Cyber Security and the UK's Critical National Infrastructure

A Chatham House Report

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke

CHATHAM HOUSE

www.chathamhouse.org

Cyber Security and the UK's Critical National Infrastructure

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke

A Chatham House Report

September 2011

CHATHAM HOUSE

www.chathamhouse.org

Chatham House has been the home of the Royal Institute of International Affairs for ninety years. Our mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all.

BAE Systems Detica delivers information intelligence solutions to government and commercial customers. We help them collect, exploit and manage data so they can deliver critical business services more effectively and economically. We also develop solutions to strengthen national security and resilience.to government and commercial customers. Our services include cyber security, managing enterprise risk and compliance, data analytics, systems integration and managed services, strategy and business change and the development of software and hardware technologies. Detica is part of BAE Systems, a global defence and security company.
www.detica.com

The Royal Institute of International Affairs
Chatham House
10 St James's Square
London SW1Y 4LE
T: +44 (0) 20 7957 5700
F: + 44 (0) 20 7957 5710
www.chathamhouse.org

Charity Registration No. 208223

ISBN 978 1 86203 251 4

A catalogue record for this title is available from the British Library.

Designed and typeset by Soapbox, www.soapbox.co.uk

Printed and bound in Great Britain by Latimer Trend and Co Ltd

The material selected for the printing of this report is Elemental Chlorine Free and has been sourced from well-managed forests. It has been manufactured by an ISO 14001 certified mill under EMAS.

Contents

About the Authors

Paul Cornish is Professor of International Security at the University of Bath. He was Head of the International Security Programme and Carrington Chair in International Security at Chatham House from 2005 to 2011, having been Director of the Centre for Defence Studies at King's College London from 2002 to 2005. Professor Cornish has taught at the University of Cambridge and the Joint Services Staff College and has served in the Foreign & Commonwealth Office and the British Army. His work has covered national strategy and defence policy, counter-terrorism and domestic security, European security institutions, the ethics of the use of armed force, arms control and non-proliferation, and the future of international security. He has also spoken and published extensively on cyber security. Recent publications include *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks* (European Parliament, 2009); *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (co-author, Chatham House, 2009); *On Cyber Warfare* (co-author, Chatham House, 2010); and *The Vulnerabilities of Developed States to Economic Cyber Warfare* (Chatham House, 2011). He is a member of the Chief of the Defence Staff's Strategic Advisory Panel.

David Livingstone is an Associate Fellow on the International Security Programme at Chatham House and the Managing Director of Napier Meridian. His company, established in 2005, provides expertise on business transformation in the national security and resilience domain, with a particular focus on the cyber domain. He was a desk officer in the Directorate of Military Operations in the Ministry of Defence (MoD) for four years in the mid-1990s, when the issue of cyber security (then in the guise of 'Information Warfare') was first identified as an emerging threat. He was a founder member of the Cabinet Office's first official committee addressing the electronic threats to the Critical National Infrastructure. In his MoD appointment he was a staff officer in COBR and worked on a number of other Cabinet Official Committees concerned with national security matters. He retired from the Services in 1999. At Chatham House he has written a number of works on cyber security, counter-terrorism, serious organized crime, and other security policy-related subjects, and is co-author of *On Cyber Warfare*. He is a Fellow of the Royal Geographical Society.

Dave Clemente is a Research Analyst with the International Security Programme at Chatham House. He was educated at the Ohio State University, the University of Damascus and the School of Oriental and African Studies, University of London. He previously worked with the International Institute for Strategic Studies and the Overseas Development Institute. His areas of research include cyber security policy, US and UK security and defence policy, and stabilization and reconstruction. He is co-author of *On Cyber Warfare*.

Claire Yorke is Manager of the International Security Programme at Chatham House. She was educated at Lancaster University, the University of Exeter and Sciences Po Lille. Following her Masters degree in Middle East Politics she worked for three years as a Parliamentary Researcher in the House of Commons. Her research interests include UK defence and security policy, cyber security, organized crime, post-conflict reconstruction and stabilization. She is co-author of *On Cyber Warfare*.

Acknowledgments

The authors wish to thank all the interviewees who assisted in the research for this project from a range of organizations. We are also grateful to those at Chatham House and elsewhere who read and commented upon earlier versions of the report. We wish to acknowledge CyberCloud for running the analysis that produced the needs and requirement statements in Annex C. Finally, we thank BAE Systems Detica Ltd for their sponsorship of the project.

The views expressed are those of the authors and any inaccuracies in fact or interpretation are their own.

September 2011 PC, DL, DC, CY

Executive Summary and Recommendations

Dependence on information and communications technology (ICT) is a defining feature of a modern, interconnected and knowledge-based society and economy. The machinery of government, critical national infrastructure (CNI) – including the provision of essential services such as water, gas, electricity, communications and banking – and much of the straightforward private life of individual people are all ICT-dependent to a large degree. With this dependency can come vulnerability to aggressors, criminals and even the merely mischievous.

Public and media attention is frequently drawn to tales of hacking and espionage and there is persistent concern about the rapid growth of cyber crime such as banking fraud and identity theft. The discovery of the Stuxnet virus in 2010 provided evidence of the growing sophistication of cyber threats and the potential damage they could cause to governments, organizations and critical infrastructure around the world.

It is clear both that the sense of threat and vulnerability is mounting and that the public and private sectors are under increasing pressure to 'do something' about cyber security. The United Kingdom National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) released in October 2010 promoted cyber security to a Tier One risk to national security, and its high status was reinforced by the UK government's allocation of £650 million to cyber security and resilience.

What should be done to meet this challenge? And who or what is best placed to tackle the problem, given that £650 million will hardly enable the government to counter all conceivable cyber threats and that, in any case, the vast majority of critical infrastructure in the UK is privately owned?

Cyber stakeholders

The first task should be to identify all those with a stake in cyber security, as the essential basis for the development of a national culture of cyber security. Yet there is currently no publicly available, comprehensive account of the UK national cyberspace stakeholder environment that could provide the basis for the development of a national cyber security regime, culture or policy framework. This report aims to fill that gap.

The Centre for the Protection of Critical National Infrastructure and the UK *Cyber Security Strategy* include in their definition of critical national infrastructure (CNI) communications, emergency services, energy, finance, food, government and public services, health, transport and water. Taking this definition as its starting point, this report asks whether the various agencies, bodies and individuals involved recognize the significance of the cyber stakeholder status that has been conferred upon them. How do these organizations identify and measure their cyber dependencies, and how well and systematically do they manage the risks and mitigate the potential vulnerabilities associated with these dependencies?

The report is based on a series of high-level interviews through which the authors sought to gauge the various organizations' overall understanding of, and response to, the problem of cyber security. Rather than interview communications officers or representatives of IT departments, the authors sought wherever possible to assess the level of cyber security awareness at board level, and particularly among the most senior executives who had no specific IT expertise.

Threat perceptions

With regard to threat perceptions and sensitivity, the principal finding of the report is that there appears to be no coherent picture or sense of what constitutes a vulnerability, or of the likely severity of the consequences of

that vulnerability. There is, in short, no agreement on the nature and gravity of the problem that is either so compelling or so widely accepted as to catalyse a society-wide response to the challenges of cyber security, embracing the public and private sectors.

Many interviewees shared the perception that the national response mechanism is for the most part fractured and incoherent. There are many sources of information on cyber threats, including specialist media and government briefings and alerts from security software companies. Yet there appears to be widespread dissatisfaction across the CNI with the quality and quantity of information-sharing between the public and private sectors. There was considered to be an absence of an authoritative 'rich picture' generated at the centre (i.e. by government) that could help to develop a more comprehensive and urgent sense of the cyber threats that need to be tackled. This picture would improve the awareness of risk in and from cyberspace and would enable a more effective collective response. The richness of this threat picture is dependent upon the willingness to share sensitive information, and to do so in a timely manner. However, the UK government is perceived by many, whether justifiably or not, to be more willing to solicit information than to divulge it.

The 2010 NSS and SDSR both stress the importance of cyberspace to national security. There is as yet, however, little sense either of governmental vision and leadership, or of responsibility and engagement within the CNI that could encourage a well-informed and dynamic political debate on cyber security as a national challenge.

Yet government cannot provide all the answers and cannot guarantee national cyber security in all respects and for all stakeholders. As a result, the report concludes that CNI enterprises should seek to take on greater responsibility and instil greater awareness about the nature of cyber risks across their organizations. Senior management should, for example, create incentives for departments and individual employees to recognize and address cyber dependencies and vulnerabilities as they arise. However, this will only be achieved to the extent that board members are themselves more aware of the opportunities and threats presented by cyberspace.

Organizational approaches

Many of the organizations surveyed in the course of this project have developed an attitude to cyber security that is fundamentally contradictory. In most cases, they declared themselves to be aware of cyber security threats. Yet these same organizations were willing, for a variety of resource and other reasons, to accept an unexpectedly high level of risk in this area. In several cases it was even decided that cyber risk should be managed at arm's length from the executive authority and responsibility of the board and senior management. Paradoxically, therefore, in these organizations a heightened perception of cyber security risk is being met with diminished resources and interest.

Several senior executives expressed a wish to become more intelligent customers, feeling that at present they speak a different language from their ICT professionals and are thus unable to consider cyber security issues in sufficient depth. It appears that more fundamental behavioural transformation is required, with the needs of the business driving ICT security rather than the other way around. This in turn requires IT security departments to develop a deeper understanding of how value is created in the organizations they endeavour to protect. For their part, the senior managers of organizations, both large and small, can no longer afford to treat cyber security as the remit of only one department. The potential for damage, both economic and reputational, from complacency over matters of cyber dependency and vulnerability is too high to be ignored by even the largest multinationals.

Although the report identified shortcomings in the management of the cyber security response in the CNI, more encouraging practices were also found. However, such incidents of 'best practice' were scattered haphazardly across the range of organizations interviewed. Most strikingly, the quality of practice could vary significantly within an organization, with some displaying both the 'best' and the 'worst' practices and behaviour in their sector. A simple expedient to raise the general level of awareness of good cyber security practice across the CNI and, by extension, across society more broadly, would be to develop a single, accessible bank of cyber security information and advice upon which organizations, enterprises, government bodies and individuals could draw.

Key recommendations

The cyber security threat cannot be met by government alone. The potential for cyber attacks to cause damage at a societal level calls for a coordinated response in which dependencies and vulnerabilities in infrastructure, industry and key organizations can all be identified and addressed. Given the scale and scope of the challenge, responsibility for the solution should be shared by government and the CNI. Acknowledging this imperative, what follows is a series of policy recommendations intended to drive a collaborative effort between the private and the public sectors.

Perceptions and the threat landscape

1. Although there is growing awareness of the threats and risks in cyberspace, there is still limited understanding of the nuances of the debate. The government should assume an integral role in shaping the discourse, informing wider society and raising levels of awareness. Government can act as a focal point for collating information while creating a broad picture in partnership with the private sector.
2. Government and the wider CNI should recognize and respond to the rapid pace of change in cyberspace and to the heterogeneous nature of cyber threats through more comprehensive internal strategies and risk awareness levels as well as updated and dynamic technologies and management processes.
3. Organizations should look in more depth at dependencies and vulnerabilities that may be hidden in other organizations on which they are dependent and which are part of a common supply chain.
4. There is a need for organizations to acknowledge and respond to the potential damage that organizational insiders can cause without interfering in the levels of productivity and creativity.
5. Research and investment in cyber security are essential to meeting and responding to the threat in a timely fashion and to nurturing human resource capabilities yet this area is currently under-resourced and lacks the appropriate long-term funding in both the public and private sector.

Managing cyber dependencies

1. Cyber security should be a fundamental component of an organization's risk strategy. While there will inevitably be 'unknown unknowns', more thorough risk assessments and more agile response mechanisms will narrow the chances of strategic shock and will increase overall resilience against cyber threats.
2. There is a need to address organizational inconsistencies in risk management and to develop a more comprehensive understanding of risk as it relates to cyber security.
3. Senior management will need to be more aware of the range of cyber dependencies within their organization and the budgetary and reputational implications of vulnerabilities. They should be sufficiently confident to ask the right questions from those tasked with providing security within their organization.
4. In the pursuit of efficiency savings and improved quarterly returns, companies should take care not to undermine risk mitigation strategies and contingency planning. Clear plans are needed and adequate resources must be allocated for disaster recovery.
5. CNI organizations will need to look further ahead to identify potential threats and to develop anticipatory responses to the potential cyber risks within the organization.
6. Training and development of staff in cyber security measures should be seen as an integral part of risk mitigation strategies.
7. The management of cyber dependencies will require the cooperation of CNI and government, and an effective collaboration should seek to clarify responsibilities and expectations within both the public and private sectors and at the correct designated level of responsibility.

Information communication and outreach

1. Detailed, specific information communication and outreach strategies are essential to achieving consistency in managing cyber risks as part of a systematic approach to developing a culture of awareness. These should be targeted at, and tailored for, both board-level members and technology experts and disseminated across organizations to enhance overall awareness of the issue.

2. Internal strategic communications regarding cyber threats should be transmitted across an organization with a clear sense of decision-making hierarchies (or 'chains of command'), responsibility and accountability.
3. Government will have to communicate with senior private-sector management in language the latter can understand. The issue of cyber risks needs to be made accessible for those who are neither familiar with technology nor highly IT-literate.
4. Cyber terminology should be clear and the language proportionate to the threat. It should also encourage a clear distinction to be made between IT mishaps and genuine cyber attacks.
5. As part of communication and outreach efforts it would be useful to have a centre of intelligence-sharing such as the Virtual Task Force (which is used to coordinate approaches to cyber crime among financial institutions) for those who need to be informed so that decisions can then be made and information disseminated both vertically and horizontally between affected organizations.
6. Greater public awareness would help acclimatize a wide audience to cyber security issues and encourage individual precautions and security measures. Public messaging must recognize the existence of disparities and varying levels of awareness.

Building a cyber security culture

1. Greater organizational and public awareness is essential to inform and shape an effective national cyber security culture.
2. Examples exist of best practice but these need to be standardized across the private and public sectors. Government and industry will need to work together to develop accepted models of best practice as well as common terminological standards.
3. Incorporating cyber risk into existing risk cultures will mean considering it together with wider organizational risks. It needs to be a standard item on the agenda rather than being seen as distinct, inscrutably complex and 'someone else's problem'.
4. A robust cyber security culture should be responsive to the rapid pace of change in technology and innovation.
5. Providing commercial and professional incentives for the private sector and broader society could positively stimulate and shape a national cyber security culture and motivate better practice, but this will require more effective communication and outreach strategies which simultaneously convey the nature of the problem and appropriate responses and precautions in a way that is accessible to a diverse array of organizations and individuals.

1. Introduction

In the United Kingdom and internationally, awareness is developing rapidly of the challenges associated with society's dependence on information and communications technology (ICT). This dependency has arguably become the defining feature of a modern, interconnected and knowledge-based society and economy. The machinery of government, the critical national infrastructure (CNI) and the provision of essential services such as water, gas, electricity, communications and banking are all ICT-dependent to a large degree.

With this dependency can come vulnerability to aggressors, criminals and even the merely mischievous. Public and media attention is frequently drawn to tales of hacking and espionage and there is persistent interest in and concern about the rapid growth of cyber crime such as banking fraud and identity theft. The discovery of the Stuxnet virus in 2010 provided evidence of the growing sophistication of cyber threats and the potential damage they can cause to governments, organizations and critical infrastructure around the world.[1] The WikiLeaks controversy in 2010 added another dimension to the debate, with the exposure of thousands of US diplomatic cables prompting further questions about the value and vulnerability of politically sensitive information. While some condemned the leaks as dangerously irresponsible, others defended them as examples of radical cyber-enabled transparency.

From the perspective of policy-makers, analysts and commentators it is clear both that the sense of threat and vulnerability is mounting and that the public and private sectors are all under increasing pressure to 'do something' about cyber security. The United Kingdom National Security Strategy (NSS)[2] and Strategic Defence and Security Review (SDSR)[3] released in October 2010 promoted cyber security to a Tier One risk to national security, and its high status was reinforced by the UK government's allocation of £650 million to cyber security and resilience. The challenge, however, is not for governments alone but for society as a whole. The UK Ministry of Defence's December 2010 Green Paper entitled 'Equipment, Support and Technology for UK Defence and Security' noted that

> perhaps the over-riding characteristic of cyberspace is the pace of change. Not just technological change, but changes in business processes and social interaction that this supports; changes in impacts that these in turn engender, and vulnerabilities that these expose; and contingent on all of these and on other – non cyberspace – factors the change in threats.[4]

But what can and should be done to meet this challenge? And who or what is best placed to tackle the problem, given that the vast majority of critical infrastructure is privately owned?

In 2009, Chatham House, in conjunction with Detica Ltd, assessed the development of cyberspace as a problem for national security in a report entitled *Cyberspace and the National Security of the United Kingdom*.[5] Describing

1 Eric Chien, Nicolas Falliere and Liam O Murchu, 'W32.Stuxnet Dossier Version 1.3', *Symantec Security Response* (November 2010), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, accessed 10 January 2011.

2 UK Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: The Stationery Office, October 2010, Cm 7953), http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf, p. 29, accessed 13 January 2011.

3 UK Cabinet Office, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (London: The Stationery Office, Cm7948, October 2010), http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf, p. 47, accessed 13 January 2011.

4 UK Ministry of Defence, *Equipment, Support, and Technology for UK Defence and Security: A Consultation Paper* (London: The Stationery Office, December 2010, Cm 7989), http://defenceconsultations.org.uk/Cm7989.pdf, p. 54, accessed 3 March 2011.

5 Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House, March 2009), http://www.chathamhouse.org.uk/research/security/papers/view/-/id/726/, accessed 14 January 2011.

cyber security as a 'complex security challenge', the authors argued that it amounts to a system-level challenge to society that in turn requires a system-level response by society as a whole. What was needed, in the authors' view, was the development of a national (and eventually international) regime or culture of cyber security in order to ensure that 'the activities of different agencies and bodies complement each other and are mutually reinforcing, rather than conflicting'.[6] This argument prompted another set of questions: (1) who or what should be involved in developing this national cyber security regime; (2) should this regime be centrally directed or more loosely coordinated; and (3) at what level politically, and by which agency or department of government, should the leadership and organization of this regime take place?

Building on this earlier work, it is these questions, in the context of pervasive cyber dependency, that the present report addresses. Before a broad and inclusive national cyber security culture can be developed – and before it becomes possible to ascertain whether such a culture should be driven centrally or allowed to develop organically – the first task must be to identify the stakeholders who should be involved in society's system-level response and to analyse the environment within which they operate. Yet there is currently no authoritative, publicly available picture of the UK national cyberspace stakeholder environment that could provide the basis for an informed, non-governmental contribution to the development of a national cyber security culture or policy framework. This report aims to fill that gap.

Examining the critical national infrastructure

The UK government's 2009 *Cyber Security Strategy* provides a starting point; it argues that it is 'vital for the Government, organizations across all sectors and the public to work together if we are to achieve our collective cyber security aspirations'.[7] The document points out 'the need to engage closely with key stakeholders to strengthen existing cross-cutting partnerships, and form new ones where required, with industry, civil liberties groups and other stakeholders, internationally and in the UK'.[8] This approach was reiterated in the SDSR 2010, which stated that the 'response must be led by government, but in doing so we must leverage the knowledge and resources of the private sector – including those parts of the private sector that own and operate large elements of the critical cyber infrastructure'.[9]

The critical infrastructure includes critical *cyber* infrastructure but it encompasses many other organizations as well, and a coherent cyber security strategy must be inclusive if it is to be effective. This report uses the definition of critical national infrastructure provided by the Centre for the Protection of Critical National Infrastructure (CPNI)[10] and the UK *Cyber Security Strategy*. This categorization of CNI includes communications, emergency services, energy, finance, food, government and public services, health, transport and water. This raises the question of what should be considered 'critical' in a modern society; does the spread of ICT technologies also expand the definition of CNI? It could be argued convincingly that the criticality of companies such as Google or Amazon to the functioning of a complex modern economy should be acknowledged by governments.

Measuring awareness of the challenges: methodology

Having identified broad elements of the national cyber constituency, this report assesses the breadth and depth of awareness of cyber security among the various stakeholders in the CNI. In order to achieve some form of stakeholder management of cyber security in terms of national policy and

6 Cornish et al., *Cyberspace and the National Security of the United Kingdom*, p. vii.

7 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (London: TSO, Cm 7642, June 2009), http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf, para 1.15, p. 10, accessed 2 November 2010.

8 Ibid., para 3.20, p. 20.

9 UK Cabinet Office, *Strategic Defence and Security Review*, 2010, p. 47.

10 CPNI, *The Critical National Infrastructure*, http://www.cpni.gov.uk/about/What-is-the-CNI/, accessed 21 February 2011; and UK Cabinet Office, *Cyber Security Strategy of the United Kingdom*, p. 9, note 7.

organizational responses, it is essential to establish how CNI companies and organizations assess their dependence on ICT and how they respond or prepare to respond to threats.

This in turn gives rise to a number of questions. Do the various agencies, bodies and individuals involved recognize the significance of the cyber stakeholder status that has been conferred upon them? How do they identify and measure their cyber dependencies, and how effectively do they manage the risks and mitigate the potential vulnerabilities associated with these dependencies? How much discussion of cyber security is there within and between the different sectors? What are the acknowledged areas of best practice in cyber security? Are there significant differences in analysis and practice across the stakeholder community, and can or should these differences be reconciled? And finally, how willing are these organizations to be drawn into or even associated with a government-led cyber security initiative?

In order to answer these questions and gauge the levels of awareness of senior individuals about the nature of cyber-related dependencies and vulnerabilities within their organization, primary research was conducted through a series of semi-structured interviews with senior executives from the CNI (including government departments and agencies) responsible for risk management, group security, finance and other general responsibilities. The decision was made not to follow the relatively predictable path of interviewing representatives of ICT departments. Instead, the purpose of the interviews was to gauge the level of cyber security awareness at board level in order to form a more accurate impression of the organization's overall understanding of, and response to, cyber security.

Although there is a growing wealth of literature on cyber security from a wide range of public- and private-sector sources, for this study emphasis was placed on first-hand experiences and anecdotal evidence as a more accurate reflection of organizational responses, mitigatory strategies and general levels of cyber security awareness. Through this process it was possible not only to identify disparities in the availability and distribution of information, but also to gain a better perspective on the mutual expectations of government and private-sector CNI and the role that each side plays and expects the other to play.

To cross-check some of the emerging findings against a control sample, one interview was conducted with a large charity – a closely related but technically non-CNI organization. Wherever possible, interviews were conducted personally by two Chatham House researchers, and for scheduling or geographical reasons some interviews were conducted by telephone. All interviews took place under the assurance of strict confidentiality, and for this reason and for the purposes of any subsequent research and analysis code numbers were allocated to each organization consulted (see Box 1).

Box 1: Codes allocated to CNI organizations interviewed

3	Defence company
9	Government agency – health
11	Independent cyber partnership organization
14	Major financial institution
18	Emergency service provider
27	International charity
28	International insurance group 'A'
33	Law enforcement agency
38	International insurance group 'B'
44	Major utility
49	International communications company
52	Major high street bank
58	International investment bank
63	Government stakeholder – 2012 Olympic Games
65	Government agency 'A'
71	International security software provider
77	Defence company
81	IT advisory organization
87	International utility
94	Government agency 'B'

During the research phase, 100 organizations were approached and twenty interviews were completed. The level of response to interview requests could be considered a research finding in its own right – perhaps indicative of a lack of senior management familiarity or interest in cyber security. Nevertheless the sample size would be considered statistically insufficient to draw many firm and decisive

conclusions from the observations and research findings. In order to substantiate the qualitative judgments made in the course of the interviews, a quantitative analysis of the data (i.e. interview notes) was conducted by a third-party organization using established business analysis tools; a proprietary combination of 'Design for Six Sigma' and 'Quality Function Deploy'.[11] The results show a high degree of correlation with the qualitative judgments and serve to validate the research findings.

Structure of the report

Chapter 1 provides an introduction to the research project, its scope of enquiry and the overall findings. The remaining chapters of this report are arranged as follows.

Chapter 2 begins by examining senior management perceptions of dependency and vulnerability within the cyber security environment. It questions how coherently these issues are dealt with by CNI organizations, and what responses are being developed or should be developed. It finds that in many cases organizations have some idea of their cyber dependencies but have only the barest idea of what constitutes a cyber vulnerability or what impact that vulnerability could have were it exploited.

In Chapter 3 the management of these cyber dependencies is analysed. It asks what level of planning or coordination is undertaken to keep these dependencies from becoming vulnerabilities, and what level of risk organizations are willing to accept along the way. The research findings show that although public- and private-sector organizations (particularly larger ones) would be expected to have a clear sense of best practice, continuity planning and risk management, in numerous instances this is clearly lacking.

Information communication and outreach are examined in Chapter 4. Once dependencies, vulnerabilities or emerging threats have been identified, how is this information communicated to the relevant organizations so that risks can be weighed in an informed manner? It is apparent that the lack of an authoritative communications strategy and infrastructure is severely inhibiting a coherent CNI response strategy, although some information-sharing groups have demonstrated progress.

Chapter 5 widens the scope of analysis to examine the importance of a culture of cyber security. Regulatory and legal pressures enable only limited progress; what is needed is more fundamental change in societal perspectives and behaviour. The use of business process models appears worthwhile here, to improve cyber security in a manner similar to other areas of business and avoid treating it as unique and inscrutably complex.

The annexes provide further information to support the research. Annex A contains the research methodology; who was approached and why, as well as the outreach and response statistics and a small selection of the more insightful negative responses.

Annex B contains the interview format and questions; how did the interviews proceed, what questions were asked and how were the responses processed and analysed in a consistent manner?

Annex C contains a third-party analysis of responses from 14 private-sector CNI organizations. As noted above, this was undertaken to augment the research methodology with a robust quantitative analysis of the interview results.

Annex D provides additional interview results that are concerned largely with ICT infrastructure. These points are considered useful but are excluded from the main report since they were not the primary area of concern.

11 See Annex C.

2. Perceptions and the Threat Landscape

Before a thorough analysis of cyber dependencies and vulnerabilities can be conducted it is important to understand better the threat landscape with which CNI organizations are confronted. The mere cyber-enabled dependency of one organization upon another is commonplace in almost every facet of the CNI. These dependencies are myriad and therefore unexceptional. Yet there is no doubt that cyber threats are proliferating and are seeking to exploit such dependencies and vulnerabilities. The first step is to identify and examine the threat actors in some detail. Once a threat is identified a response must be developed, but this is clearly a very complex process when coordination is required between multiple organizations.

The processes of threat identification and response are coloured by the perceptions of those making decisions and allocating resources to mitigate the threat. How do they perceive the landscape and what weight do they give to potential risks? A primary differentiating factor between secure and non-secure organizations is evident in how their leaders perceive the cyber threats that could potentially turn cyber dependencies into vulnerabilities. Although these dependencies vary between sectors, it is instructive to gauge the level of awareness these leaders have of evolving cyber threats and how are they preparing to meet the challenges presented by a dynamic and increasingly interconnected environment. Is cyber security an issue that merits the regular attention of senior management within the CNI or is it relegated to the IT department? In too many cases it is obvious that the complexity and proliferation of emerging threats are overwhelming the ability of CNI organizations to develop and implement a coherent and strategic response.

A changing environment

It is widely recognized that knowledge-based economies are in a period of transition into an era of near-total dependency on ICT, with few opportunities to return to non-ICT modes of operation. The sheer speed of change in cyberspace is opening new frontiers as well as adding often unseen dependencies and vulnerabilities. For many in the public and private sectors this change is accompanied by a significant growth in cyber-related threats, which pose widespread and systemic challenges. Whatever their sector, ICT-dependent organizations must be prepared for a challenging and rapidly changing environment. Across the CNI organizations involved in this study there was broad acknowledgment that cyber security threats are not homogeneous [interview codes 33, 63, 71, 87 – see Box 1 on p. 3] and are in some cases growing more quickly than they can be measured [11, 52, 58]. The threats are seen to be widespread and unaffected by geographic location. In this way it could be said that there is no 'postcode' dimension to cyber threats, and that they can affect users of cyberspace regardless of their physical location [11].

> 'Cyber security is quite a boring subject and we need to make it attractive'
>
> Law enforcement agency interviewee

As one measure of change, as of early 2011 the data flows from mobile devices were estimated to be close to surpassing the data flows to personal computers [71]. This linked in with the assessment of one investment bank which considered the main cyber challenges of the near future to be mobile device security and the implications

of cloud computing [58]. These are perhaps some of the more prominent contemporary trends. Yet both large and small cyber dependencies and vulnerabilities often go unrecognized in management strategies and risk registers. In some cases cyber risks may be obscured and hidden inside the wider supply chain, several steps removed from the analysis and decision-making centre of a given organization.

Proliferation of threats

In addition to the pace of change it is also clear that cyber threats to public and private organizations are becoming increasingly significant. These threats are broad in scope, ranging from increases in the levels of sophisticated malicious software (malware), to disruptive activity by online activist and nationalist groups, to organized crime and sophisticated electronic espionage operations aimed at stealing valuable and/or strategically significant intellectual property. The range of threats is vast, and includes the hypothetical possibility of an attacker acquiring the ability to damage a financial institution by infecting a large percentage of cash withdrawal machines with malware, as noted by a large investment bank [58], or linking hijacked computers in robotic networks (botnets) to attack a target *en masse* or, as a more flexible alternative, 'hiring' a botnet from a third party to achieve the same aim.

Among commercial organizations the exponential growth in cyber crime is a frequent concern. There is a feeling that these threats can affect any financial sector and will continue to grow in severity [11]. In many ways, cyber crime is becoming an adjunct to 'traditional' crime, a constant background problem for commercial organizations. One financial institution reported that the volume and sophistication of threats are now outstripping the organization's capacity to respond [52]. Other related organizations commented that East European criminal gangs appear to pose the biggest threat [33] and noted increasing collusion among organized criminal groups that are targeting the financial industry in particular [58]. This conjunction of cyber threats and organized crime is particularly pertinent to the 2010 UK *National Security Strategy*, which considered them to be distinct entities and placed them in separate risk 'tiers'.[12] It is worth questioning whether this distinction remains valid when there is clearly an increase in cyber crime that could be considered both 'serious' and 'organized'.

While there is a growing realization of the external threat posed by hackers and criminals (organized or otherwise), several organizations reported a significant increase in the threat from insiders, with one investment bank reporting concerted efforts to 'groom' employees to compromise their corporate loyalty [58]. Another bank pointed out an internally generated potential vulnerability of a different kind, noting that its IT department regularly faced pressure from employees (particularly financial traders) for less restricted access to the internet [14]. These internal vulnerabilities and threats are compounded by external ones, and in combination they are exacting a growing cost. As a measurement of the losses being sustained by the financial system, one government law enforcement agency noted that for every $100 in the financial system, one-tenth of one cent is believed to be lost through fraud [33]. When aggregated across the trillions of dollars flowing annually through the global economy, these figures reveal a significant impact on public and private balance sheets and help to explain why financial e-crime is so lucrative and therefore attractive.

Many of these attacks are launched using malware, and one security software provider reported a tenfold increase in malware attacks, rising from 6,000 detections per day through its systems in 2008 to 60,000 per day in 2009 [71]. It also noted that its threat event horizon and response time had shrunk to just three months between detecting an emerging threat and developing a strategic solution, and that attacks by new variants of known malware types had forced the development of costly tools that must now provide a countermeasure within fifteen minutes of initial threat detection [71]. However, this proliferation of malware has been contested, with one European Union report noting that it is due in part to the way in which

12 UK Cabinet Office, *A Strong Britain in an Age of Uncertainty*, p. 27, accessed 15 May 2011.

malware is counted. It described how advanced 'server-side polymorphic malware' configures itself for each machine it infects, and these slightly different variants are in some cases counted individually by security software companies, thus increasing (or even 'over-reporting') the annual levels of malware.[13] Nevertheless, these threats and others are adding complexity and ambiguity to the landscape.

Continuing uncertainty

Many CNI organizations are uncertain how to manage emerging threats and need their own understanding expanded and reinforced. In some organizations the perception of threat is at such a high, and perhaps exaggerated, level that the initial operating presumption is that a significant loss of service should be treated initially as the result of a cyber attack rather than a software or hardware failure [87]. This posture is exacerbated when there is limited awareness of the nature and impact of the threat and the harm it can cause, meaning that many organizations remain under-prepared and vulnerable to predation. Determining what information is accurate and which threats are genuine is crucial to shaping the most appropriate and effective response. It is also essential in order to know what is actually being threatened and what therefore must be prioritized.

> 'There is too much bad stuff in cyber space, and it's blended too much with the good'
>
> International security software provider interviewee

One international utility noted that, according to internal estimates, only 3–5 per cent of its data are sensitive material it would not want to see on the front page of a newspaper. This is the material that must be protected, and to try to protect everything would simply be too difficult [87]. This kind of granular assessment methodology assists significantly with preparing informed responses, but it tends to be the exception rather than the rule. An interviewee at one major high street bank was distinctly lacking in optimism, noting that (in terms of evolving threats) there seemed to be 'no natural predator to the bad guys' and predicting gloomily that 'we have crossed the Rubicon; we are not going to keep ahead of this' [52].

Across both public and private sectors there were a number of cases that demonstrated a lack of awareness, a sense of complacency or an exaggerated perception of the threat. This makes it important to ensure adequate information is available for organizations to develop a more agile risk response. It also suggests that there does not yet exist a formal system of threat intelligence collection, analysis, integration and dissemination (a 'rich picture') that could become the single coherent source of cyber threat knowledge within the United Kingdom. Most notably with regard to cyber threat perceptions, there appears to be no coherent picture or sense of what constitutes a vulnerability, or what impact that vulnerability could have, that is sufficient to catalyse a coordinated large-scale response across the public and private sectors.

Developing strategic responses

A coordinated response to emerging cyber threats and exploitable vulnerabilities is necessary to lay the foundations for sustained growth and stability. One international security software provider noted that an opportunity could be opened for the United Kingdom to become known as a centre of excellence, particularly in the secure storage, management and responsible distribution of data [71]. Yet to develop this capability would require a concerted effort, not least in higher education, where advanced cyber security classes are generally not made available in university curricula. The raw talent is out there but needs to be nurtured. The training process can be lengthy; the same organization reported that in some cases it could take up to five years to train an antivirus operator [71].

13 Ross Anderson, Rainer Bohme, Richard Clayton and Tyler Moore, *Security Economics and the Internal Market* (European Network and Information Security Agency, 2008), http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec, pp. 31–33, accessed 20 April 2011.

In many cases cyber security training in the workplace remains ad hoc, even though it is apparent that emerging threats require both increased agility among cyber security experts and closer dialogue across organizational hierarchies so that a more comprehensive risk picture can be developed. Would it therefore be possible, or appropriate, to establish nationally accepted levels of training or qualifications designed to produce leading cyber security experts? In some cases cyber threat mitigation is a generational problem, and this is where a focus on wider public education could prove useful [58], perhaps in a manner similar to demographic-specific messages from the National Health Service (NHS). However, significant changes would be required in public awareness and engagement before any such potential could be realized with regard to cyber security.

There is little doubt that the rapid pace of change in cyberspace is a complicating factor in efforts to engage the public. But the speed of change is unlikely to slow and the capacity of cyberspace to create surprises is unlikely to shift to any significant degree. Both must be accepted as 'a feature, not a bug, i.e. an intentional facility, not a mistake' in the design of the internet.[14] This is a central reason for both the significant benefits and the daunting challenges that have proliferated since its inception. Research and investment are necessary to meet constantly evolving threats, and skilled personnel will be required to implement the necessary measures. However, the security software provider mentioned above expressed frustration that, despite the fact that it possessed significant technical capability that could potentially be used for national benefit, these resources are at present not being exploited to the fullest extent within a government-coordinated national response [71].

This observation prompts an obvious question: is government the right entity to coordinate a national response given the scale of the problem and the different dimensions it presents? How much of this should be the responsibility of government, and is it even possible for government to create a coherent contemporary picture of vulnerabilities and threats in cyberspace? Would the creation of a 'rich picture' be a significant step towards catalysing an adequate response, and should organizations in the private sector play a leading role in that response given that they own the vast majority of the CNI? If not by government, how should information about cyber threats and risks be shared and disseminated?

At present there is a multitude of threat information sources available for consumption. These come through many avenues such as specialist media and government briefings and alerts from security software companies. However, there remains a sense of dissatisfaction in the CNI with the quality and quantity of information-sharing between the public and private sectors, with the government being perceived (rightly or wrongly) as more willing to solicit information than to share it. Consequently many CNI organizations have a strong desire for more accurate and up-to-date information on rapidly changing and emerging threats. For many enterprises threat integration seems to be done 'at the coal face', with a distinct lack of uniformity between CNI organizations regarding the management of risks, both cyber- and non-cyber-related.

Summary

The research shows a rapidly shifting landscape that is leaving many decision-makers several steps behind. Risk assessments in the CNI are becoming gradually more granular and responsive, but there is uncertainty over what an efficient information-sharing mechanism would look like or what would constitute an appropriately strategic response. The lack of awareness and misperceptions regarding emerging threats (leading to an over- or under-reaction) call for a balanced approach in which cyber security should in equal measure be threat-informed, dependency- and vulnerability-focused and effect-driven. This approach would appreciate more fully the variability and dynamism of the threat landscape.

14 John Naughton, 'The internet: everything you ever need to know', *The Observer*, 20 June 2010, http://www.guardian.co.uk/technology/2010/jun/20/internet-everything-need-to-know, accessed 26 June 2011.

It would lead to better understanding of the nature of cyber-enabled dependencies (both internal and external) and a focusing of efforts on the potential vulnerabilities that might arise. And ideally it would go beyond looking at inputs ('our antivirus protection is up to date') and look instead at the effect those inputs are achieving ('are we safer or has the threat merely shifted focus to another part of the organization?').

If balance cannot be achieved in these three areas (threat, effect, vulnerability), then inconsistency on one side of the virtuous triangle is likely to result in unreliable or inappropriate deductions on the other two. This could cause difficulty in estimating the possible effect of a cyber attack on an organization, and appropriate risk management could become far more difficult.

3. Managing Cyber Dependencies

The management of cyber security varies considerably between and within organizations and sectors. For some, it rates highly on the standing agenda at board meetings. In other cases middle management encounters difficulty and even resistance in raising the visibility of cyber security with senior executives and leaders. Although it is discussed with increasing frequency at senior levels of leadership in the public and private sectors, in a number of instances it appears that the management of an organization's cyber security policy is not delegated (in a constructive managerial way) but is deliberately pushed below the boardroom level in order to remove a complex and baffling problem from sight. All too often our interviews showed that cyber security issues were treated as the sole preserve of a chief information officer (CIO) or the ICT department despite their relevance to the organization's business strategy as well as its reputation and balance sheet.

As the likelihood and impact of cyber attacks on the CNI and wider society have become more prominent in recent years,[15] so the problem of cyber security has also risen to the top of national risk agendas. In the United Kingdom, the 2009 *Cyber Security Strategy* and the 2010 *National Security Strategy* both illustrate this trend. It is clear that cyber attacks that could exploit ICT dependencies and vulnerabilities now comprise a substantial part of the risk landscape for public and private organizations. In a rapidly evolving security environment, these organizations would benefit from developing measures to manage their cyber dependencies. One starting point for this can be found in the ideas and practices associated with risk management and mitigation.[16]

Although one might expect public and private organizations, particularly the larger ones, to have a clear sense of best practice, continuity planning and risk management, this is not always the case. Despite talk of threats and tactical responses, there appears to be limited discussion of the integration or adaptation of established best practice. In particular, sharing of views within and between government and the CNI regarding what should be 'natural', 'inherent', or 'regulated' in the electronic environment occurs all too rarely. This can result in imprecise or narrowly focused guidelines for the development of cyber security management and information distribution structures.

Across the CNI there is growing acknowledgment that cyber security and cyber dependencies are matters that should be more closely considered by all levels of an organization and in all business areas. One security software provider reported that as recently as 2009 some of its clients considered cyber security to be little more than an 'IT problem' [71], and a respondent from a government health-related agency stated that 'nobody here talks about cyber security. One doesn't hear it among employees' [9]. One communications company noted that these issues were best approached holistically, and that problems tended to arise when senior management separated technical issues from security issues and missed their interlinkages [49]. To avoid this, one option is to strengthen the link between the tactical (technical and security) and strategic (senior management) levels by encouraging greater dialogue. CNI organizations also acknowledge the need for enhanced dialogue and cooperation between the public and private sectors to manage the diverse challenges of cyber security more effectively.

15 The 2010 National Risk Register listed cyber attacks on data confidentiality as relatively high-likelihood but low-impact risks while cyber attacks on infrastructure were seen as relatively low-likelihood but relatively high-impact risks, http://www.cabinetoffice.gov.uk/sites/default/files/resources/nationalriskregister-2010.pdf.

16 For the purposes of this paper risk management is understood as the identification, analysis, prioritization and mitigation of harm or potential harm to the structure, functioning and purpose of an organization.

Public–private cooperation

The first challenge of cooperation is to ensure that public and private organizations have broadly compatible approaches to cyber security. The establishment of the UK Office of Cyber Security and Information Assurance (OCSIA) and the Cyber Security Operations Centre (CSOC) has gone some way to improving relations between government and CNI organizations regarding their exposure and responses to cyber threats. These are in addition to existing institutions such as the Centre for the Protection of National Infrastructure (CPNI), the Communications-Electronics Security Group (CESG) and its parent organization the Government Communications Headquarters (GCHQ, which also houses CSOC). Organizations such as the recently formed Defence Cyber Operations Group (housed within the Ministry of Defence) will also be a key component of the national mechanism. However, as shown in the previous chapter, awareness of the threat varies widely across the CNI.

Another concern relates to high-level national governance and partnership. While organizations are aware that cyber security is an area of emerging national policy, many have been critical of what they view as the fractured condition of the government's machinery for managing and ensuring cyber security. A major financial institution, among others, expressed a wish for the many agencies involved in cyber security to be more 'joined up' and did not consider the UK government's cyber security strategy to be centrally directed and organized [52].

Whether or not this view is accurate and reasonable, it is shared by many of those interviewed, suggesting that key sectors of British society remain generally unaware, uninformed or unimpressed about the development and scope of the government's cyber security policy and strategy. These issues prompt questions about an awareness gap in public-sector outreach and partnership. Does the government view its partnership efforts as sufficient largely because it has spoken to CEOs rather than IT departments? And when government discusses these matters with senior management in the CNI, is its guidance and advice couched in the accessible language of 'risk registers' or 'risk mitigation' rather than terms used by IT specialists such as 'advanced persistent threats'?

In addition to heavy dependence on ICT, both sides are dependent upon each other for various needs. But what level of partnership is understood to be implicit by each side when it talks about public–private partnership? What portion of the private sector interprets government overtures towards 'partnership' as truly in search of 'alliance'? And do the majority of senior government officials agree with those who have expressed concern that industry expects government to step in and solve the majority of cyber security issues? The answers to these questions will reveal much about the compatibility of public- and private-sector conceptions of cyber security.

Dependency

Given that society is increasingly dependent on cyber-enabled technologies for many functions of daily life, it would be reasonable to assume that these technologies are underpinned by redundancy, resilience and close scrutiny in order to avoid harmful disruptions. Yet certain kinds of scrutiny, such as methodical audit practices, regarding ICT in a wider business environment appear to be rare in the area of cyber security. Ideally these wider audit practices would assess up-stream and down-stream dependencies ('Who are we dependent upon for services and who is dependent upon us?'). This audit methodology appeared only in the financial sector, where the loss of ICT would represent immediate and measurable impact. This indicates a strategic deficiency in general boardroom-level understanding of cyber dependency and provides some evidence of a systemic failure in risk management in a worryingly large proportion of the sample cases. In one case senior management had little sense of the company's unmitigated cyber dependencies, and when ICT staff raised concerns they were told that no further funding was available [18]. In addition, there was no strong testing regime or contingency planning in place to stress-test potential responses to cyber vulnerabilities.

Beyond an organization's immediate concerns, perception of the need actively to assess critical business dependencies such as supply chains is generally lacking. Although one organization actively identifies and grades its critical

business relationships according to impact and then reviews them regularly to identify new dependencies [28], this does not appear to be a common practice. The directors of a large insurance company reported that they did not know how they should manage or mitigate vulnerabilities caused by the dependency on certain systems, services or relationships [38]. In addition to this internal uncertainty there is even less understanding of how critical business partners are addressing cyber security issues.

Within the financial sector there are some isolated examples of close attention being paid to the performance of suppliers and the security of their ICT systems. This included on-site inspection of systems at the first degree of separation (i.e. a supplier or producer connected directly to the auditing organization), and remote audit of systems at the second degree of separation (i.e. a supplier or producer two steps removed from the auditing organization) [52]. Within the same sector a single example was found of a mature cyber security messaging strategy, with different messages adapted for board members, middle managers and cashiers [58]. However, such strengths seemed to be heavily dependent upon the innovation and energy of the managers who introduced and oversaw their development.

> 'Organizations are bad at defining what they want people to do'
>
> International security software provider interviewee

There appears to be a trend of organizational reliance on contractual terms regarding continuity of supply (with an expectation that services will be provided and the prevailing assumption being that 'IT will work' within the chain of dependency). This represents the chief method of assurance for many organizations, and reveals a high level of dependence on single providers with poor backup modes of supply, and in some cases no backup whatsoever. Some organizations have not even conducted basic contingency planning to cope with cyber-related dependencies. This level of contractual faith – occasionally bordering on naivety – may explain why dependency and risk are not assessed more fully. While one sceptical individual from an international insurance group insisted that one must 'never make assumptions; never rely on a good reputation' [28], it was interesting that this same organization omitted cyber security as a standing board agenda item.

Drawing comparisons between the public and private sectors, there is surprisingly little commonality in the way critical dependencies and relationships in both sectors have been first mapped and then transposed into a dynamic system whereby they could adjust to the rapid changes in the environment and be audited on a regular basis. Within these organizations, where should responsibility lie for mapping these relationships and communicating with the appropriate parties? Ideally this sort of system would identify and grade critical relationships and dependencies according to the predictable consequences of a breakdown of that relationship on the organization concerned. This assessment would then allow for more effective risk prioritization and mitigation. It would involve a regular review of these relationships and dependencies for relevance, in order to make a cost-benefit assessment of the merits of protecting them, and to identify new interactions and re-prioritize as necessary. While there is some overall understanding of the need to undertake analysis of this sort, in only one instance – an international insurance group – was such an appraisal conducted in a robust and replicable manner [28]. The need for more sophisticated risk management is clear and indicates there is a niche waiting to be filled more systematically.

Risk

The research showed that risk-modelling practices varied across organizations, as did expectations of what this modelling could or should provide. More fundamentally, it is apparent that some organizations or their representatives have a less than rigorous understanding of the mechanics of risk assessment, and *how* and *when* risk can be mitigated by investment of appropriate resources (i.e. equipment, personnel and decision-making time and capacity), let alone any concept of the agility needed to mitigate the threat. In many cases although risk manage-

ment is a feature of CNI organizations and appears to be practised, the practical understanding of the term in relation to cyber security appeared to be limited and in some cases confused. It also appears, however, that very few organizations are familiar with or experienced in making 'balance of probability' judgments which would allow proportionate and efficient countermeasures first to be prepared and then to be implemented once a cyber security incident has occurred. Effective risk management requires sufficient awareness of the risks at the right level of seniority even if the responsibility for action is then delegated to another level, and in the sample surveyed high levels of inconsistency were observed.

One of the most striking observations was the lack of awareness of an organization's vulnerability to the high-level consequences of an ICT failure in another element of its value or operational chain (i.e. the business implications of a cyber attack that could cause the cessation of critical supplies or processes). This is the mapping that was referred to in the section above, and lack of mapping makes it difficult to undertake the fundamental tasks of risk management: prioritizing cyber-related risks in order to identify those that can be tolerated, those that can be avoided or displaced in advance and those for which there must be mitigation responses (which places demands on already finite resources).

Although cyber security issues are at least noted in corporate risk registers, management of cyber risks seems rarely to be systematic or consistent. In one case concerning an emergency service provider, the prospect and consequences of a serious ICT failure were not considered to be a major risk to the functioning of the organization – a seemingly complacent outlook which was reflected in the reported absence of a robust contingency planning regime [18]. A large insurance group indicated that its board did not examine ICT risks on a regular basis. Policy was reviewed from time to time, and at that moment ICT risks were considered. Disappointingly, however, a comprehensive assessment tended to take place only after a significant cyber attack [28]. A large utility reported that it considered its ICT risk-modelling process to be fully mature, yet it was retained and managed at the ICT management level rather than at a more senior level [44]. In the light of these examples it appears that organizational risk-management principles and practices (and any complacency in this area) stem in large part from the lack of understanding of the threat/effect/vulnerability triangle (as explained at the end of Chapter 2).

Reflecting the financial stringency of the current economic climate, an organization's appetite to absorb higher levels of cyber risk often appears to be more pronounced than might be expected. This risk position is normally caused or exacerbated by a need to retain profit despite poorer trading conditions, leading to a lack of resources and capacity (equipment, personnel and processes) for mitigating cyber security vulnerabilities. There is a clear contradiction in the position taken by many of the organizations involved in this project. For the most part they demonstrated growing awareness of increasing cyber security threats even though understanding of systemic challenges was lacking. Yet these same organizations were willing, for a variety of resource and other reasons, to accept an unexpectedly high level of cyber security-related risk. There was even a tendency, as noted earlier, to distance the handling of this risk from the authority and responsibility of the board or senior management. This distancing appeared in many cases to be a result of inattention to cyber security issues as opposed to intentional neglect. As a result awareness, while growing, often remained at a low level. Increased risk, in other words, was met with both diminished resources and diminished interest. Given this imbalance it remains unclear what would prompt a reassessment of these priorities, yet it is evident that a reassessment is needed and that alternative ways of approaching the issue may be required. An organization may need to experience an unpleasant surprise or shock before senior management fully grasps the pervasiveness and potential impact of cyber security threats.

Alternative management responses

There are number of management responses that can be adopted with regard to cyber dependency and risk. Some organizations have a considered and reasoned approach that eschews a conventional risk-based perspective. One

advocated a homeostatic dynamic in which the system (or in this case a management structure) can maintain a steady state while external factors vary in type and intensity [71]. Thus in times of financial stringency the business instinct might be to decentralize and delegate because of the need to reduce overhead costs, yet when an adverse incident occurs the instinct would be to centralize the response because senior management is held responsible for any losses.

Another organization noted the tension between the tendency towards centralization and the need for the agility that decentralization can provide [11]. It is clear that maintaining the capability required to enable both a centralizing and a decentralizing response may not be appropriate for all sectors, given the organizational flexibility that would be required, but it could be a useful option for some. Having identified the potential motivating factors in these two different management responses, the primary challenge is to manage the intensity and effect of the stimuli in order to maintain stability and predictability in cyber risk management. This dynamic was described as a natural condition in which there are continual variations in senior management's desire to exercise influence [71].

The research provided many indications of the absence of common standards and processes in the management of cyber security risks and consequently of pronounced qualitative differences in the understanding of these risks. Whether or not common standards exist is only partly relevant. Even if they exist in a usable form, if they are too difficult to find, then they are not being used to maximum effect. In one instance, where a significant source of government information was uncovered, the credibility of the data was compromised as they were severely out of date, with guidance documents several years old. Even if these documents had been reviewed in the interim, there was no 'review date' appended to give reassurance that the advice they contained was still relevant, authoritative and useful.

Box 2: Emergency planning

Given their expertise in emergency planning one might expect the emergency services to have in place the appropriate arrangements to import specific and codified best practice in cyber-related (and other) contingencies, for example drawing from guidance supplied by the UK Cabinet Office Emergency Planning College (EPC) at Easingwold. But these do not seem to have been applied for cyber security.

The case of one emergency-service provider provides a valuable illustration of the inflexibility of management structures. Following a cyber incident it became clear that uncertainties existed in the continuity of no fewer than six of the organization's critical business supply chains including the power supply, critical medical items and communications. As this incident was related and reflected upon, the senior manager commented that 'the more I sit here, the bigger the can gets' [18].

Moreover, there were some instances of less than optimal practice driven by the pursuit of efficiency savings. For example, this organization's back-up servers were housed in the same building as the main servers, with no apparent realization that, far from mitigating risk through robust business recovery planning, the organization was essentially deluding itself and generating a false sense of security. This risks putting the organization in a worse position than having no recovery plan at all. Senior management in one department was reluctant to allocate resources for training in the management of specific contingencies (in this case concerning chemical, biological, radiological or nuclear incidents) on the grounds that staff would be away from their normal duties and performance targets would suffer.

This evidence suggests that, if a training regime does exist, the EPC's guidance, no matter how worthy, does not appear to be achieving the effect required. Short-cuts in performance and cost-saving measures fundamentally undermined the overall ability of the emergency-service provider to function robustly and effectively.

If regulation were to become the government's preferred route to manage CNI cyber risks, then several aspects of the current environment should be considered. One utility complained that its regulator made decisions on costs and profits, and attempted to ensure that ICT networks were resilient, but did not appear to have sufficient cyber expertise for its policies, decisions and recommendations to be considered well-founded and authoritative [44]. A government agency closely linked with cyber security policy said it opposed over-regulation because, in its experience, this would lead to a well-rehearsed condition of 'audit dodging' (which we take to be a condition of superficial compliance with a set of regulations or performance indicators, while effectively ignoring the underlying policies and the spirit of the initiative), and that when regulators were in the room 'people don't talk' [94]. This observation is consistent with the conclusion of Chatham House's 2009 report that a tight, centrally driven and highly regulated approach to cyber security will impede a regime-style approach to cyber security across the departments, agencies and organizations of government and the wider CNI.[17]

By this view, over-regulation would stifle the tempo of the response which, to be effective, requires good communication, trust and transparency among all the parties concerned. However, the more finely calibrated regulatory powers lodged with one IT advisory organization do appear to have achieved some success in mitigating the loss of private data [81]. Clearly there is a balance to be struck between regulation and control on the one hand, and devolved authority and flexibility on the other. The likelihood is that regulatory powers will be enhanced after an incident, or in the face of an emerging threat, and then eased over time in quieter periods. This introduces the possibility of more effective public-sector cyber security outreach and information-sharing, in order to make regulatory initiatives feel less burdensome and to increase compliance.

Summary

There are clear inconsistencies, gaps and omissions (through ignorance or negligence) in the way in which organizations are managing cyber dependencies, particularly in assuring the functioning of critical business relationships. These inconsistencies provide ample opportunity for threat actors to exploit an organization's vulnerabilities directly or to leverage the dependencies between organizations to attack indirectly. There is also growing acknowledgment that these dependencies should be more closely considered at all levels of an organization, and not just within the ICT department. Senior management need to be involved and in doing so must avoid over-reliance on contractual terms of service. It should work with departments and employees to recognize and learn how to address cyber dependencies and vulnerabilities. This heightened awareness about the nature of cyber threats will also assist with the development of more finely calibrated risk assessments.

Nonetheless there appears to be no authoritative 'rich picture' being generated centrally that would underpin a comprehensive understanding of which threats need to be addressed, by whom and when. Although there is a widespread common understanding that something needs to be done, most response mechanisms appear fractured and uncertain. Various competing priorities are in play, not least the tension between finite resources and an increasing organizational appetite for accepting cyber risk in a search for greater profits. The management of cyber dependencies through the development of standards of best practice, continuity planning and risk management would all be steps in the right direction, but these steps should be communicated effectively and in a way that allows all stakeholders to participate in the dialogue.

17 Cornish et al., *Cyberspace and the National Security of the United Kingdom*, p. 21 and Chapter 4.

4. Information Communications and Outreach

Both the 2010 UK National Security Strategy (NSS)[18] and the Strategic Defence and Security Review (SDSR)[19] are clear in their assessments of the importance of cyberspace to national security. As yet, however, it is not entirely clear that there is a coherent thread of vision and leadership, combined with developed stakeholder engagement and communications strategies, that would foster an informed political debate on the issue of cyber security as a national challenge. If the government cannot itself be coherent about cyber security then it is unlikely to be able to communicate effectively to others. This places a premium on high-quality and purposive communication, which must be part of any comprehensive response to cyber threats. Communication regarding 'knowledge of the threat' among CNI organizations is identified in this report as an area where government has the opportunity to convey relevant intelligence to the CNI, in an accurate and timely fashion, in order (a) to use effectively for the benefit of the CNI the information only government possesses and (b) to assist in swiftly limiting the effects of a cyber attack.

Addressing vulnerabilities and dependencies will require government engagement not only with the CNI but also more widely with society. But the process of communication and outreach cannot be simply a one-way street from central government out to the surrounding environment. Effective communication also requires an openness to listen. However, some organizations consider themselves to be self-taught where vital information about cyber threats and challenges is concerned, seeking it through the 'jungle telegraph' (i.e. through informational conversations and exchanges with colleagues, peers and other organizations) and private research [44]. As a result they are less interested in communicating with government, as they see little benefit in doing so.

A lack of effective communication (in this case, on the source and target of the cyber threat) can also cause problems in other areas. In many cases the absence of accurate threat information causes organizations (public or private) to analyse an attack or disruption of service in inconsistent and incompatible ways. Some organizations will assume a worst-case scenario (i.e. that they are under attack) while others may perceive it as a technical glitch. The outcome is predictable; in a widespread attack that affects different parts of the CNI, having one organization reporting a technical failure while another one describes the same incident as a cyber attack will promote disorder from the outset, reminiscent of the confusion that initially surrounded the response to the London bombings in July 2005, with early reports of power surges that obscured the actual nature of the attacks.[20]

Communications strategy and infrastructure

An effective outreach approach to cyber security requires implementation of a communications strategy that facili-

18 'Activity in cyberspace will continue to evolve as a direct national security and economic threat, as it is refined as a means of espionage and crime, and continues to grow as a terrorist enabler, as well as a military weapon for use by states and possibly others.' UK Cabinet Office, *A Strong Britain in an Age of Uncertainty*, p. 29, accessed 17 January 2011.

19 'The rapidly changing nature of these threats and opportunities to the UK demonstrates the need for a flexible cyber security response, in line with the principles of our adaptable posture and the National Security Tasks and Planning Guidelines. That response must be led by government, but in doing so we must leverage the knowledge and resources of the private sector – including those parts of the private sector that own and operate large elements of the critical cyber infrastructure.' UK Cabinet Office, *Securing Britain in an Age of Uncertainty*, p. 47, accessed 17 January 2011.

20 House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005* (London: The Stationery Office, May 2006, HC 1087), http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf, p. 7, accessed 10 January 2011.

tates dialogue about both the threat and the rationale for a given response, and that enables this information to be communicated horizontally between affected or responding organizations. The broad aim of a communications strategy should be to improve situational awareness across cyber security stakeholders, making it possible for risk to be identified and assessed and for the chosen response to be received with the widest possible understanding.

Effective foresight and preparation of this sort can only be achieved if, in addition to a communications strategy, there is a communications infrastructure in place. Yet there is ample evidence that such an infrastructure is largely deficient, if not entirely absent. One financial institution noted that it had a good relationship with the police but the relationship did not encompass cyber security issues. Despite the emergence of novel methods of attack that were increasingly difficult to detect, the organization had to go out and search to learn more about the threats it faced [58]. When organizations rely on informal communication networks this not only indicates the lack of a proper communications relationship with central government, it also reinforces the idea that there is no communications infrastructure in place.

Critically, without this infrastructure (whether this is the 'pushing of information' to recipients, or making information available to 'pull' from a centralized repository) and without firm efforts to ensure that the information can reach those who need it in a timely fashion, there will be no confidence that all concerned are benefiting from the best situational awareness available. Ideally, the environment should be retuned to establish a condition of awareness in organizations that are seeking to reduce their vulnerabilities; a good level of awareness will result in greater sensitivity to the issues at hand. With better awareness, organizations would become more intelligent clients to their advisers, and less prone to being driven into short-term tactical reactions by simple anecdotal evidence or the latest dramatic cyber security incident.

At best, a condition of comparative ignorance is likely to result in opportunity costs and inefficiencies. An organization with minimal awareness of cyber threats could spend either too much or too little on security measures, wasting resources or opening itself to attack, and in either case placing itself at a disadvantage compared with more well-informed organizations or competitors. At worst the outcome of these communications deficiencies will be a chaotic environment in which parts of the CNI will either over-react or be complacent, rather than responding appropriately to the actual emergency. Both a cyber communications strategy and a robust infrastructure are necessary to build greater awareness of the threat environment and encourage a culture of risk management, and the entire process will be aided by the use of more finely calibrated tactical communication mechanisms and structures to implement this process.

Communication management

In terms of information communication, both internal and external, there appears to be an absence of authoritative management structures that would supply basic data needed to respond to cyber threats. In addition to details of the threat itself, any other useful information such as lessons learned or best practice seems to be located in pockets, with organizations being required to unearth them in a continuous process of discovery. Even if this information could be bought together into a single environment, the data would need to be communicated or made accessible in a uniform way to support the development of a broad and inclusive culture of cyber security.

The scope, quality and immediacy of information required vary widely, and are usually a function of the size of the organization concerned and other factors such as geographical spread, cultural considerations and the challenge of ensuring high-quality (e.g. encrypted) communications over long distances. For example, the group risk manager of an international communications company explained that he spent a significant amount of time looking at possible geo-political motives behind cyber attacks on the company's systems, including those in the United Kingdom and more than two dozen local markets [49]. Yet although important and timely information could be acquired in the course of his research – information that could be of high value to the cyber

security community – there was no obvious mechanism for disseminating this kind of intelligence and integrating it into an efficient, closely coordinated national or international intelligence management system.

The formation of a suitable structure to enhance this process would be complex given the many inhibiting factors involved (e.g. the multiplicity of stakeholders, the reluctance to share commercially sensitive information and the unwillingness to let any single organization lead or be seen to lead this process), but the current situation seems to be in need of improvement. This information and outreach management problem is not unique to the public and private sectors. Discontinuities in threat-related communication are apparent in the third sector where there is a regulatory requirement for charities to report electronic attacks to the Charities Commission [27]. However, in some cases information concerning cyber attacks, having been reported to the commission via established procedures, is not redistributed to the wider charities community to encourage greater awareness of threats and rationalize defensive and protective actions. This would suggest a 'black hole' – or even a series of them – in the management and dissemination of cyber security-related information and warnings.

One useful addition to the communications environment would be formal 'lessons learned' procedures that can be shared within and between organizations (and with regulators), both public and private. However, it is clear that although some organizations have thought carefully about identifying and sharing best practice in cyber security, in many other cases formal and standardized lessons-learned processes were notably absent, and there appears to be little willingness to share information of this nature with similar organizations.

Internal and external CNI outreach

In order to achieve more complete societal engagement and to instil a much-needed sense of community among everyone confronting cyber threats, a communications strategy could be operated on two parallel paths – internal and external. Within certain organizations there was found to be evidence of mature communications policies and practices that conformed to this standard [28, 58]. But they were far from uniform or consistent among similar entities or sectors. As a result, organizations may tend to under-report cyber security incidents on the grounds that while information would be requested and absorbed by higher authorities, this would become a one-way channel, and nothing beneficial would be given back. Several organizations indicated that they felt little incentive to expend resources on developing reporting lines up to national intelligence and security authorities when there was little or no perceived return on investment [27, 52, 71].

Many members of the CNI and wider commercial sector do not feel this area is especially well managed by the government in spite of initiatives such as the national Information Exchange Groups (IEGs). IEGs, sponsored by the CPNI, are forums for sharing cyber-related information on threats and vulnerabilities within key components of the CNI. They have at times been regarded as ineffective [87] and interested more in discussion than in action [44]. The representative of one international utility felt that most government cyber security resources were targeted at protecting the government and, despite the frequent mention of an increasing risk to both public and private sectors, little advice on preventive action was issued to the latter [87].

There is a range of views on how cyber security-related messages (where they exist) are being disseminated, both vertically and horizontally, between corresponding stakeholders in different parts of the cyber security response community. There appears to be little coherence in CNI communications management, although some successful initiatives have emerged. One financial organization encapsulated this neatly, commenting that government strategy did not feel 'joined-up'; it was still very 'stove-piped' and the organization did not feel it was looked after by the UK government [52].

Some central government organizations are taking a more active approach to cyber security communication than these comments might suggest. The CPNI, for example, maintains close relations with industry, and GCHQ organizes classified briefings to heads of companies in the private sector and to others on a regular basis. Yet

the representative for the international utility noted that a briefing it had received from GCHQ was 'just vanilla' and felt that it contained 'empty promises' [87]. It is difficult to determine how the receiving organization utilizes the privileged information imparted during these briefings. Is the information highly restricted or is it distributed in suitable format through organizational channels to maximize its value? If such briefings are given on the understanding that the intelligence shared is to be retained at a personal level by those who attended the briefing, then arguably these outreach efforts could be largely ineffective.

Box 3: The charity sector

One example of resourcing issues can be found in the charity sector. Following the Haiti earthquake in January 2010, appeals had swiftly attracted criminal elements perpetrating large-scale fraud through a variety of cyber attacks [27]. Prompt and efficient information-sharing between charities in this (entirely predictable) threat environment could provide benefit disproportionate to the resources employed. Although financial losses in the charity sector may be quantitatively small compared with those in the financial sector, the psychological harm involved could be equivalent, with some private donors suffering significant loss of hard-earned savings. The lessons learned from the Haiti appeal primarily concern the need for constant vigilance and can be applied to a wide range of charity appeals.

Virtual Task Force

In terms of horizontal communications across corresponding levels of the CNI, the financial crime Virtual Task Force (VTF), which is described in the ACPO E-Crime strategy,[21] serves as a useful model for self-starting groups. Its structure is designed to allow organizations to exchange information and respond to threats in an environment of collective protection and mutual self-help. The VTF consists of staff from major UK-based financial institutions along with some of the major network providers.

Although they compete vigorously with one another, the operating principle of the VTF is that financial institutions should share information about cyber security threats. Generally, information shared behind closed doors remains private to VTF participants. Protocols for information exchange are drawn from CPNI and IEG templates, and all members share in the benefits of the overall system. This helps to increase the speed of the response and shortens the time between the detection of an emerging threat and the unified implementation of counter-measures across the sector.

By the end of 2010 the VTF had begun to show distinct and measurable benefits in the financial sector where, despite its current ad hoc nature, it has helped to disrupt a number of criminal campaigns directed against the UK banking sector. This approach makes it possible for cyber security to become a non-competitive, self-help practice, with no single member being able to advertise a better security response as part of its appeal to new customers. If it is extended to other sectors, the VTF idea might also prevent incidents such as that in which a well-known computer virus infected the network of one of the UK's major police forces, yet the information necessary to enable a sector-wide response was not shared with other emergency services [18].

One possible adverse consequence of the VTF initiative, however, is that the deliberate dampening of competitive spirit in the name of a comprehensive and more effective response to cyber threats removes an important stimulus to improving individual responses in order to achieve competitive advantage. As a result, even though the development of processes and technologies to mitigate cyber threats might be admirably uniform across a sector, innovation and response might occur at a slower pace than if the usual rules of competition still applied.

21 Association of Chief Police Officers of England, Wales & Northern Ireland (May 2009) *ACPO e-Crime Strategy, Version 1.0*, http://www.xact.org.uk/information/downloads/internet/Ecrime_Strategy.pdf, p. 9, accessed 11 January 2011.

Public communication

Public communication strategies regarding cyber security are essential but need to be managed with care. Any assumptions that the public is a single, tractable entity are likely to prove false, and messaging needs to be geared to specific groups and communities to ensure that advice is as relevant and timely as possible. Information is disseminated most effectively by identifying the target audience and establishing clearly the *motive* that drives the communication, then by defining the *message* that needs to be transmitted, and finally by selecting the most appropriate *medium* of dissemination. The goal of a focused large-scale communication strategy of this sort would be explain the challenges of cyber security without exaggerating fears. Such a strategy could also emphasize the long-term benefits that would accrue from greater awareness and education (such as a more competitive workforce) [71].

This goal is not without difficulties. How can the importance of cyber security be made personally relevant to a large and diverse group of people without overstating the dangers? One UK government agency noted that established practices already exist in relating specific messages to different segments of the public [65]. For example, the style and content of messaging from the NHS in communicating matters affecting those aged 16–25 differ markedly from those messages intended for, say, elderly people. This could be a useful methodology if adapted with care, making it possible to distribute segmented and specific information about potential dangers in cyberspace without making sweeping declarations that might exaggerate the threat, or not be understood by a significant portion of the target audience.

One possible avenue for improved communication and outreach is the development of a cyber security 'brand' that reaches out to as much of its market as possible (public or private sector, or society at large). This 'brand' could become the cyber security selling message and would aim to improve awareness and establish a solid foundation of basic good practices. Branding is a specialist skill, however, and one at which government does not always excel. The needs of the customer must be carefully considered when designing a messaging strategy in order to distribute information efficiently while avoiding dissonance. In this respect cyber security is no different from any other large-scale government messaging exercise. In many cases the value delivered by this messaging would take the shape of timely information on cyber threats coupled with tangible recommendations for mitigation. But it remains true that the target audience will only pay attention if the message delivers something of value. If it is perceived to be lacking in substance or disconnected from reality the 'customers' will ignore it. For example, a warning system in the form of colour-coded alerts would be both ineffectual and widely ignored – and rightly so, as it would serve only to increase tension while providing no suggested course of action.

In terms of outreach the Information Commissioners Office (ICO) appears to have a mature strategy, particularly for small and medium-sized enterprises (SMEs). The ICO focuses on data protection, and its 2009/10 annual report noted that its helplines handled over 214,000 calls (a six per cent increase over the previous year).[22] It has an easily comprehensible online service and is clearly capable of handling large volumes of enquiries, a majority being from SMEs and private individuals. It will probably be difficult for the ICO to extend its remit to handle more general cyber security issues without significant extension to its responsibilities (and corresponding funding). However, as public outreach policy is developed by the government, it may be useful to model a government-to-public interface along the lines established, seemingly successfully, by the ICO. It appears that the UK government is aware of the need to convey the message in a more effective manner. Public communication regarding cyber security remains an under-developed area and the government is actively considering new communications strategies [65].

22 Information Commissioner's Office, *Information Commissioner's Annual Report 2009/10: Upholding Information Rights in a Changing Environment* (London: The Stationery Office, July 2010, HC 220), http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf, p. 26, accessed 11 March 2011.

Summary

There appears to be a general lack of uniformity in the way in which cyber security intelligence, information and practices are communicated from central authorities to society more widely, although some initiatives show potential for further development. The traditional existing communications channels seem to have neither the scope nor the agility required of an authoritative response system that must keep up with the pace of change in cyberspace. There is significant scope for improvement in this area, with opportunities for communication strategies that would deliver value and bring both short- and long-term benefits.

This process does not work uni-directionally from central government outwards. Effective communication and outreach also require willingness by other parties to listen. The VTF is one example of a dynamic and interactive communications process – in this case led by the private sector but with government participation. Regardless of whether communication and outreach are directed internally or externally, the process must be underpinned by a strategy. This should provide the foundation for a communications infrastructure that can distribute granular and targeted messages to the desired audience. Currently such an infrastructure appears to be deficient in many segments of the public and private sectors. This suggests that a more fundamental cultural change may be necessary to drive large-scale transformation in cyber security outreach and awareness.

5. Building a Cyber Security Culture

The near-universal accessibility of the internet and the speed and dynamism of this environment have created a condition in which opportunities for malicious, criminal or hostile activity can be exploited with ease. In contrast to this, the pace of cultural progress towards greater awareness of cyber security remains slow, and poor behaviour affects many users including third parties that may have little recourse to remedial action. Cyberspace is a novel environment for the tens of millions of new users around the globe who experience it for the first time each year. Among them there will always be some who are less adept and security-conscious than most. The ability of the public sector to nudge society towards improved internet security behaviour is limited but not insignificant, and in some areas this ability is improving. In many cases those who craft and debate cyber security law and regulation are themselves relatively new users, and as their awareness and understanding of cyberspace increases this will be reflected in government.

If the creation of a robust culture of cyber security is the desired end state, then agreement upon standards of best practice for the public and private sectors, perhaps based on established models of business process, should be a logical step towards this goal. Yet even best practice often appears to be lacking, and senior managers within the CNI are struggling to keep up with the needs of their organization while providing a safe operating environment. They are attempting to keep ahead of emerging threats but are often thwarted by a poor security culture both inside and outside their organizations. The necessary tools and standards are available but convincing users they need to adopt and use these measures consistently is often the most difficult task. Inward-looking analysis and behaviour, together with a preoccupation with the protection of an organization's area of interest or 'turf', also work against a more comprehensive and inclusive culture of cyber security. Functional boundaries, perhaps within a sector such as financial services, or between competing commercial ventures, can be easily identified and ruthlessly exploited. Once a tangible loss occurs, a primary need is to minimize further losses and develop strategic countermeasures as fast as possible.

> 'We have to protect customers from themselves to some extent'
>
> International communications company interviewee

From a commercial perspective there are also structural deficiencies in cyber security culture. Incentives are often unbalanced, as noted by one member of the financial industry who called for a change in the nature of the contract between banks and their clients [52]. This respondent reported a lack of motivation for banking customers to adopt good security practices, due in large part to a lack of penalties for poor behaviour. This bank recognizes that the public perception of the cyber threat is low, and now assumes that its customers will freely surrender all personal information (through social networking sites, etc.) needed for the process of online banking identification. Although the bank underwrites the vast majority of online losses (due to fraud etc.), the respondent made a case for the need for greater individual responsibility, arguing that individuals who display poor internet behaviour and fail to provide themselves with basic online security products should be held more accountable for their losses, despite the resulting legal complexities [52].

Business process and practice

Despite these challenges the prospect is not entirely bleak. There is – admittedly isolated – evidence of a robust and effective approach within a number of organizations. For example, there seems to be a culture of privacy and data security in the charities sector, where the assured anonymity of donors has for a long time been seen as paramount [27]. However, these strengths all too rarely amount to what could be considered a culture of cyber security and are undermined by significant weaknesses or gaps in awareness. Approaching these strengths and weaknesses from the perspective of a business process model is useful; this enables cyber security to be placed in context as one organizational task among many, but a task where failure can have a significant effect on the organization. For every other critical function of an organization there are business processes in place to optimize and standardize a particular function, whether it be a financial audit, merger and acquisition or research and development. Repeating and honing these processes creates efficiency, and ultimately a culture of doing things the 'right way'. Why should cyber security be any different?

Cyber security issues permeate nearly every corner of the CNI, and should not be separated in any meaningful way from larger organizational processes. In other words, cyber security cannot sit apart from other functions and needs. It should be regarded as what it is – integral to nearly every function of an organization – and not as a task overseen only by the ICT department.

Across a wide range of public- and private-sector organizations, various exemplars of good, improving and poor practice regarding *awareness* and *management* of cyber security can be identified within the ranks of senior management. These two metrics are a robust indicator of the maturity of an organization's cyber security culture. The extracts below represent a collation of carefully selected comments and observations gathered during interviews to illustrate the range of practices (good, improving and poor) that emerged from a wide range of sectors. Analysis of this sort is useful because it filters cyber security through a business process lens, examining cyber issues with the same critical eye and in the same manner as non-cyber-related aspects of the public and private sector.

Good practice reflects a high level of awareness of cyber dependencies within senior management, an understanding of the supply chains that an organization both contributes to and is dependent upon, and a longer-term perspective for monitoring risks and responding to threats.

- Business protection and IT security are considered at a very high level. [38]
- Critical business relationships are identified and graded according to the effect they would have if their provision of service was lost. These relationships are regularly reviewed for relevance and any new interactions identified. [28]
- A high street bank is moving towards the use of multiple methods to establish the identity of its online customers. [52]
- [The use of a lesser known suite of applications] 'gives us an inherent level of protection as it is less common than similar […] products and therefore less visible to attack.' [27]
- A security software provider takes a five-year view on cyber security and has an internal think-tank which monitors technological trends. [71]
- 'We have a policy for cyber lessons learned and pass findings to our workforce.' [58]
- There is one person in group security whose sole responsibility is to raise security awareness, for both employees and external clients. [49]
- 'We identify the corporate material that must be protected at all costs. To try and protect everything is just too difficult.' [87]
- 'We have mapped our cyber-related dependencies. This is aided by the fact that various partners have good relationships with each other, and we see practical benefit in maintaining these relationships.' [63]
- A large utility conducted a cyber security exercise that included a simulated distributed denial of service (DDoS) attack. [44]
- 'We use customer advisory boards comprised of senior people chosen from among our IT clients.' [71]

- 'We risk-assess our supply chain, and for the most critical suppliers we physically go onsite and conduct an audit.' [52]

Improving practice shows a more limited awareness of cyber dependencies within senior management and uncertainty as to how to develop and implement risk mitigation and response strategies.

- Cyber security issues have come onto their risk register only recently and they are becoming more rigorous with their risk management. [87]
- More corporate resources are being devoted to cyber security issues. [87]
- More boards have cyber-related business continuity in their high-level view, though this has only started to happen in the past two years. They know resilience matters but are uncertain how to manage it. [71]
- 'A potential ICT-related strike is a concern for us, and we are meeting with similar organizations to form a contingency plan.' [18]
- A communications company conducts close scrutiny of clients, especially those in foreign countries. This scrutiny can involve UK government officials, who sometimes tell the company CEO that information that disqualifies the company from working with a potential client is classified. [49]
- A large insurance group has terminated some business relationships with suppliers owing to their non-compliance with IT risk management standards. [28]
- A security software provider uses customer advisory boards comprising senior members chosen from among its clients. [71]
- A government stakeholder in the 2012 Olympics has a process in place for testing its cyber dependencies. [63]

Poor practice demonstrates minimal awareness of cyber dependencies and limited understanding of risks compounded by a lack of attention by senior management.

- There does not appear to be a relevant cyber security strategy within the organization. [63]
- The CEO knows the organization is heavily cyber-dependent but does not know where to find appropriate guidance regarding risk mitigation. [18]
- Chief information security officers (CISOs) still come largely from a technical background and this needs to change. No one seems to know what the discussions between CISOs and the board should look like as they tend to speak different languages. [71]
- There is a high level of internal cyber vulnerability, yet few decision-makers know precisely where the vulnerabilities lie. [94]
- There is little senior-level awareness or understanding of cyber dependencies. [49]
- No cyber-related due diligence was carried out during a recent acquisition. [44]
- 'Organizations have a tendency to go through a checklist of "cyber security measures" (antivirus, firewalls, updates, etc.) and then stop there. They don't always know where their data reside, and this makes it difficult to quantify risk accurately.' [71]

The instances of poor practice show deficiencies that are both non-systemic and systemic. Some poor practices could be improved significantly through the streamlining or implementation of basic information and communication processes, while others require a more fundamental and systemic change in organizational culture.

These extracts also show numerous instances of good or improving practice, but they are scattered between different stakeholders and are not applied consistently throughout the CNI.

Though good practice in one industry sector might not necessarily translate into another, there is a problem when the 'good' is not being identified, collected and shared in a meaningful way, and this allows the 'poor' to proliferate. If all CNI stakeholders, and indeed the wider public, had the incentive to coalesce around similar standards of good practice in cyberspace, it could prompt a quantifiable improvement in security. There are two core problems: first, there does not seem to be a common repository for this information; and, second, even if some sort of repository does exist, there appears to be no communications strategy to make that information available to organizations that wish to improve their cyber security processes.

Box 4: Best practice in action

One international investment bank [58] has integrated numerous elements of cyber security best practice into various levels of its management structures, and the case provides a broad range of examples for other organizations to emulate. Within the organization the following points were demonstrated:

- Cyber is a risk-management exercise and falls in the top three board-level concerns.
- There is broad accountability for cyber issues, and it is on the agenda of senior management.
- Service-level agreements with utilities and other critical business relationships have been identified.
- Cyber security policy falls under the umbrella of traditional security arrangements rather than being an adjunct to them.
- Extensive due diligence is conducted with IT, procurement and finance as well as critical third parties, and over the past decade the high-risk scenarios that could affect business have been considered.
- The board is involved in walk-throughs for contingency planning, and the effect that a cyber attack would have on the company has been tested.
- Training is conducted from the board level to the shop floor, and includes involvement of directors in scenario-based training for cyber attacks such as 'denial of service'.
- The organization is working on more age-specific cyber security education for the younger elements of its workforce.
- It monitors online sources of information such as Twitter for brand awareness as well as for attacks on its reputation, and passes intelligence back to the appropriate authorities.
- A system is in place to distribute notices quickly, such as via SMS and office monitors, for a variety of emergencies or incidents including cyber attacks.

The unexpected

In addition to the implementation of best practice, effective cyber security requires the agility to handle unexpected challenges. It is not enough to tick all the necessary boxes. A mature culture of cyber security would pull together and harness the strands of workplace training, business processes, organizational memory and creative thinking. In isolation, any one of these is insufficient to handle the wide range of cyber vulnerabilities, which often arise suddenly in areas that defy prediction. The following two cases illustrate instances of cyber security vulnerabilities that caused surprise.

One organization's internet service provider owns a major ICT network control centre that had been built on a former landfill site. While this was arguably a laudable contribution to corporate social responsibility and the green agenda, an unpredicted consequence has been regular evacuations of the site owing to unacceptably high levels of methane gas [18].

As a consequence of low-level criminality seeking to capitalize on the buoyant scrap-metal market, regular theft of valuable metals such as copper cabling is resulting in interruptions to data flows and information systems [44]. In early 2011, for example, the whole of Armenia lost internet service after an elderly woman in Georgia accidentally cut a fibre-optic line while scavenging for copper cable.[23]

Some of these issues are revealed and can therefore be confronted only when they arise. Other potential

23 Tom Parfitt, 'Georgian woman cuts off web access to whole of Armenia', *The Guardian*, 6 April 2011, http://www.guardian.co.uk/world/2011/apr/06/georgian-woman-cuts-web-access, accessed 15 May 2011.

problems may be more apparent to a select group of people within an organization, but owing to poor communication the information is not disseminated effectively and the entire organization suffers as a result. Many of these dependencies and vulnerabilities could be mitigated more effectively by building additional resilience into cyber security systems and procedures. With hindsight this seems obvious enough. Yet given the rapid pace of change and increasing complexity in cyberspace, surprises will doubtless frequently continue to occur.

Summary

Those responsible for managing cyber security risks would acknowledge that 'unknown unknowns' can be experienced no matter how rigorous the planning for every conceivable eventuality. However, the response mechanisms in any organization or group of organizations need to contain a high level of cooperation, capability and agility to cope with these risks. At the strategic level these response mechanisms should incentivize and standardize cyber security best practice while gradually minimizing poor practice. This can be done through heightened senior management awareness and management of cyber security. These mechanisms should provide the capability for a rapid transition from a condition of surprise to active incident management and then to restoration of services. The unpredictability and speed of change in cyberspace call for an organizational culture that is confident yet healthily paranoid – simultaneously respecting the ability of cyber aggressors and remaining constantly vigilant while retaining confidence in its internal agility and decision-making skills.

Additional work is also needed on improving the culture of cyber security at the societal level, with clearer guidance on what it means to be a 'good internet citizen'. It is a telling and sobering indicator of a poor security culture when financial institutions assume their customers will freely surrender all personally identifiable information. Progress towards improving this culture would serve to establish a kind of immunity to the most widespread and common threats, while also educating a broad group of users about emerging threats. The development of this culture can be improved through policies that seek to nudge societal cyber security behaviour in the desired direction while remaining flexible enough to deal with a rapidly shifting environment, and there is still significant progress to be made in this area.

6. Conclusion

When this policy research project was launched it was expected there would be a reasonably uniform level of awareness across the UK's critical national infrastructure of the implications of increasing levels of dependence on ICT. Had this overall consensus been discovered, then the project would have pursued its original purpose, which was to develop a methodology to map the types and relative criticality of ICT dependencies within the UK CNI stakeholder environment. It would then have been possible to explore the extent and the significance of CNI vulnerability to cyber threats, where 'cyber vulnerability' is understood as an unknown or unmitigated ICT dependency.

However, at an early stage in the interview process, and having uncovered a disparate patchwork of knowledge, capabilities, processes and attitudes, it became clear that to continue along the original path would have resulted in information that would soon become out of date, publication of which would not have contributed materially to the public policy debate. The project therefore shifted focus to identify how the issue of cyber security was being managed in the CNI in order to establish a knowledge baseline that would better inform future policy direction. As a result, the authors of the report found themselves examining a business and public policy environment that is in transition, from a condition in which cyber security was the responsibility of the organization's ICT department, to one in which it is increasingly an issue that merits (or should merit) regular attention at boardroom level.

The authors have argued earlier that the only effective response to large-scale cyber security challenges is one in which society as a whole is fully informed of the risks inherent in cyber dependency and is closely coordinated in its response.[24] The present study revealed, however, a marked lack of uniformity and consistency in policy and practice, such that it would be very difficult to describe the UK as possessing anything approaching a society-wide response to cyber vulnerabilities and threats.

The quality and effectiveness of cyber security management vary dramatically between and within CNI sectors. The evidence suggests an environment in which the core motivation remains short-term self-interest, rather than one guided either by mutual self-help or by centralized policy (and the effective communication of that policy). Where cyber security is concerned, the CNI is characterized by organizations doing the best they can. But in many cases they lack the skills or knowledge to identify and mitigate the harm caused by a wide variety of emerging threats in cyberspace, and this is compounded by their systemic dependency on other vulnerable actors in the environment.

Awareness

In *Cyberspace and the National Security of the United Kingdom*, a simple metaphor was used to show why a societal-level response should be developed. If security could be likened to a perimeter wall (and it is acknowledged that security is more likely to be achieved by defence in depth than by a linear barrier), then in the first instance the wall does not need to be built to a great height but it must be continuous and unbroken.[25] The present study has shown, however, that reality is rather less tidy. Instances of best practice in cyber security were found, yet these practices are sporadic and are scattered among organizations in various sectors. A small number of organizations do seem to understand the multitude of challenges posed by heavy dependence on ICT systems and have

24 'We argue that the regime offers the most suitable basis for a national cyber security strategy which must include (yet not direct) a wide variety of actors, agencies and stakeholders, and which must be sufficiently agile (yet without losing focus) to meet a rapidly evolving and transforming security challenge.' Cornish et al., *Cyberspace and the National Security of the United Kingdom*, p. 30.

25 Ibid., p. 17.

in some cases begun to adapt themselves appropriately. But these beneficial measures have been accompanied by other practices that can only be described as irresponsible, insecure and damaging. In some cases this qualitative disparity was found to occur within a single organization.

Given the scale of the task, the UK government appears to have recognized the need for a concerted response. The 2009 *Cyber Security Strategy* argues that it is 'vital for the Government, organizations across all sectors and the public to work together if we are to achieve our collective cyber security aspirations'[26] and highlights 'the need to engage closely with key stakeholders to strengthen existing cross-cutting partnerships, and form new ones where required, with industry, civil liberties groups and other stakeholders, internationally and in the UK.'[27] This approach was reiterated in the 2010 *Strategic Defence and Security Review*, which stated that the 'response must be led by government, but in doing so we must leverage the knowledge and resources of the private sector – including those parts of the private sector that own and operate large elements of the critical cyber infrastructure'.[28]

This proposed architecture involves the government, but cannot be led by it. The nature of the problem is ingrained and systemic to the extent that a central authority can merely provide incentives to encourage a societal remedy but cannot mandate it. In simple terms, the £650 million allocated to cyber security (over four years) by the SDSR cannot 'fix' or 'secure' the critical national infrastructure, though it can help to catalyse greater attention to these issues within government. This places a significant burden of responsibility in the hands of those who confront these issues most immediately: organizations in the private sector. The development of such architecture would place the government in the position of a provider of knowledge, advice and encouragement while using regulation in a measured way (remaining mindful of the possible unintended consequences such as observation of the letter of the law but not the spirit).

While the question of cyber security appears to be ascending in boardroom consciousness, many senior managers still seem largely uninformed about the nature of cyber threats to their businesses and – just as significantly – do not know where to turn for high-quality information on threats and responses. Few, if any, organizations do everything right where cyber security is concerned. And very few interviewees felt their organizations were coping adequately with the current security environment. Equally, the research found no organization which did everything wrong; after all, any such organization would soon fall victim to digital Darwinism. Most organizations present a mixed performance – some good practice and some bad – and it is this confused condition that presents the greatest challenge for those seeking organizational transformation to meet emerging cyber security challenges more effectively. This also makes it difficult for government agencies and advisers to approach the cyber security environment as one that is relatively stable and can be systematically improved. Faced with this mixed record, government might legitimately ask 'where do we begin?'

One early finding was the lack of engagement by prospective interviewees, with uptake being slow and resulting in a smaller sample than desired. That said, it is worthy of note that UK government departments and agencies were quick to come forward and participate in the project. Commercial organizations engaged less and produced a lower response percentage. Nearly half (48 per cent) of those invited failed to reply in any form, despite a series of prompts. This leads to the conclusion that, for whatever reason, some organizations may wish to remain detached from the debate for as long as possible, which would be inadvisable in such a fast-moving environment. Or they may be averse to engaging with a subject that they perceive to have the stamp of central government upon it, which would be unfortunate give the centrality of the private sector to the cyber security debate.

With appetite for business risk (including that related to cyberspace) rising in some sectors owing to the current financial environment, it seems that without a consol-

26 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom*, para 1.15, p. 10, accessed 2 November 2010.
27 Ibid., para 3.20, p. 20, accessed 2 November 2010.
28 UK Cabinet Office, *Strategic Defence and Security Review*, 2010, p. 47.

idated threat picture (provided by whatever the best source might be), appropriate resources are unlikely to be devoted to cyber security. Paradoxically, this tendency is in contrast to the perceived increase in cyber-related threats that all respondents were fully willing to acknowledge. However, if a single threat picture could be generated, it would be reasonable to assume it might result in a more uniform security response, even from those organizations that have no regular contact with central government's cyber security authorities, and even if the totality of the response were more limited than in former, less economically constrained times.

The senior managers involved in this study indicated their wish to become more 'intelligent customers', feeling that at present they speak a 'different language' from their ICT professionals and are thus unable to consider cyber-related issues in sufficient depth [33]. This demonstrates that a deeper behavioural transformation might be required, with the needs of business driving cyber security, rather than the other way around. In only three instances did the research reveal a comprehensive system of mapping, for the benefit of the board, of an organization's cyber-related business dependencies [52, 58, 63]. This shows there is not only a difference in language that is spurring confusion but also a lack of awareness regarding cyber dependencies.

Elsewhere, there were found to be some highly developed audit processes that examined cyber dependencies, with one instance where a business relationship with a supplier was terminated owing to its lack of compliance with cyber-related contingency requirements [28]. There were also isolated findings of comprehensive contingency planning and related exercises, in some cases involving board members, but this was not routine. Overall no single source of information was found which provided the best practice necessary for a business-process approach to managing cyber dependencies. In addition, many organizations were willing to rely on contractual arrangements for the provision of ICT services and considered these contracts to be all that was needed to ensure continuity of critical supplies or services. This reliance on contracts, and the attendant lack of urgency regarding resilience, appears to be misplaced in circumstances where a loss of service would exact a heavy economic or reputational cost on the affected organization. In fact, such losses are likely to fall outside the scope of contractual obligation, making the lack of resilience even more damaging.

Engagement

The view presented by private-sector participants in this study is that the UK government's cyber security organization is fragmented and does not show an identifiable lead. Nevertheless, there were acknowledged to be a number of promising strands such as the IEGs sponsored by the CPNI – despite some criticism, participants considered these to be an initiative of continuing relevance – and the development of the VTF concept. And despite the perceived fragmentation it is to government that industry tends to turn for intelligence and information, particularly on high-level cyber security threats.

There was consequently a consistent demand from the private sector for a deeper and more meaningful engagement with government, and a plea to be more trusted as part of the national response. Some respondents saw their participation in this study as a way to voice that plea. The private sector also wanted to know how best to communicate its concerns to government without falling foul of information 'black holes', or an unequal condition in which it offered much but felt as if it received little. In the view of some organizations, the government's response resources are focused too closely on its own stakeholders rather than wider UK society.

Official representatives of the UK government have acknowledged that there is scope for improvement.[29] Encouragingly, they understand clearly the perils of developing an over-regulated environment, which would be costly to administer and would slow national responses to a rapidly evolving range of threats. They also noted that the majority of cyber risks could be mitigated by getting the basics right, which would allow specialist agencies to focus

29 In unattributable interviews.

on the more sophisticated threats [65]. There are some established business processes inside government and the CNI, particularly with regard to public communications strategies. For example, the Information Commissioner's Office and the Department of Health were identified as having effective outreach and messaging techniques. It is feasible that some of these procedures could be adopted and used in a consolidated cyber security communications strategy. Although this was not a focal point of the research, it could be beneficial if relationships between the security and police services and the civilian community in the fields of counter-terrorism, organized crime and public order were expanded to encompass cyberspace.

Change in the cyber security culture needs to be implemented in a manner that is uniform and constant, and supported by an environment in which best practice is shared together with aspects of the threat picture and optimal responses. Although some excellent methods have evolved for managing cyber-related risks, these tend to be dispersed among the many stakeholders in the CNI. The scattered distribution of critical information that is needed to combat a sophisticated and agile cyber threat, and the varied ways in which this information is managed, point to a requirement for a more structural and less ad hoc approach.

The most serious vulnerability associated with cyber dependencies is not that they can be exploited. It is to be found at a more fundamental level, where the apparent lack of vision and mission, the revealed absence of uniform strategies (particularly regarding necessary transformation) and the lack of effective communication and knowledge distribution processes all contribute to the image of a society undergoing a slow, erratic, uncomfortable and very insecure period of transformation. The systemic changes required to build a culture of cyber security within the CNI are bound to be difficult, but if they are managed consistently by informed and proactive leaders there could be grounds for optimism.

Postscript

Since the completion of research interviews and the writing of this report, a number of UK public- and private-sector changes have taken place regarding the ways in which cyber dependencies and vulnerabilities are perceived and handled. As well as increased resources being devoted to cyber security, the discussion has evolved and become more nuanced. There is wider agreement that, in addition to technological improvements, there is a need for a change in public attitudes to the issue. Education and awareness of cyber security are essential parts of a holistic approach, as the human element is often the greatest point of weakness.

The UK government's approach has evolved following the October 2010 Strategic Defence and Security Review and Spending Review. The National Cyber Security Programme is taking shape and, with funding of £650 million over four years, will work to mitigate the risks posed by cyber crime, industrial espionage and threats to national security. In February 2011 the prime minister met senior representatives from UK industries and asked them to share their cyber security expertise and experience for the benefit of the public and private sectors. Encouragingly, this consultation included parts of the private sector that are not traditionally technology-based but that depend on cyberspace for the smooth functioning of their businesses.

These actions are helping to catalyse ministerial and wider public-sector interest in cyber security, and broadening the discourse across government. This refinement in policy includes the 2011 UK Cyber Security Strategy, which notes the transformative effect that cyberspace has had on society and commerce, and acknowledges the heightened risk this presents to a public ever more dependent on information and communications technology. The FCO is also placing emphasis on the economic and social benefits that cyberspace offers, and is hosting a conference in late 2011 which aims to work towards a consensus on principles and norms of behaviour for governments and other actors in cyberspace.

In addition to government activity, there is some evidence of growing private-sector awareness of cyber dependencies and vulnerabilities. In part this appears to have been prompted by the number of significant cyber attacks that have been made public in 2011, as well as the economic and reputational losses that have been suffered as a result. There appears to be increasing willingness in certain sectors to report attacks swiftly and publicly. In some organizations the level and severity of attacks are translating into more detailed risk assessments; in others, however, the discussion of cyber security among senior management remains at a formative stage.

Through all this we see the emergence, if not of the culture of cyber security advocated in our first report,[30] then at least of a public discourse that encourages the development of greater awareness and understanding. This is a positive signal for the future, and if this report can help to encourage the development of a wider culture of cyber security then it will have achieved its purpose.

30 Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House, March 2009), http://www.chathamhouse.org.uk/research/security/papers/view/-/id/726/. p. 17.

Annex A: Research Methodology

Key organizations were selected from across the UK CNI according to two criteria. Organizations with which Chatham House already has a relationship (i.e. as corporate members or in research projects) were approached initially. This sample was then extended by selection of prominent CNI organizations from financial listings in the national media. Selection was not made on the basis that these organizations were perceived to be either most threatened or most vulnerable to a breach of cyber security. The intent was to conduct interviews with each category of CNI, assuming that common threads of risk and response could be found within each, and then to identify any occurrences of common business process relating to cyber security across the CNI.

Interview requests were directed at executives responsible for risk management, group security, finance and other general responsibilities. Meetings with representatives of ICT departments were deliberately avoided so as to establish more accurately senior and board-level awareness of the problems of cyber security and subsequently to assess the quality of organizational responses. A total of 100 invitations to participate were sent to board-level members of target organizations, both governmental and CNI (as well as other bodies acting as control samples). In order to clarify the purpose of the exercise, each invitation to participate was accompanied by a copy of the Chatham House report *Cyberspace and the National Security of the United Kingdom*.[31]

In the absence of a reply, reminders were sent after an interval of one month. A second non-reply triggered a telephone enquiry. A third non-reply was followed by a short email questionnaire, which provided the invitee with several answers from which they could choose in order to indicate their reason for not participating in the research. The 100 invitations resulted initially in 28 positive responses, out of which 20 respondents were willing and able to participate, and were subsequently interviewed. There were 24 negative responses. In spite of several rounds of outreach 48 invitations received no response at all.

It had been expected that the increasing number of cyber security-related anecdotes in the media would have catalysed a higher level of engagement. As the study progressed, however, the range of respondents to the survey appeared to be usefully representative of the UK cyber security culture as a whole. It should be noted that most of the government departments and agencies approached quickly and readily engaged with the project.

The level of response could be explained in a number of ways:

- The nominated individual (identified through the most current information available, such as company websites) was no longer in post, and the invitations had been discarded;
- The individual had no time available owing to other priorities;
- The recipient did not see the significance of the study;
- The nominated organization or enterprise had already contributed to another related study on cyber security, and was not disposed to expend more resources on the issue;
- A positive response to the Chatham House request would have implied knowledge of an issue that the enterprise or individual did not want to confront, and would have jeopardized a position of plausible deniability.

Negative responses

What follows is a selection of responses from organizations that chose not to participate in the project. These

31 Cornish et al., *Cyberspace and the National Security of the United Kingdom: Threats and Responses.*

quotations provide some indication of the way in which the research questions were perceived by the senior management of certain organizations.

- *Medical device provider* – 'At this time I do not feel it is appropriate for myself to engage in this project. As a global organization, we recognize there is an increasing threat through malicious (cyber) activity. However, it is not an area that we have capability or firm views on that would warrant your time in a discussion with myself and any of our UK executives. At XXXX we continually review our technology susceptibility and have spent many millions of pounds with consultants to minimise the risks we are exposed to. Our global network is handled by ourselves from (country XXXX) and a number of supporting technology firms.'
- *Mining company* – 'I have spoken to our relevant IT people and they have advised me that as we are already involved with a security community outreach programme we will decline your offer to participate at the present time.'
- *Large supermarket/retailer* – 'As you can imagine XXXX receives many requests such as yours, but has to decline the majority in order to leave time for the day job.'
- *Energy company* – 'Consequent to having reviewed the contents of your letter and the enclosed information, I have concluded that our involvement in the project would not be something to which we could make a meaningful contribution. While XXXX is a FTSE100 company, the number of staff that we employ is relatively small and security of data is manageable.'
- *International bank* – 'Over the last few weeks we have made some small changes in the Information Security organization which unfortunately means that we will no longer have sufficient security representation physically located here in the UK to participate in this project.'

Outreach and response statistics

The statistics tabulated below represent the numerous rounds of outreach conducted during the course of the research. They are divided into several response categories, and the response rate itself is then divided between the public and private sectors.

Table A1: Survey response rates

	Number	%
First invitation (by post)	100	100
Positive response	10	10
Negative response	9	9
No response	81	81
Second invitation (post or email)	81	100
Positive response	12	15
Negative response	12	15
No response	57	70
Third invitation (email or phone call)	57	100
Positive response	4	7
Negative response	3	5
No response	50	88
Fourth invitation (non-response email survey)[a]	15	100
Positive response	2	13
Negative response	0	0
No response	13	87
Total (after all rounds of invitations)	100	100
Positive responses[b]	28	28
Negative responses	24	24
No response	48	48
Invitations by sector	100	100
Public sector	11	11
Private sector	89	89
Number of interviews	20	100
Public sector	5	25
Private sector	15	75

a These were sent to selected organizations for which email contact details were readily available.

b The number of positive responses was greater than the number of interviews for various reasons including: invitee expressed interest initially but did not commit to an interview, invitee committed to interview but had to cancel, invitee expressed interest but passed invitation to another (less senior) individual in the organization who did not commit to interview.

Annex B: Interview Format

To maintain uniformity between interviews, a question structure was developed that would provide a point of reference during the discussions, and ensure a level of consistency within the research from which comparisons could be drawn. These questions were designed to illuminate cyber dependencies within the responding organization and pinpoint the vulnerabilities that they might cause or exacerbate. Each interview was conducted by two researchers when possible and lasted approximately one hour. All interviewees were given the assurance of complete confidentiality. After establishing information about the organization's internal structure, the researchers proceeded to the core issues with an examination of the organization's experience and understanding of cyber security and cyber-enabled dependencies as well as risk-management strategies. Time was also devoted to understanding the baseline of the challenges faced by the organization, and to assess the scale and impact of cyber threats confronted on a regular basis. Interviewers' notes were compared after each discussion to ensure a fair and complete understanding of the responses.

It is acknowledged that there are dangers inherent in drawing firm and generalized conclusions from a sample size of twenty interviews. However, the response size represents an important research finding in its own right, as it indicates an identifiable lack of engagement with cyber security at the senior management level of various CNI organizations. In assessing the many hundreds of individual data points that emerged through the course of the project, emphasis was placed on views and opinions that were supported by either a specific comment made by another interviewee, organization or enterprise, or by comments made by interviewees who expressed very similar sentiments. This increased the likelihood of drawing conclusions that were qualitatively consistent and robust. In this way themes and broader findings emerged and were grouped together from the series of interviews, while space was also provided for notable points that were raised only by a single organization. Interviews with UK government departments and agencies were intended first to understand better the way in which the UK government protects itself from cyber threats, and secondly to record and evaluate perceptions of how cyber security is currently managed by government agencies and how, in particular, it is perceived to be managed by the CNI.

Interview questions

The interview model was based upon standard commercial market analysis processes (SEAM).

Situation – gather background information and develop understanding of the context.
Experience/Understanding – what is the organization's relationship with the cyber environment?
Assessment – what are the implications and risks to business?
Mitigation – develop a potential road map to mitigate the risks.

Situation – concerning the core purpose of the organization; where Information Security (IS) fits into the wider risk strategy of the organization, and where/with whom accountability for IS lies.

- What is the objective of the organization?
- What are the organization's critical business relationships and functions?
- Does Information Security (cyber) management fit into the wider risk strategy of the organization? Is it considered and/or managed at board level?
- Where is the accountability for Information Security in your organization?
- Who determines business continuity policy and where is this authorized/signed off?

- What measures are in place to ensure the security of information flows?

Experience/Understanding – the identification, measurement and management of the enterprise's cyber-enabled business dependencies; the organizational mechanisms in place for processing 'lessons learned', and which sources are used for trustworthy advice.

- What is your business process or methodology for *identifying* Information Security dependencies (upon other organizations, suppliers, trading partners, etc.)?
- How do you *measure* these dependencies, and grade them according to their level of importance or criticality in relation to other business risks?
- How do you actively *manage* the risks associated with these dependencies?
- How do you educate employees and raise the overall level of awareness of cyber security and information assurance issues?
- To what extent do you empower staff to use and recommend new technologies to enhance business performance?
- What kind of cyber 'lessons learned' process exists within your organization?
- Which standards and practices do you adhere to for Information Security?
  - Are these standards and practices internal or external skills-based?
- Where do you go for trustworthy information and advice on Information Security and cyber advances/changes that may affect your organization in the future?

Assessment and Implications – the assessment of impact relating to the loss of a given service or capability and its bearing on the functioning and output of the organization. This was dependent on answers to Experience and Understanding.

- What impact would loss of X have on Y? What impact would loss of X have on the variety of organizations that are dependent on the goods or services that Y produces?

Mitigation and Road Map – concerning the security of ICT and how it enables either new business initiatives or processes, or presents opportunities for competitive advantage.

- How will your business model evolve in the future, and what Information Security opportunities and risks will this present?
- To what level do you use Information Security to enable new business initiatives or processes?
- How would Information Security present opportunities for your organization to gain competitive advantage?
- How will you ensure compliance with Information Security regulations and standards, while not losing sight of other important Information Security issues?
- How would you choose to share your Information Security experiences and development with other organizations?

Annex C: Quantitative Analysis[32]

This annex provides a quantitative analysis of responses from 14 CNI organizations out of the total of 20 interviewed during the course of this project. For the purposes of this analysis five government respondents and one charity [27] were excluded in order to focus solely on the responses of private-sector CNI (as defined by CPNI). The analysis team was informed of the purpose of the study and the method of data collection in order to place the audit task in the correct context but was otherwise not privy to drafts of the report.

1. 178 statements were obtained of which two were deemed irrelevant and the remaining 176 were verbatim statements of need and problems expressed in the interviews.
2. These statements were then analysed and grouped into 22 main categories of common problems and needs.
3. These categories were processed using the Enterprise Value Transformation – Quality, Function, Deploy (EVT – QFD) method, and twelve requirements were identified (see Table A2) that encompassed the common problems and needs. The following process was used for the quantitative analysis.

   The reports from the interviews were analysed to identify individual statements of problems/needs raised by each of the interviewees. The statements from all interviewees were then grouped using Affinity Diagramming, wherein the statements of need/problem were grouped and allocated a title describing a shared need/problem. The number of individual statements per grouping gave an indication of areas of shared concern and hence the first level measure of priority. The need/problem groupings were entered into a Customer Voice Table in which the description of the solution that would address the 'need/problem' descriptions was developed. The processes described above constitute the initial analyses of the modern QFD process. Three papers (in footnotes) that describe these processes in more detail focus on application of methods to software development and complex IT systems, their common theme being to use the methods to focus quickly on high-priority customer needs and ensure development efforts address these.[33]
4. These twelve requirements were refined by repeated reviews against the common needs/problems and tested to ensure the statement of requirement is:
   a. Unambiguous
   b. Complete
   c. Measurable
5. Once the twelve requirements were refined against the above criteria, the 176 verbatim statements were re-mapped to them to test for completeness and validity.

A statistical analysis was conducted of the number of verbatim statements addressed by each of the twelve requirements to give a first-level numerical prioritization and measure of validity and completeness. The twelve statements of requirement that result from the analysis may form the basis of critical success factors for the development of a cyber threat strategy in relation to the CNI. This analysis has been undertaken as a preliminary exercise without benefit of follow-up

32 This analysis was done by CyberCloud. http://cybercloud.co.uk/home.php (accessed 3 March 2011).

33 R. Zultner, 'BLITZ QFD -Software QFD for Very Rapid Development', 2000. Zultner & Company. K.E. Stansfield, J. Cole and G. Mazur, G.,'Complex IT Design Using Both Traditional QFD and Blitz QFD®', ISQFD'10 – Portland, Oregon (2010); and 22nd North American Symposium on QFD, Portland, Oregon, 22–24 September; Glenn H. Mazur, 'QFD & The Office of Homeland Security', 13th Symposium on QFD, Baltimore, Maryland, November 2001.

access to the stakeholders. Nevertheless it is clear that strong messages have emerged and are unlikely to change substantially, but further insights would doubtless appear during a more in-depth follow-up. This flowchart demonstrates the sequence of steps taken during the analysis.

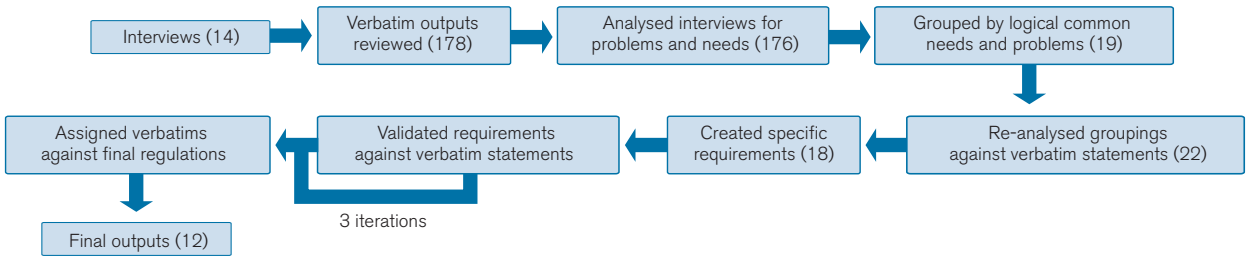

Table A2: Statements of requirement

Req. No.	No. of verbatims mapped to requirement	Requirement statement
1	66	In order to make UK a hard target for cyber crime it is necessary to develop effective engagement and coordination at the national level between government, commerce and industry. Ideally this will aid the development and dissemination of a mature threat response strategy.
2	28	It is essential to create a confidential, cooperative no-blame culture across government and industry in order to encourage the timely reporting of information necessary for robust threat responses. The success of this could be measured by the overall percentage increase of reported incidents.
3	96	A detailed analysis of CNI cyber vulnerabilities and interdependencies should be carried out, with particularly critical CNI systems subject to primary analysis. Vulnerabilities, either physical or logical, should be identified and their potential impacts on interdependent CNI systems and consequential impacts on the UK and its interests should be defined.
4	33	A specific register of what needs protecting in relation to requirement 1, and how this is to be achieved, should be created and updated regularly.
5	32	It would be helpful to develop policies in relation to the use of domestic or international law as a weapon of offence and defence in relation to conflict in cyberspace.
6	35	A strategic understanding of cyber threats should be produced and reviewed constantly in relation to the continually changing modes of communication technology and social trends, and a mitigation strategy produced at the national level.
7	24	Current information assurance standards should be reviewed in relation to emerging cyber threats and assessed for adequacy and upgraded as needed to reflect best practice.
8	79	Intelligence on the criminal response to cyber countermeasures should be made available to trusted organizations with a need to know and circulated to the appropriate parties. This would serve to communicate lessons learned and advise on emerging threats.
9	61	A mechanism for general industry and governmental use is required to test for and mitigate emerging cyber threats.
10	11	Cyber-specific business continuity needs should be identified and categorized in terms of: i) what must be in place for the continued governance of the country; ii) what must be in place to support commercial infrastructure; and iii) what should be recommended or mandated for industry, commerce and individual citizens.
11	29	Government policy for cyber threats should be set in relation to hard fact, based on their economic and political requirements, in consultation with other governments and international bodies. This should be reviewed on a regular basis in order to keep up with the pace of change.
12	All	Any analyses carried out must be subject to validation for appropriateness, completeness and accuracy.

Annex D: Additional Infrastructure-related Interview Results

Additional results were revealed during the course of the programme of interviews. Since these responses were concerned largely with ICT infrastructure, which was not the primary area of concern, they are presented here rather than in the main report. Some may be directly relevant only to ICT departments or to organizations involved in global governance of the internet such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU), as opposed to the senior management within the CNI. However, we believe these results also have a broader value because they pose interesting questions regarding resilience, redundancy and risk management in the public and private sectors.

- The radiology department's X-ray system is heavily dependent on the Picture Archive Exchange (PAX), and when it goes down the hospital is crippled. There is no backup system in place for this vulnerability. [18]
- The National Health Service supply chain is essentially run by DHL. [18]
- A charity has dozens of branches around the world. All branches have their own ICT systems, and there are some issues with compatibility. [27]
- A charity has an airwave licence for some radios for use in the UK, but has other radios that cannot be used in the UK because they are not on the licence. [27]
- 27 per cent of domain names are not identifiable. [33]
- There is a need for further development of trusted ISP services. [33]
- Hosting of internet services is a critical choice – whether to choose onshore or offshore hosting. [38]
- There is no real strategy for dealing with threats to SCADA systems, and management of these systems is done in isolation. [44]
- Infection of automated banking machines is a potential risk – 30% infection rates could cause severe disruption to a bank. [52]
- Cheaper anti-virus tools are needed, as many are quite expensive. [58]
- Smartgrid is a whole new risk area. [71]
- A large utility experienced a very large email crash that affected its entire system. This counted as a 'priority 1 incident'. [87]

BAE SYSTEMS Detica

CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org

Charity Registration Number: 208223

ISBN 9781862032514