HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 554 May 2017

Cyber Security of UK Infrastructure

The Government identifies 'cyber' as one of six Tier 1 threats to national security.[1] This note focuses on the cyber threat to the UK's critical national infrastructure, describes measures to improve cyber security and challenges in how to implement them. It also examines national and international policy and legislation.

Overview

- The number of attempted cyber-attacks on critical national infrastructure is growing.[2]
- Technical and organisational measures can improve cyber security, and minimise disruption during and after an attack.
- The Government has stated that market forces have not led to cyber risk being properly understood or managed.[3] The new National Cyber Security Strategy promises greater intervention to improve this.
- There is a cyber skills shortage, with specific challenges for infrastructure security.
- Cyber-attacks can facilitate espionage or cause disruption. Several nations are developing offensive cyber capabilities.

Background

The impact of cyber crime is difficult to quantify,[4-6] but is estimated to cost the UK roughly £1-27bn per year.[7-9] The National Cyber Security Centre (NCSC) reports around 60 'high-level' cyber-attacks on the UK a month, many of which threaten national security.[10,11] The most disruptive cyber-attacks on national infrastructure to date affected Ukraine's electricity grid in 2015 and 2016 (Box 1). In the UK, cyber attacks on NHS trusts have led to cancelled operations, including the WannaCry attack in 2017 that affected 45 NHS organisations.[12,13]

This POSTnote focuses on the cyber security of the UK's critical national infrastructure (CNI), although similar threats and security measures apply to other sectors such as critical businesses and major stores of hazardous substances.[3,14] The Government classifies infrastructure as CNI on the basis of the likely impact of its disruption (Box 2).[15] It categorises CNI into 13 sectors: chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport and water.[16]

The Cyber Threat to CNI

Computer systems increasingly underpin UK CNI.[17] Examples include inter-bank payment systems,[18] NHS data networks[18] and industrial control systems that monitor and operate physical infrastructure (such as nuclear power plants[19] or railway signals[20]). Such systems are increasingly connected into large networks to allow centralised monitoring and remote or automated control, so as to make operation and maintenance more efficient.[21] These networks often connect to the internet, either directly or indirectly via the operators' other networks.[22-25] As more industrial control systems connect to computer networks, the potential for cyber-attacks to cause physical effects increases.[26,27,28] The

Box 1. Cyber-Attacks on Ukraine's Power Network

The first confirmed instance of a disruptive cyber-attack on an electricity network occurred in Ukraine in 2015.[3] A cyber-attack on three power distribution companies caused a power outage that affected 225,000 customers.[29] Power was manually restored after a few hours, but all affected companies were still running reduced operations months later.[29] The attackers are thought to have used fraudulent emails to gain access to the target networks six months before the power outages, during which time they gained the security credentials and knowledge of the infrastructure needed to complete the attack.[30] During the outage, the attackers also overwhelmed the energy company's call centre with telephone traffic to obstruct communications during the incident response.[30] A more sophisticated attack caused another outage in 2016.[31-33] The Ukrainian security service has accused Russian security services of orchestrating both attacks.[30,34]

The Cambridge Centre for Risk Studies estimates that the immediate economic impact of a significant cyber-attack on a UK regional electricity distribution network would be £12-86bn, including consequent disruption to transport, digital communications and water supplies. They note that this represents an extreme example used for stress testing, not a prediction of what is imminent or probable.[35]

Box 2. UK Critical National Infrastructure

The Government defines CNI as the assets, facilities, systems, networks or processes which, if lost or disrupted, would affect national security or the delivery of essential services, leading to severe economic or social consequences or loss of life.[16] The majority of UK CNI is privately owned.[36,37] The Government says that the responsibility for managing cyber risk in private sector CNI lies with the operators, but that it will monitor and ensure CNI cyber security, working with private operators through a variety of channels.[3]

- Lead Government Departments – Each CNI sector has a lead department that identifies CNI,[18] assesses its resilience and works with operators and others to improve resilience where necessary.[15]
- Regulators – there is no dedicated cyber security regulator, but the Information Commissioner's Office regulates data security.[38,39] Many sector-specific regulators cover aspects of cyber security, with varying powers and responsibilities.[3,18,40,41]
- The National Cyber Security Centre (NCSC) – the NCSC was established in 2016 as a single point of contact to simplify Government co-operation with industry.[42] It provides technical guidance, bespoke support (such as help designing and testing networks) and incident response assistance, and is the Government's main source of cyber expertise.[42] However, it does not have a statutory role to enforce its recommendations.[43]

The National Cyber Security Strategy provides some details on the roles and responsibilities within these public-private partnerships,[3] but critics claim that they remain unclear.[37,44-47] Concerns have been raised that the Government and private operators have different cyber security priorities, such as investment levels and how fast service is restored following an attack.[28,44] The Government's current role mostly constitutes non-mandatory support,[40] but it is reviewing CNI regulation to ensure that it has the measures in place to intervene where necessary.[3,48]

extent of connected computer systems in CNI is likely to continue to grow. For example, the Government is leading a roll-out of smart energy meters (POSTnote 471),[49] and the NHS is aiming to digitise all medical records by 2020.[50]

Computer-based CNI systems are vulnerable to electronic failure, design flaws, operator error, physical damage[51,52] and cyber-attack.[28,53] Cyber-attacks can be delivered physically (for example via a USB stick) or via the internet. Internet-based attacks range from simple scam emails sent in large numbers, to advanced attacks targeting specific institutions.[54] Sophisticated attacks progress in multiple stages, probing the network after an initial breach to gain information and control over periods that can last years.[55] Common attack methods (Box 3) may be used for the initial breach before more tailored and advanced methods are deployed.[54]

Motivations for Cyber Attacks

Cyber-attacks on CNI may be conducted for financial gain (e.g. by ransom), to manipulate public opinion, demonstrate an attacker's prowess, conduct espionage or cause physical disruption.[56,57] Potential attackers range from individuals and activist or terrorist groups with limited capability to organised crime groups and nation-states with significant expertise and resources.[3,58] Although targeted attacks on CNI typically require sophisticated techniques,[2] the NCSC warns that the technical barrier to launching successful attacks is decreasing.[10] The Government says that foreign states or state-sponsored groups regularly attempt to penetrate UK networks, targeting in particular the defence, finance, energy, telecommunications and government sectors.[3] However, the distinctions between different adversary groups are starting to blur,[10] in particular as attack tools and expertise are shared and sold, often over anonymised parts of the internet known as the 'darknet' (POSTnote 488).[28,57,64]

Box 3. Common Methods of Cyber-Attack

Cyber-attacks often exploit technical vulnerabilities in computer systems or a lack of awareness among people using computer systems; attacks frequently target both. Common attacks include:[54]

- **Phishing** – sending fraudulent emails in an attempt to manipulate the recipient into revealing sensitive information or installing malicious software on their network. **Spear-phishing** targets specific victims, using previously-gathered information to make the email appear more convincing.
- **Web-based attacks** – using fake websites or compromising authentic websites to trick visitors into downloading malicious software, sometimes automatically.[59]
- **Ransomware** – encrypting files on a target computer and demanding a ransom to make the files usable again. The ransom is often set to be small enough that payment is the cheapest solution for the victim, although there is no guarantee that it will unlock the files.[60] The National Crime Agency advises against paying any ransom.[61]
- **Distributed denial of service (DDoS) attacks** – using large numbers of previously infected devices to overwhelm a target with internet traffic (such as requests for information or emails), reducing its ability to respond to genuine traffic. The scope for such attacks is growing as rapidly increasing numbers of devices are connected to the 'Internet of Things' (POSTnote 510).[62,63]

Methods for Improving Cyber Security

Technical Methods

The Government's Cyber Essentials scheme provides guidance to protect against the low-level threats that form the bulk of all cyber-attacks;[3,65] the NCSC's '10 Steps to Cyber Security' deal with more targeted attacks.[54,66] CNI operators are expected to implement advanced cyber security measures.[67]

- Encryption – Sensitive data can be stored or transmitted in a form that is un-readable without a digital key.[68]
- Integrity checking – System files can be checked against previous records to detect changes and identify attacks.[69]
- Network monitoring – Detecting suspicious behaviour, such as a user accessing many separate parts of a network or transferring lots of data, can provide early warning of an attack and prompt responsive measures.[70]
- Penetration testing – Conducting controlled cyber-attacks on systems can test their defences and identify their vulnerabilities.[71] This can range from the use of automated tools to more in-depth, tailored approaches (Box 4).
- Security by design – Systems can be designed to perform narrowly defined actions and only accept instructions from verified sources, and networks can be designed to minimise the impact of any single failure.[72,73]

- Disconnection – The most critical systems can be disconnected from networks or replaced with non-digital systems.[19] However, this is difficult to achieve and forfeits the benefits of connected digital systems.[74] Disconnected systems can still suffer physically delivered attacks.[28,75]

Training and Managing Personnel

Attackers can target computer users as well as technical flaws, using 'social engineering' techniques to manipulate human operators into facilitating the attack.[76] The Boston Consulting Group found that around 35% of the largest data breaches between 2011 and 2016 were caused by human negligence, ignorance or malicious intent of internal staff.[77] Raising awareness and providing clear, practical guidance can help staff identify and respond to an attack.[77] Vetting staff, restricting system or data access and editing rights (e.g. requiring two separate individuals to approve major changes), and physical security measures such as swipe cards, can provide some defence against malicious intent.[3,77-79]

Information Sharing

Intelligence agencies and organisations targeted by cyber-attacks can prepare their defences by sharing information about previous and imminent attacks.[2,37] The NCSC's joint Government and industry Cyber-security Information Sharing Partnership (CiSP) comprises over 2,225 organisations.[80] CiSP has been used to deal with real and simulated attacks and is generally seen to work well,[37,81,82] though some feel incidents are still under-reported, especially in certain sectors,[10,28,72] and co-operation could be improved.[37]

Cyber Resilience

No combination of security measures can guarantee immunity from cyber-attack.[3,36,56,77,83] The Cabinet Office aims for CNI 'resilience', combining protective measures that minimise the chance of an attack succeeding with the ability to continue to provide essential services during an attack and to recover fully from it afterwards.[84] Beyond technical methods, frameworks and standards for CNI cyber risk management include organisational measures, such as:[85-88]

- identifying critical assets and their interdependencies
- communicating risks to external stakeholders
- backing-up data and maintaining reserve systems
- preparing and testing incident response plans
- amending security in response to previous incidents

Insurance

The nascent cyber insurance market is expected to grow as the risks involved become better quantified and cyber security becomes more regulated.[2,89,90] As well as limiting the financial loss an attack can inflict, insurers could promote or mandate best practice and standards among their clients.[89] Premiums put a cost on cyber risk, which could motivate better cyber security, but only if prices reflect the specific risk that an organisation faces.[28,89,91,92]

Box 4. Intelligence-Led Cyber Vulnerability Testing

In 2014, the Bank of England introduced the 'CBEST' framework for rigorous penetration testing of firms at the core of UK financial market infrastructure, involving realistic attack methods tested on live systems.[93,94] The attacks are designed specifically for each firm, drawing on Government and private sector intelligence to mimic the most sophisticated threats they face.[94] CBEST includes several measures to minimise the risk of accidental disruption to critical services during testing. These include: specific training for accredited penetration testers; pre-agreed boundaries for testing and response measures for incidents; liability (and insurance where applicable) arranged in advance; and oversight by the firm being tested, which can temporarily halt the test as appropriate.[94] Participation is voluntary, but 30 of the 35 firms invited to take part had completed testing by November 2016 with the rest either undertaking or scoping the work.[95]

Challenges for CNI Cyber Security

Challenges Posed by CNI Systems

Many CNI computer systems were designed before cyber security was a major concern.[96,97] More recent systems can also become vulnerable if their vendors stop supplying security updates.[98] Legacy systems can be expensive or risky to replace so they often rely on the security of the systems they connect to,[98] reducing the layers of defence.[72]

CNI safety requirements can complicate or even conflict with standard cyber security measures.[99] Security updates alter computer systems, and may need extensive testing to comply with safety requirements.[72] Often, downtime in safety-critical systems must be minimised, making it difficult to install updates frequently or isolate targeted systems during an attack.[99] Safety can be provided by secondary systems that take over if the main system fails. However, these do not provide cyber security if they use similar software, and can reduce it by providing an alternative route of attack.[99,100]

Supply Chains

CNI operators are increasingly replacing proprietary computer systems with commercial products.[21,101] The wider use of similar products allows attack methods to be shared and applied to different CNI.[72,102] Many feel that the market incentive for manufacturers to supply secure products is too weak, with some calling for greater regulation or accountability,[103-105] or fundamental changes to production and testing techniques.[106] It has been estimated that software typically contains roughly 3 errors per 100 lines of code (1 per 1,000 for safety-critical systems);[107] software can contain millions of lines of code.[36] Standards can guide the procurement of secure products, but their use is limited by the diversity of standards available, the cost of compliance and the rapid evolution of technologies and threats.[108-110] Globalised supply chains make it difficult to source all components from trusted or national companies,[36] or even to know their full provenance.[111] Concerns have been expressed about the potential for vulnerabilities to be purposefully introduced into CNI systems supplied from abroad (Box 5). A leaked document from 2010 showed that the US National Security Agency was intercepting exports of

Box 5. Foreign Involvement in UK CNI

Supply Chain Involvement

A Chinese company, Huawei, has supplied equipment for UK communications CNI since 2007.[36] In 2008, MI5 stated the theoretical potential for the Chinese state to exploit vulnerabilities in Huawei equipment to intercept or disrupt UK communications.[36] GCHQ reported that the risk was mitigated by measures including designing networks to be difficult to attack but easy to monitor, and the establishment of a Cyber Security Evaluation Centre (CSEC), run by Huawei but jointly overseen by GCHQ, to test Huawei's products for vulnerabilities.[36,112] In 2015, CSEC found three issues that required intervention in deployed networks;[112] GCHQ has said that it is impossible to guarantee detection of all software flaws.[36] The USA and Australia have previously excluded Huawei from government contracts,[36] but the UK National Security Adviser noted that in reality foreign technology is used in virtually all networks worldwide.[113]

Foreign Investment and Direction

In 2016, the Government approved the construction of a nuclear power plant at Hinkley Point by Electricité de France and China General Nuclear Power Corporation, who will own a 66.5% and 33.5% stake respectively.[114,115] In 2015, the Government declared its support for a Chinese-led project at Bradwell;[116,117] a Chinese reactor design is currently under review by the Office for Nuclear Regulation, whose remit includes cyber security.[118] Senior military and intelligence figures have allegedly expressed concern at Chinese involvement in Hinkley Point,[119] but some cyber security experts have said that global supply chains make Chinese-made components difficult to avoid, and that similar cyber security measures will be required, whoever owns the plant.[120] The Government highlighted the UK's strong nuclear regulation,[121] and published a civil nuclear cyber security strategy.[122] It is also developing a new legal framework for foreign investment in CNI, for future projects.[123]

computer network devices and implanting access points for later exploitation.[124-126]

Skills Shortage

A cyber skills non-profit organisation, *(ISC)²*, predicts a shortfall of 1.8m people in the global cyber security workforce by 2022;[127] one employment agency found that the UK had the second largest cyber skills gap of 10 major countries.[128] CNI-specific skills challenges include the need for experts with experience of infrastructure technology as well as computer systems,[129] and nationality requirements.[130]

National and International Policy

The National Cyber Security Strategy

The Government published its second five-year national cyber security strategy in 2016, with £1.9bn of investment.[3] The core aims are to defend the UK from cyber-attacks, deter potential attackers and develop the UK's cyber security industry. CNI cyber security is listed as a priority. It states that the previous strategy's dependence on market forces did not achieve sufficient progress, with cyber risk currently 'not properly understood or managed' across CNI. The new strategy promises greater intervention, including:

- increased intelligence and law enforcement activity to identify, anticipate and disrupt cyber adversaries
- investment in academic and industrial research and innovation, including start-up companies[131]

Box 6. Cyber-Related EU Legislation

The Networks and Information Security (NIS) Directive

The EU adopted the NIS Directive in 2016, to be transposed into national law by May 2018.[132] It requires Member States to:[133]

- adopt a national cyber security strategy
- designate one or more national competent authorities with the necessary powers to assess and enforce compliance
- designate one or more Computer Security Incident Response Teams (CSIRTs) to monitor threats, respond to incidents and participate in an EU CSIRT network
- participate in a new Co-operation Group, to support strategic cooperation and information exchange between Member States.

Operators of essential services will have to take technical and organisational steps to manage the risks to their networks, and notify authorities of significant security incidents. The Government intends to set out details of how it will implement the NIS Directive in 2017.[48]

The General Data Protection Regulation (GDPR)

The GDPR aims to strengthen privacy rights and imposes new security obligations with large fines for non-compliance.[134,135] It covers all personal data, including some relevant to CNI (e.g. medical data).[136] EU Member States must apply the GDPR by May 2018 (see House of Commons Briefing Paper 7838).[134,135]

- measures to raise public awareness of cyber security, to support cyber training in different formats and at all education levels (including apprenticeships with CNI operators[137]),[138-140] and to develop the cyber security profession
- working with communications service providers and industry to make the internet more secure to use[141]
- more support for CNI operators such as sharing threat intelligence and best practice, and conducting joint exercises to test and develop their cyber resilience
- the potential for increased regulation, for example via implementation of the EU's NIS Directive (Box 6).

International Action

The UK co-operates internationally by sharing information on best practice and current threats,[142,143] conducting simulated attack exercises[144,145] developing standards,[3,109,146] funding schemes abroad,[147,148] and co-operating on international law enforcement.[149,150] International infrastructure, such as air traffic and satellite systems, is increasingly used.[91,151] The new strategy aims to expand international co-operation.[3]

The Government states that much of the cyber threat to the UK originates overseas.[3] Cyber-attacks easily cross borders and it can be difficult for law enforcement agencies to take action in jurisdictions with limited extradition arrangements.[3] The Budapest Convention on Cybercrime is the standard international agreement used to tackle cyber crime,[149] with signatories agreeing to criminalise relevant activities (e.g. intentional interference with a computer system).[152,153] The UK is one of 52 signatories, but countries including Russia, China and India are not, citing concerns over sovereignty or limited involvement in drafting the treaty.[154-157] New EU legislation on cyber security will come into force by May 2018 (Box 6).

Offensive Cyber Capabilities

Offensive cyber activity entails deliberate disruption of computer systems. US officials stated that over 30 nations were developing offensive cyber capabilities in 2016.[56] The UK's National Offensive Cyber Programme is developing such capabilities, partly to deter prospective attacks.[3] Critics have highlighted the potential difficulty in achieving targeted, proportionate deterrence due to the interconnectedness and complexity of computer networks,[23,158,159] the bespoke preparation required to attack a specific target,[160,161] and difficulties in attributing the source of cyber-attacks[162] (attacks often take complex routes around the internet, sometimes via previously-infected devices, to mask their origin).[23,163]

Endnotes

1 'National Security Strategy and Strategic Defence and Security Review 2015', HM Government (2015)
2 'Annual Report 2015/2016', CERT-UK (2016)
3 'National Cyber Security Strategy 2016-2021', HM Government (2016)
4 'The Threat of Cyber-Crime to the UK: RUSI Threat Assessment', Royal United Services Institute (2014)
5 'National Strategic Assessment of Serious and Organised Crime 2015', National Crime Agency (2015)
6 'The Cost of Incidents Affecting CIIs', ENISA (2016)
7 'NCA Strategic Cyber Industry Group - Cyber Crime Assessment 2016', National Crime Agency (2016)
8 'Over £1bn lost by businesses to online crime in a year', ActionFraud (2016)
9 'The Cost of Cyber Crime', Cabinet Office (2011)
10 'The Cyber Threat to UK Business', National Cyber Security Centre and National Crime Agency (2017)
11 'Russia steps up cyber-attacks on UK', The Times, (2017)
12 'Lincolnshire operations cancelled after network attack', BBC News (2016)
13 'NHS cyber-attack: Amber Rudd says lessons must be learnt', BBC News (2017)
14 'The Control of Major Accident Hazards Regulations 2015: Guidance on Regulations', Health and Safety Executive (2015)
15 'Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards', Cabinet Office (2010)
16 'Summary of the 2015-16 Sector Resilience Plans', Cabinet Office (2016)
17 'Communiqué from the 'Strengthening the cyber security of our essential services' event', Policy paper (2014)
18 'Sector Resilience Plan for Critical Infrastructure 2010', Cabinet Office (2010)
19 'Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities', Nuclear Threat Initiative (2016)
20 'Rail Cyber Security: Guidance to Industry', Department for Transport (2016)
21 'Guide to Industrial Control Systems (ICS) Security', US National Institute of Standards and Technology (2015)
22 'Cyber Security Assessments of Industrial Control Systems: A Good Practice Guide', Centre for the Protection of Critical National infrastructure (2011)
23 'Reducing Systemic Cybersecurity Risk', OECD (2011)
24 'Communication network dependencies for ICS/SCADA Systems', ENISA (2016)
25 'Securing the Industrial Internet of Things', Information Systems Security Association Journal, p.24-30 (2015)
26 'A Survey of SCADA and Critical Infrastructure Incidents', Proceedings of the 1st Annual Conference on Research in Information Technology (2012)
27 Written Evidence from the Institution of Engineering and Technology to the Joint Committee on the National Security Strategy inquiry, 'Cyber Security: UK National Security in a Digital World' (2017)
28 'Internet Organised Crime Threat Assessment', Europol (2016)
29 'Alert (IR-ALERT-H-16-056-01) - Cyber-Attack Against Ukrainian Critical Infrastructure', ICS-CERT (2016)
30 'Analysis of the Cyber Attack on the Ukrainian Power Grid', SANS Institute (2016)
31 'Ukraine power cut 'was cyber-attack'', BBC News (2017)
32 'Latest Ukraine Blackout Tied To 2015 Cyberattackers', Dark Reading (2017)
33 'Responding to another Ukrainian power attack', Atkins, (2017)
34 'Ukraine charges Russia with new cyber attacks on infrastructure', Reuters (2017)
35 'Integrated Infrastructure: Cyber Resiliency in Society', University of Cambridge (2016)
36 'Foreign involvement in the Critical National Infrastructure', Intelligence and Security Committee (2013)
37 'Public–Private Security Cooperation: From Cyber to Financial Crime', Royal United Services Institute (2016)
38 'Data Protection Regulatory Action Policy', Information Commissioner's Office (2013)
39 'The Guide to Data Protection', Information Commissioner's Office (2017)
40 'The UK's Cybersecurity Regulatory Landscape: An Overview', Hogan Lovells (2016)
41 'Cybersecurity Capacity Review of the United Kingdom', Global Cyber Security Capacity Centre (2016)
42 'Prospectus: Introducing the National Cyber Security Centre', HM Government (2016)
43 'Cyber Security in the Financial Services Sector', Letter from Rt Hon Philip Hammond MP to Rt Hon Andrew Tyrie MP, 20th January 2017
44 'Public–private partnerships in national cyber-security strategies', International Affairs, **92** p.43-62 (2016)
45 'Protecting information across government', House of Commons Committee of Public Accounts (2017)
46 'Cyber Security in the Financial Services Sector', Letter from Rt Hon Andrew Tyrie MP to Ciaran Martin, 7th December 2016
47 Written evidence to the Joint Committee on the National Security Strategy, Information Assurance Advisory Council (2017)
48 'Cyber Security Regulation and Incentives Review', HM Government (2016)
49 'Smart Metering Implementation Programme: Fourth Annual Report on the Roll-out of Smart Meters', Department of Energy and Climate Change (2015)
50 'Personalised Health and Care 2020: Using Data and Technology to Transform Outcomes for Patients and Citizens – A Framework for Action', HM Government (2014)
51 'The Internet Under Crisis Conditions: Learning from September 11', The National Academies Press (2003)
52 'Cyber War in Perspective: Russian aggression against Ukraine', NATO CCDCOE (2015)
53 'Connected Nations 2016', Ofcom (2016) – Figure 34 outlines causes of disruption to communications networks
54 'Common Cyber Attacks: Reducing the Impact', National Cyber Security Centre (2016)
55 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', Lockheed Martin (2011)
56 'Foreign Cyber Threats to the United States', Joint Statement for the Record to the Senate Armed Services Committee, US Office of the Director of National Intelligence (2017)
57 'Know Your Cyber Enemy', IBM (2016)
58 'ENISA Threat Landscape Report 2016', ENISA (2017)
59 'Web Based Attacks', Symantec (2009)
60 'Protecting your organisation from ransomware', NCSC (2016)
61 'ALERT - Mass ransomware spamming event targeting UK computer users', National Crime Agency (2013)
62 'Infrastructure Disruption: Internet of Things Security', Statement of Prof. Kevin Fu to the U.S. House Energy and Commerce Committee, 16th November 2016
63 'Strategic Principles for Securing the Internet of Things (IoT)', US Department of Homeland Security (2016)
64 'The National Cyber Security Strategy: Steady as She Goes or Significant Change?', RUSI Commentary (2016)
65 'Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks', HM Government (2014)
66 '10 Steps to Cyber Security', National Cyber Security Centre (2016)
67 'Cyber Essentials Scheme: Summary', HM Government (2014)
68 'Data Encryption', POSTbrief 19 (2016)
69 'NIST Special Publication on Intrusion Detection Systems', National Institute of Standards and Technology (2001)
70 '10 Steps To Cyber Security - Monitoring', NCSC (2016)
71 'Penetration Testing: Assessing Your Overall Security Before Attackers Do', SANS Institute (2006)
72 'Cyber Security at Civil Nuclear Facilities: Understanding the Risks', Chatham House (2015)
73 'The smart security behind the GB Smart Metering System', NCSC (2016)
74 'Private sector cyber resilience and the role of data diodes', NCC Group (2016)
75 'W32.Stuxnet Dossier', Symantec (2011)
76 'An Introduction to Social Engineering', CERT-UK (2015)
77 'Building a Cyberresilient Organization', The Boston Consulting Group (2017)
78 'Mitigating Insider Sabotage', SANS Institute InfoSec Reading Room (2009)
79 'Cybersecurity for SCADA Systems', William Shaw (2006)
80 'Cyber-security Information Sharing Partnership (CiSP)', NCSC
81 'Competitive Analysis of the UK Cyber Security Sector', Pierre Audoin Consultants (2013)

82 'Waking Shark II Desktop Cyber Exercise: Report to participants', Chris Keeling (2013)
83 'Partnering for Cyber Resilience', The World Economic Forum (2012)
84 'Summary of the 2016 Sector Security and Resilience Plans', Cabinet Office (2016)
85 'Framework for Improving Critical Infrastructure Cybersecurity', National Institute of Standards and Technology (2014)
86 ISO/ISEC 27000 Family, International Organization for Standardization
87 'Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide', US Department of Homeland Security (2016)
88 'Cyber Security Capability Maturity Model (CMM) – V1.2', Global Cyber Security Capacity Centre, University of Oxford (2014)
89 'UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk', HM Government (2015)
90 'Cyber Insurance: Recent Advances, Good Practices and Challenges', ENISA (2016)
91 'Space, the Final Frontier for Cybersecurity?', Chatham House (2016)
92 'Business Blackout: The insurance implications of a cyber attack on the US power grid', Lloyd's (2015)
93 'Managing cyber risk – the global banking perspective', Speech given by Andrew Gracie, Executive Director, Resolution, Bank of England to the British Bankers' Association Cyber Conference, London (10th June 2014)
94 'CBEST Intelligence-Led Testing: CBEST Implementation Guide', Bank of England (2016)
95 'Resilience and security of IT systems in financial services', FCA/PRA response to Treasury Select Committee, 04/11/2016
96 'UK Cyber Security and Critical National Infrastructure Protection', International Affairs **92**, p.1079-1105 (2016)
97 'Cyber Security for SCADA Systems', Thales (2013)
98 'Mitigating Cyber Security Risks in Legacy Process Control Systems', Honeywell (2014)
99 'Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems', Developing Safe Systems: Proceedings of the 24th Safety-Critical Systems Symposium, C.W. Johnson (2016)
100 'Managing Cybersecurity for Industrial Control Systems', Agence nationale de la sécurité des systèmes d'information (2012)
101 'Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors', ENISA (2015)
102 'CyberSafety: On the Interactions between CyberSecurity and the Software Engineering of Safety-Critical Systems', 20th Annual Conference of the UK Safety-Critical Systems Club, C.W. Johnson (2012)
103 'Software manufacturers have little incentive to make products secure', Letter to the Financial Times, Prof Martyn Thomas, Visiting Professor of Software Engineering at Oxford University, 04/01/2015
104 'What Trump Can Do About Cybersecurity', Bloomberg (2016)
105 'Rise of the Machines: The Dyn Attack Was Just a Practice-Run', Institute for Critical Infrastructure Technology (2016)
106 Written evidence to the Joint Committee on the National Security Strategy, Prof Martyn Thomas, 9th March 2017
107 'Software in Safety Critical Systems: Achievement and Prediction', Nuclear Future, **2** 3 (2006)
108 'UK Cyber Security Standards', Department for Business, Innovation and Skills (2013)
109 'Standards for Cyber Security', ENISA (2014)
110 Ofcom evidence to the House of Commons Culture, Media and Sports Committee's inquiry into 'Cyber Security: Protection of Personal Data Online' (2015)
111 'Cyber-Security Risks in the Supply Chain', CERT-UK (2015)
112 'Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2016', Huawei Cyber Security Evaluation Centre Oversight Board (2016)
113 'Huawei Cyber Security Evaluation Centre: Review by the National Security Adviser', HM Government (2013)
114 'Hinkley Point C to power six million UK homes', Press release (2015)
115 'Hinkley Point C' Collection, Department for Business, Energy & Industrial Strategy
116 'Statement of Cooperation in the Field of Civil Nuclear Energy 2015' (2015)
117 'Agreements in place for construction of Hinkley Point C nuclear power station', Press release, EDF (2015)
118 'UK HPR1000 Reactor', Written statement HCWS398 (2017)
119 'Nuclear deal with China is threat to UK security', The Times (2015)
120 'Concern about Chinese involvement at Hinkley Point is misdirected, say experts', SC Magazine UK (2016)
121 'GCHQ seeks to allay Hinkley security fears', Financial Times (2015)
122 'Civil Nuclear Cyber Security Strategy', Department for Business, Energy and Industrial Strategy (2017)
123 'Government confirms Hinkley Point C project following new agreement in principle with EDF', Press Release, Department for Business, Energy & Industrial Strategy (2016)
124 'Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets', NSA Documents Archive, American Civil Liberties Union (2010)
125 'Glenn Greenwald: how the NSA tampers with US-made internet routers', The Guardian (2014)
126 'No Place to Hide', Glenn Greenwald (2014)
127 'Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022', (ISC)² blog (2017)
128 'Indeed Spotlight: The Global Cybersecurity Skills Gap', Indeed (2017),
129 'Mitigating the Cybersecurity Skills Shortage', Cisco (2015)
130 'Cyber Security Skills', HM Government (2014)
131 'Making Cyberspace "Cyber Safe" - New Government initiative for Cyber startups will drive innovation', Press release (2016)
132 'Directive on Security of Network and Information Systems', European Commission – Fact Sheet (2016)
133 'Directive (EU) 2016/1148 of the European Parliament and of the Council', Official Journal of the European Union (2016)
134 'Regulation (EU) 2016/679 of the European Parliament and of the Council', Official Journal of the European Union (2016)
135 'Brexit and data protection', House of Commons Library Briefing Paper 7838 (2016)
136 'Overview of the General Data Protection Regulation (GDPR)', Information Commissioner's Office (2017)
137 'Cyber security CNI apprenticeships', Department for Culture, Media & Sport (2017)
138 'Cyber Security: A Guide to Programmes and Resources for Schools & Further Education', HM Government (2015)
139 'Fresh drive to develop next generation of cyber security experts', NCSC (2017)
140 'Inside Cyber', Issue 1, Cyber Security Challenge UK (2016)
141 'Active Cyber Defence - tackling cyber attacks on the UK', NCSC blog post (2016)
142 'Cybersecurity Cooperation: Defending the digital frontline', ENISA (2013)
143 'Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation', Office of the White House Press Secretary (2015)
144 'Cyber Europe 2016 – Questions and Answers', ENISA (2016)
145 'Transatlantic exercise to tackle cyber threat', News story, HM Treasury (2015)
146 'White Paper No. 01 – Recommendations for a Strategy on European Cyber Security Standardisation', CEN/CENELEC/ETSI Cyber Security Coordination Group (2014)
147 'FCO Cyber Security Capacity Building Programme', News Story, British Embassy Mexico City (2016)
148 'The UK Cyber Security Strategy 2011-2016: Annual Report', Cabinet Office (2016)
149 'Cyber Crime Strategy', Home Office (2010)
150 'International cyber crime exercise tests multi-agency response', National Crime Agency (2015)
151 'European ATM Master Plan', Single European Sky's ATM Research (2015)
152 'Convention on Cybercrime', European Treaty Series No. 185, Council of Europe (2001)
153 'T-CY Guidance Note #6: Critical information infrastructure attacks', Council of Europe Cybercrime Convention Committee (2013)
154 'Chart of signatures and ratifications of Treaty 185', Council of Europe
155 'Russia prepares new UN anti-cybercrime convention', Cyber Security Review (2017)
156 'Bilateral Discussions on Cooperation in Cybersecurity', China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS) Joint Statement (2012)
157 'India won't sign Budapest pact on cyber security', Governance Now (2013)
158 'FM 3-38: Cyber Electromagnetic Activities', US Army (2014)
159 'Task Force on Cyber Deterrence', US Department of Defense (2017)
160 'Inside the secret digital arms race: Facing the threat of a global cyberwar', Tech Republic (2014)
161 Written evidence to the Joint Committee on the National Security Strategy, Royal United Service Institute (2017)
162 'Defence and Cyber-Security', House of Commons Defence Committee (2012)
163 'A Survey of Challenges in Attribution', Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for US policy, National Academies Press, p.41-52 (2016)