.uk/government/people/francis-maude>.

‘Working for JFC - Joint Forces Command - GOV.UK’ <https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment>.

Alex Carmichael, ‘UK Critical National Infrastructure’ <http://www.coess.eu/_Uploads/dbsAttachedFiles/Intervention_Alex_Carmichael.pdf>.

Association of Chief Police Officer of England, Wales & Northern Ireland, The ACPO e-crime strategy, 2009 < http://www.acpo.police.uk/documents/crime/2009/200908CRIECS01.pdf>.

CISP, CERT-UK webpage <https://www.cert.gov.uk/cisp/>.

David Cameron, Great Britain and Cabinet Office, A Strong Britain in an Age of Uncertainty the National Security Strategy ([Norwich]: Stationery Office, 2010) <http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf>.

European Commission, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard, Broadbands (Supply and Take-Up), UK', 2013 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={%22indicator-group%22:%22broadband%22,%22ref-area%22:%22UK%22,%22time-period%22:%222013%22}>.

European Commission, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard, eGovernment, UK' <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={%22indicator-group%22:%22egovernment%22,%22ref-area%22:%22UK%22,%22time-period%22:%222013%22}>.

European Commission, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard, eCommerce, UK' <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={%22indicator-group%22:%22ecommerce%22,%22ref-area%22:%22UK%22,%22time-period%22:%222013%22}>.

European Commission, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard, eBusiness, UK' <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={%22indicator-group%22:%22ebusiness%22,%22ref-area%22:%22UK%22,%22time-period%22:%222013%22}>.

Evaluation Centre: Review by the National Security Adviser, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266487/HCSEC_Review_Executive_Summary_FINAL.PDF>.

House of Commons and Defence Committee, Defence and Cyber-Security: Sixth Report of Session 2012-13, Vol. 1: Report, Together with Formal Minutes, Oral and Written Evidence (The Stationery Office, 2013), <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf>.

Julian Richards, *A Guide to National Security: Threats, Responses and Strategies*, Oxford University Press, 2012.

'Keeping The UK Safe In Cyber Space - Policy - GOV.UK', 2013 <https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace>.

UK Cabinet Office, 'Digital Britain 2: Putting Users at the Heart of Government's Digital Services', 2013 <http://www.nao.org.uk/wp-content/uploads/2013/07/10123-001-Digital-Britain-2-Book.pdf>.

UK Cabinet Office, 'Office of Cyber Security and Information Assurance' <https://www.gov.uk/government/policy-teams/office-of-cyber-security-and-information-assurance>.

UK Cabinet Office, 'The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World', 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>.

UK Cabinet Office, A National Information Assurance Strategy, 2007 <http://www.eurim.org.uk/activities/ig/idg/NationalInformationAssuranceStrategy.pdf>.

UK Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space (Stationery Office Books 2009).

UK Cabinet Office, Digital Landscape Research - GOV.UK, 2012 <https://www.gov.uk/government/publications/digital-landscape-research/digital-landscape-research>.

UK Cabinet Office, Government Cloud Strategy, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266216/government-cloud-strategy.odt>.

UK Cabinet Office, Government Digital Strategy - GOV.UK, 2013 <https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy>.

UK Cabinet Office, Government ICT Strategy, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf>.

UK Cabinet Office, Modernising Government, 1999 <http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm>.

UK Cabinet Office, National Risk Register of Civil Emergencies, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf>.

UK Cabinet Office, Progress Against the Objectives of the National Cyber Security Strategy - December 2013, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265384/Progress_Against_the_Objectives_of_the_National_Cyber_Security_Strategy_December_2013.pdf>.

UK Cabinet Office, The National Cyber Security Strategy Our Forward Plans - December 2013, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf>.

UK Cabinet Office, The National Security Strategy of the United Kingdom: Security in an Interdependent World (The Stationery Office, 2008), <http://books.google.com/books?hl=en&lr=&id=Oe8E2Vkb3YQC&oi=fnd&pg=PA3&dq=%22power+blocs+has+been+replaced+by%22+%22the+connections%22+%22new+opportunities+for%22+%22the+United+Kingdom+directly.%22+%22crime,+pandemics+and+%EF%AC%82ooding%22+%22strategy,+CONTEST,%22+%22to+understand+them+better,+act+early%22+&ots=2fuVeJg41H&sig=Vjax57NGOceFzr812D0mHUX22m8>.

UK Department for Business, Innovation and Skills, ‘Cyber Security Organisational Standards, A Call for Views and Evidence’, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf>.

UK Government, ‘Joint Communique from the ‘Strengthening the Cyber Security of Our Essential Services’ Event’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284085/Communique_-_Strengthening_the_Cyber_Security_of_Our_Essential_Services.pdf>.

UK Government, A Strong Britain in an Age of Uncertainty the National Security Strategy.

UK Government, Government End User Device Strategy, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/175618/government-end-user-device-strategy_0.pdf>.

UK Government, Government ICT Capability Strategy, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266328/government-ict-capability-strategy.pdf>.

UK Government, Government ICT Strategy - Strategic Implementation Plan, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266169/govt-ict-sip.pdf>.

UK Government, Greening Government : ICT Strategy (2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/155098/greening-government-ict-strategy.pdf>.

UK Government, Securing Britain in an Age of Uncertainty the Strategic Defence and Security Review. (London: HM Government, 2010) <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf>.

UK Government, Serious and Organised Crime Strategy (London: Stationery Office, 2013).

UK Government, Supporting the National Security Council (NSC): The central national security and intelligence machinery <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61948/Recommendations_Suppporting_20the_20National_20Security_20Council_The_20central_20national_20security_20and_20intelligence_20machinery.pdf>.

UK Government, The United Kingdom's Strategy for Countering Terrorism (Norwich: TSO, 2011).

UK Home Department, Cyber Crime Strategy (London: Stationery Office, 2010).

UK Home Department, FTSE 350 Cyber Governance Health Check Tracker Report, 2013 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf>.

UK House of Commons Defence Committee, 'Defence and Cyber-Security Commons Debate on 4 Mar 2014', 2014 <http://www.theyworkforyou.com>.

UK House of Commons Defence Committee, Defence and Cyber-Security, Written Evidence, 2012 <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/1881.pdf>.

UK House of Commons Defence Committee, 'House of Commons - Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13 - Defence Committee', 2013 <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm>.

UK House of Commons Defence Committee, 'House of Commons - Defence and Cyber-Security - Defence Committee; 2 MoD Networks, Assets and Capabilities', 2013 <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm>.

UK House of Commons, Home Affairs Committee, E-Crime, Fifth Report of Session 2013–14, 2013 <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf>.

UK Intelligence and Security Committee, Foreign Involvement in the Critical National Infrastructure: The Implications for National Security (London: Stationery Office, 2013). See also the Huawei Cyber Security

UK Intelligence and Security Committee, Intelligence and Security Committee Annual Report 2011-2012. (London: Stationery Office, 2012).

UK Intelligence and Security Committee, Intelligence and Security Committee of Parliament Annual Report 2012-2013.

UK Ministry of Defence and Joint Forces Command, 'New Cyber Reserve Unit Created - News Stories - GOV.UK' <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit>.

UK Ministry of Defence, ‘Supplementary Written Evidence from the Ministry of Defence’ <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm>.

UK Ministry of Defence, ‘The Strategy for Defence’, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27398/stategy_for_defence_oct2011.pdf>.

UK Ministry of Defence, Cyber Primer, 2013, available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf>.

UK Ministry of Defence, Defence Plan 2010-2014, 2010 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27163/Defence_Plan_2010_2014.pdf>.

UK Ministry of Defence, How Defence Works, version 4.1 30 September 2014, available at. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360143/20140930_24153_How_Defence_Works.pdf>.

UK Ministry of Defence, MOD Information Strategy 2011, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27388/mod_information_strat2011.pdf>.

UK Treasury, Spending Round 2013 (London: Stationery Office, 2013).