Cyber Security and Global Interdependence: What Is Critical?

Dave Clemente

February 2013

CHATHAM HOUSE

Cyber Security and Global Interdependence: What Is Critical?

Dave Clemente

February 2013

CHATHAM HOUSE

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 278 1

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

Cover image: © istockphoto.com

Designed and typeset by Soapbox Communications Limited
www.soapbox.co.uk

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

Contents

About the Author

Dave Clemente is a Research Associate in the Chatham House International Security Department. He has worked at the International Institute for Strategic Studies and the Overseas Development Institute, and his areas of expertise include technology and cyber security policy and US and UK security and defence policy. He is co-author of *On Cyber Warfare* (Chatham House, 2010) and *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, 2011).

Acknowledgments

I am grateful to the Norwegian Institute of International Affairs (NUPI) and Multinational Experiment 7 (MNE7) for supporting this research, in particular to Hans-Inge Langø and Karsten Friis for their assistance and encouragement. The views expressed are mine alone, as are any inaccuracies in fact or interpretation.

D.C.

Executive Summary and Recommendations

Modern life is increasingly dependent on a multitude of interconnected and interdependent infrastructures. While sectors such as food, water, health and transportation and the infrastructure that supports them have always been critical, their ability to deliver is increasingly enmeshed with the information and communications technologies that have become essential components of daily life.

Although cyberspace – the sum of these components – is sometimes categorized as a discrete sector, in practice it is so deeply embedded into sectors such as energy and transport as to make any separation meaningless. Cyberspace can be visualized instead as a thin layer or nervous system running through all other sectors, enabling them to communicate and function.

Security of the cyber layer is of great societal importance, yet the dense interconnections between sectors – facilitated by cyberspace – make it harder to decide what to protect. As transportation intertwines with food distribution and telecommunications, and as these and many others sectors are supported fundamentally by the finance and energy sectors, it is more difficult to draw clear boundaries between critical areas.

It is becoming harder to identify the nodes and connection points whose protection must be prioritized. The result is that in the public debate, at least, critical infrastructure sectors tend to be categorized very broadly, to the extent that they encompass almost every aspect of daily life. The problem, therefore, is that when everything is 'critical', nothing is.

This makes it difficult to counter emerging threats, which are growing along with dependencies. Dramatic yet hypothetical scenarios, such as acts of cyber-enabled terrorism, cannot be ruled out, but they overshadow the more mundane but identifiable and persistent damage caused by organized crime and hacking.

This complexity does not lessen the responsibility of owners, operators and service providers to secure their infrastructure. Potential vulnerabilities are discovered regularly and, although few of these are exploited on a large scale and even fewer result in severe damage, the risk of disruption will continue to increase in parallel with growing connectivity.

What is critical?

A 2011 Chatham House report on cyber security asked: 'what should be considered "critical" in a modern society; does the spread of information and communication technologies also expand the

definition of critical national infrastructure?'[1] This report expands on that question by developing a more meaningful understanding of critical infrastructure.

It analyses primary challenges surrounding interdependence as it relates to cyber security and the protection of infrastructure. The report sheds light on these broad and often opaque categories, and demonstrates the need for clarity and specificity when prioritizing and investing in security measures. It asks: to what extent does increasing digital complexity and dependence make societies more vulnerable? If risks are growing, how can responses be developed in a way that increases security while preserving the economic benefits and social freedoms that come with interconnection? Or are these mutually incompatible goals?

These questions are becoming more difficult as cyber-enabled critical infrastructure dependencies spread across national boundaries and become global. These are areas where a diverse group of actors – with widely varying interests and incentives – interact and compete in a predominantly commercial space. Both the public and private sectors are intimately linked, regardless of their individual wishes.

These global interdependencies are redefining understandings of critical infrastructure, which in turn challenges notions of national sovereignty and forces policy-makers to reconsider the tensions inherent in this highly optimized yet fragile system of physical, logical and social connections.

Each country approaches the shared benefits and problems of globalized infrastructure in different ways and often without a shared language. The report examines the European Union, Russia, Japan, Brazil and others by looking at how they define 'critical', 'critical infrastructure', critical infrastructure 'sectors' and 'critical information infrastructure' in order to demonstrate the similarities and differences in national approaches to infrastructure protection.

Managing risk at the speed of change

Traditional categories of critical infrastructure do not adequately capture the complexity or speed of the modern ecosystem, and many countries depend increasingly on infrastructure and assets over which they have little or no control. For this reason the report does not refer to 'critical *national* infrastructure'. While the individual assets in question (such as factories, power plants or mines) are critical at a national level, many of them are partially or completely outside the geographical or jurisdictional control of the consumer (i.e. a state or its citizens).

Risk management is more difficult as a result. Interdependencies in critical infrastructure have multiplied to the extent that it is difficult, if not impossible, to define defensive perimeters. Such a concept has little meaning when connectivity is valued above security. Broad sectors such as food, water and transport are labelled 'critical', leaving ambiguity as to what needs to be prioritized within these sectors. Risk assessments are often conducted with only vague metrics for threats, vulnerabilities or potential impacts. This requires close scrutiny for countries that are dependent on complex, interdependent global networks – in short, for nearly every country around the world.

There is no avoiding the security implications emerging at the intersection of cyberspace and critical infrastructure. Ambiguity in defining and delineating infrastructure dependencies is

1 Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, September 2011), http://www.chathamhouse.org/publications/papers/view/178171, p. 2.

hindering the development of security measures. The 'critical' label should be used sparingly, and rigorous prioritization encouraged to avoid spending too much or too little on risk management.

A transparent approach based on inputs and outputs (i.e. what resources were used, and what they achieved) will facilitate more accurate prioritization and risk management measurements. It is also likely to gain wider stakeholder acceptance, as opposed to proscriptions or regulations that can become outdated quickly or are often circumvented or watered down.

Case studies

The prioritization of critical infrastructure is studied here by considering two closely connected case studies.

The first looks at the evolution of the US Department of Homeland Security National Asset Database, which listed over 77,000 items by 2006. Minimal central government guidance in the identification phase meant that state and local officials produced poor-quality data that included the likes of car dealerships, bean festivals and petting zoos as 'assets'. The database contained too many low-priority assets and in some cases was inaccurate.

A critical official report noted that the goals for building the first generation of the database had not been accomplished, and as a result government grants for protection of critical infrastructure could not be effectively prioritized.

This failure of prioritization in selecting assets undermined the entire exercise, demonstrating how asking the wrong questions at the beginning can lead to delay and disruption. It also shows how incentives – in this case government security grants – can create behaviour that runs counter to the overall aim of more effective infrastructure risk management.

The second case study examines the US Department of Homeland Security/State Department project to compile an inventory of critical infrastructure and key resources located outside US borders, and whose loss could critically affect public health, economic security or national security.

The existence of this international asset database was revealed by WikiLeaks in 2010. As with the self-reporting (from state and local officials) in the National Asset Database, US embassies were asked to submit a list of critical infrastructure in their host country. The list of 259 sites included ordnance manufacturers, pharmaceutical corporations, hydroelectric dams, suppliers of rabies vaccine, telecom providers and major ports.

The list's content – although in some cases broad and out of date – demonstrates the truly global nature of critical infrastructure. The list focuses less on military dependencies and more on energy, heavy industry and telecommunications. It reflects a process of interconnection that has evolved over decades but has recently been supercharged by the advent and spread of cyberspace. It also demonstrates the extent to which a country can be dependent on infrastructures around the world.

Both case studies emphasize the importance of prioritization at an early stage of data collection, given the impossibility of generating accurate analysis from faulty, incomplete or imprecise data. While the US model is not universally applicable, it is evolving on a scale large enough to reveal

progress and potential pitfalls that other countries can learn from as they grapple with complex and interdependent infrastructures.

These interconnected infrastructures span the globe, meaning that developed economies are heavily dependent on an 'outsourced inside' – critical infrastructure or key assets that are owned, operated or manufactured internationally – to provide the daily necessities upon which their societies depend.

Resilience is particularly important at the international level because digital interconnections create efficiency but increase dependency. A fragile equilibrium sustains these dependencies but can be disrupted in unexpected ways. For example, the 2010 the volcanic eruption in Iceland created a sudden and severe impact on air traffic, while natural or accidental damage to submarine cables frequently causes internet disruption in countries with poor infrastructure resilience.

Interaction between the private sector (which owns and operates most infrastructure) and the public sector is also crucial. Different incentives and pressures drive rational actors on all sides, and these dynamics are shaping and being shaped by the rapid evolution of digitally connected infrastructures. Efficiencies grow in all sectors through these connections, but so do dependencies and potential vulnerabilities.

Understanding and managing the risk that arises from these dependencies is rarely straightforward or transparent. If the financial crisis that began in 2008 has demonstrated anything, it is that opaque or obscured risk can also be dispersed risk – that may ultimately be owned by everyone. This is particularly true of critical infrastructure, upon which whole economies and societies depend.

Conclusions and key recommendations

The challenges posed by highly interconnected infrastructures are significant and growing, and are compounded by imprecise language and bureaucratic inertia. The recommendations below frame these challenges from a big-picture perspective. They provide a way of addressing some of the issues that are most intractable, while leaving room for individual organizational interpretation and implementation.

- **Adapt:** There is a need to acknowledge the uncertainty inherent in the complex systems that sustain us. Encouraging and mainstreaming adaptability and flexibility within organizational hierarchies will facilitate faster responses to emerging risks, and may also provide competitive commercial advantages. This may require restructuring or coordination between departments that deal with strategic direction, risk management and value-chain dependencies. It will require better shared understanding of what is critical between those who protect an organization and those who set its strategic direction.

  Grappling with 'big data', cloud computing and a host of emerging technologies is driving greater specialization, and hiring talent is a significant area in need of adaptation. Retention and promotion of this talent signals that these skills provide opportunity for upward mobility, and will ultimately improve the understanding of these issues in senior management. There is also a need to embrace new concepts of what is critical. Distinctions between 'infrastructure' and 'information infrastructure' are increasingly irrelevant, as data become as valuable as physical infrastructure.

- **Prioritize:** Scrutinize upstream and downstream risks, and consider restricting dependency where uncertainty is too high and opaque or dispersed risk is too great. It is necessary to examine the links in a value chain that are subject to the highest levels of risk, and where risk may be poorly understood. Methodologies of information collection and categorization must be refined continually in order to ask the right questions and avoid being overwhelmed by low-priority risks.

  Too few decision-makers are willing to accept the political risk that might come with removing an item from the 'critical' list, and the temptation is to continually expand the circle of things that are considered critical. This level of ambiguity is wasteful as resources are not directed to where they can have the most impact.

  It is also strategically unwise. Given the increasing rate of dependence between critical infrastructure and cyberspace, ambiguity in prioritization and protection is counter-productive. This is particularly true in sectors that are critical at a societal level, and the discussion should be a public one in order to gain widespread consensus on the use of public resources to protect critical infrastructure.

  Methods of analysing broad sectors (e.g. 'food') and narrowing them down to a manageable set of truly critical sub-sectors are more essential now that dependencies are spreading ever further beyond borders. At the highest level of prioritization (e.g. critical nodes in government networks) this information will be confidential, but far more of the current discussion surrounding criticality can be made public.

- **Incentivize:** Better understanding of the economic and political incentives that guide stakeholder behaviour will help to avoid unwanted surprises. In cyberspace, the majority of the commercial world tends to prioritize speed over security (e.g. for competitive advantage, for speed to market, etc.). Governments focus more on delivering services to society at a politically optimum level (i.e. at a level adequate to sustain political advantage). Nuanced understanding of these differing incentives can reveal greater room for agreement.

  Higher levels of cyber security lead to higher costs of doing business, meaning that policy interventions should be calibrated with a long-term perspective and awareness of potential second- and third-order consequences. The guiding principle for all sides could be 'cooperate where it will prevent the most societal harm' (with acknowledgment that 'harm' is a contested concept). Some will nominate industrial espionage for first priority, but the reduction of cyber crime may also be a primary objective, given the damage it causes at a societal level. Addressing these problems and others will require patient cooperation and sustained and regular interaction between senior policy-makers at the national and international levels.

- **Invest in resilience:** Focus on protecting dependencies that also enhance societal, physical and cyber resilience and/or redundancy. Exploit areas where commercial and societal resilience overlap, and where gains in both areas can be made simultaneously through focused investment. One example would be alternative energies, which are increasingly commercially viable (though this may require subsidies initially), but which also make the energy grid and dependent populations more resilient to disruptions in energy generation and transmission.

> Resilience of physical infrastructure understandably feels more tangible than societal resilience, but building public confidence in the security of the critical infrastructure ecosystem and its governance is essential to avoid policy-making driven by reactive or stove-piped interests. A widespread infrastructure failure or crisis would undoubtedly drive change; however, decision-making in such an environment increases the likelihood of unintended consequences. An open and transparent process of risk management can help to build public confidence in protection of critical infrastructure, and ultimately this is just as important as building physical resilience.

Certainty – and by extension security – implies control in both physical and virtual domains, yet the internet has been called a 'global machine for springing surprises'.[2] This makes adaptability and prioritization core priorities for the protection of critical infrastructure.

Many of the most intractable cyber security issues are inherently socio-technical. They truly are 'wicked' problems (i.e. complex, often socio-technical policy problems), yet the anxiety they provoke need not be the focal point of societal interaction with cyberspace. The possibilities offered by cyberspace are far greater than the dangers it contains – many of which are framed in the kind of dramatic and apocalyptic language that reveals deeper fears of technology getting out of control.

Government policies can shape the landscape for better or worse, but there are no solutions that will satisfy all stakeholders, since they are shaped by the subjective perspectives and inevitably limited knowledge of decision-makers. As elsewhere, security in cyberspace – and of critical infrastructure specifically – is a means to an end; it is intended to facilitate the provision of a multitude of social and economic goods. The task facing policy-makers is to design security measures that can achieve societal consensus and preserve the ability of cyberspace to flourish, thrive and provide these goods and wider benefits. This is one of the most difficult policy challenges of the early 21st century, and those that can find an optimal balance between freedom and security in cyberspace will reap rewards that are far greater than the costs.

2 John Naughton, 'The internet: Everything you ever need to know', *The Observer*, 20 June 2010.

1 Introduction

The fabric of modern life – at the individual, national and international levels – is increasingly dependent on a multitude of interconnected and interdependent infrastructures. While services such as food, water, health and transport have always been critical for human survival, their delivery is increasingly enmeshed with communications infrastructure and cyberspace more broadly. Underpinning all of these is the energy sector, without which no other sector could function at scale. These services and others are vital to healthy economies and societies. Protecting them is therefore vital, and there is no escaping both their essential nature and their inherent interdependencies.

Critical infrastructure (CI) is generally understood to include the particularly sensitive elements of a larger ecosystem, encompassing the public and private sectors and society at large. This goes beyond physical infrastructure to include data – which can be considered a form of logical infrastructure or 'critical information infrastructure'. Cyberspace and associated information and communications technologies (ICT) have become essential components of modern life. Although cyberspace is sometimes categorized as a discrete sector, in practice it is so deeply embedded into other sectors as to make this distinction meaningless. It can be visualized as a thin layer (or a nervous system) running through all other sectors, enabling them to function and interconnect. The energy and telecommunications sectors in particular are integral to cyberspace, but it is also true that cyberspace is essential to the functioning of most, if not all, CI sectors.

UK infrastructure sectors

- Communications
- Emergency services
- Energy
- Financial services
- Food
- Government
- Health
- Transport
- Water

These linkages and dependencies raise important questions. By now it is a familiar refrain that security of the cyber layer is of great importance. But with dense interconnections it can be extremely difficult to identify the vulnerabilities – and therefore the connections, nodes or systems – whose protection must be prioritized. How does cyber security fit into the debate over protection of critical infrastructure, and how can the pieces of the puzzle that require the highest level of attention be identified? Where are the critical points within these complex systems and networks, and how can one determine what level of cyber security is needed, so as not to spend too much or too little?

These questions are not easy to answer, and they are becoming more difficult as cyber-enabled critical infrastructure dependencies spread beyond sovereign boundaries and become global. These are areas where a diverse group of actors – many with widely varying interests and incentives – interact and compete in a predominantly commercial space. This, then, is about more than just governments; both the public and private sector are intimately linked, whether they like it or not. These globally complex interdependencies are redefining what constitutes critical infrastructure. They challenge concepts of national sovereignty and force us to consider the tensions inherent in a highly optimized yet fragile system of physical, logical and social connections.

A 2011 Chatham House report on cyber security and critical infrastructure raised the question:

> *what should be considered 'critical' in a modern society; does the spread of information and communication technologies (ICT) also expand the definition of critical national infrastructure? 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.*[3]

This report expands on that question by developing a more meaningful understanding of critical infrastructure. It analyses some of the challenges surrounding dependence and interdependence as they relate to cyber security and the protection of CI. Its aim is to shed light on these broad and often opaque categories, and by doing so demonstrate the need for clarity and specificity when defining CI and investing in security measures. Does increasing cyber complexity and dependence equate to increased vulnerability? And if risk is increasing, how can responses be developed in a way that increases security while preserving the economic and social benefits of interconnection? Or are these mutually incompatible goals?

The report argues that ambiguity in defining and delineating critical infrastructure and associated dependencies is hindering the development of security measures. The 'critical' label should be used sparingly, and strict prioritization encouraged to avoid spending too much or too little on risk management.

This is illustrated by two closely connected case studies that deal with prioritization of CI. These examples are drawn from the United States in part because of the volume of available material and related analysis, but also because the high level of US CI interconnectedness (largely cyber-enabled) is regarded as a model for emerging countries. While the US model is not universally applicable, it is evolving at a scale large enough to reveal progress and potential pitfalls for countries that may wish to emulate it. This report also looks at the interaction between the private sector (which owns and operates most CI) and the public sector, the incentives and pressures that drive rational action on all sides, and how these dynamics are shaping (and being shaped by) the rapid evolution of cyber-enabled infrastructure.

Chapter 2 looks at the growth of the complex adaptive systems that underpin the fabric of our daily lives, and gives some historical perspective on this change. It outlines some of the main categories of interdependency, and how they can obscure which link or node in the chain is critical, or liable to fail catastrophically.

3 Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, September 2011), p. 2, http://www.chathamhouse.org/publications/papers/view/178171.

Chapter 3 provides an overview of definitions surrounding CI categories and sub-categories, in order to gauge the extent to which these classifications are measurable, verifiable and, ultimately, fit for purpose.[4]

Chapter 4 examines two closely connected case studies that focus on the national and international nature of modern CI dependencies, and demonstrate how prioritization is essential.

Chapter 5 provides perspectives and recommendations for public- and private-sector organizations that are thinking urgently about these issues, in the hope of making a complex problem more accessible from a policy perspective.

4 'At our present skill in measurement of security, we generally have an ordinal scale at best, not an interval scale and certainly not a ratio scale. In plain terms, this means we can say whether X is better than Y but how much better and compared to what is not so easy. Having an ordinal scale is nevertheless well and good as knowing which is the better of two alternatives is what decision making is about.' Dan Geer, 'Keynote', *Source Boston Conference*, 13 March 2008, http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html.

2 Increasing Complexity

'Some problems are so complex that you have to be highly intelligent and well informed just to be undecided about them.'

Laurence J. Peter[5]

Many governments have attempted to define which parts of critical infrastructure are truly critical, with limited success. Current systems of CI categorization struggle to account for the complexity of cyberspace – upon which most infrastructure is now dependent. The scale and pace of interconnection pose problems and offer unprecedented opportunities. The myriad connections between CI and cyberspace are an area of growing interest. Modern infrastructure is entirely reliant on the physical and logical components of cyberspace – which itself is often considered to be critical.

This cyber-enabled interdependency widens the scope of analysis significantly (i.e. in principle almost everything can now be connected to everything else) and is a major factor in the growing complexity of CI. This complexity is increasing exponentially, 'through the extension of the geographical reach and the expansion of the services provided; the introduction of new components with richer functionality using diverse technologies; the increasing number of networks, nodes, and links and interdependencies; and the layering of systems over systems'.[6] Cyberspace itself can be divided into several categories, which include physical, logical and social layers.

At current growth rates, it has been estimated that by 2020 there will be 50 billion 'things' connected to the internet.[7] This sea of devices is often called the 'internet of things', and they use cyberspace to exchange, aggregate and extract information. These devices range from what would be considered obvious – such as personal computers, smart phones and tablets – to less obvious (or at least less visible) things such as washing machines, electricity and gas meters, and even health sensors for cows.[8] Factor in the autonomous interactions between these devices, mix in the creativity and unpredictability added by their human controllers, and the implications could be truly amazing. The potential advantages are nearly limitless but the resulting security risks could dampen enthusiasm.

5 Jeff Conklin, 'Wicked Problems and Social Complexity', in *Dialogue Mapping: Building Shared Understanding of Wicked Problems* (Wiley and Sons, 2006), http://cognexus.org/wpf/wickedproblems.pdf, p. 1. Dr Peter was an educator and management theorist, who is perhaps best known for having formulated the Peter Principle. This is the idea that in a hierarchical organization, where advancement is based on achievement and merit, every employee will eventually be promoted to his or her level of incompetence.

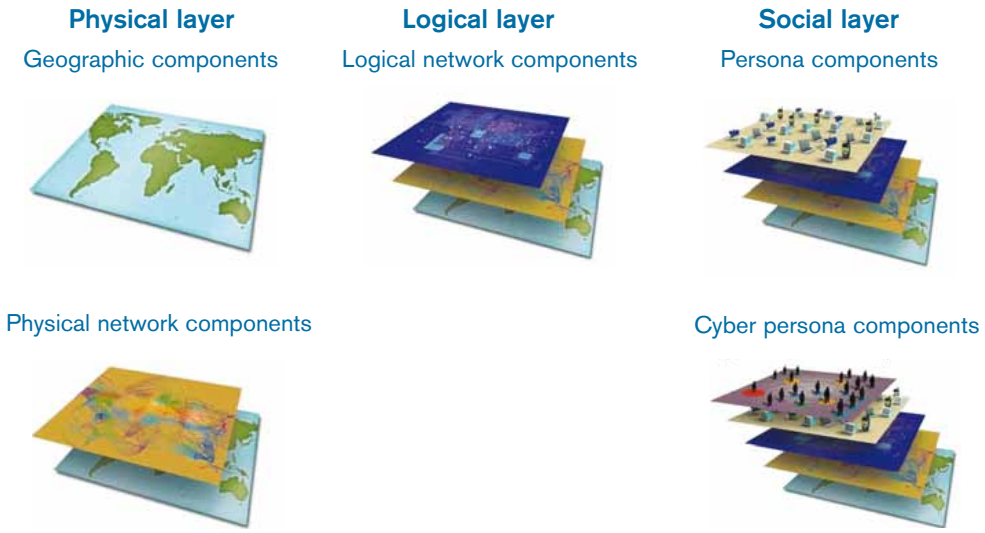
6 Myriam Dunn Cavelty, 'Systemic cyber/in/security – from risk to uncertainty management in the digital realm', Swiss Re Centre for Global Dialogue, 15 September 2011, http://cgd.swissre.com/features/Systemic_Cyber_In_Security.html, accessed 10 March 2012.

7 Arik Hesseldahl, 'Cisco Reminds Us Once Again How Big the Internet Is, and How Big It's Getting', *All Things* D, 14 July 2011, https://allthingsd.com/20110714/cisco-reminds-us-once-again-how-big-the-internet-is-and-how-big-its-getting/.

8 Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco Internet Business Solutions Group White Paper, April 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Figure 1 demonstrates one way of visualizing this increasing complexity. It separates cyberspace into three layers; the physical layer (i.e. hardware such as submarine and ethernet cables, routers and switching devices), the logical layer (i.e. software or lines of code that allows the hardware to function and communicate), and the social layer (i.e. interaction between online personas that represent people or, increasingly, machines). These three layers are fundamental to the core functions of cyberspace, and they are continuing to grow in diversity, richness and complexity.

Figure 1: Three layers of cyberspace



Source: Department of the Army Headquarters, United States Army Training and Doctrine Command (2010), 'The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028', TRADOC Pamphlet 525-7-8, http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf, p. 8.

This systemic complexity has been driven by a number of changes that will be discussed further – including post-Cold War perspectives on CI, industrial privatization, the incentives that drive global commerce and increasing global interdependence. Ultimately it has been driven by the possibility of greater efficiency and productivity. By connecting people and devices in so many different ways, the internet has streamlined pre-existing commercial, social and political processes. In the process it has created economic, social and political possibilities where none existed previously. As James Lewis noted; 'the effect of the internet is to lower transaction costs – everything else is just advertising'.[9]

As these cyber-enabled interconnections increase, so too does the difficulty of drawing discrete boundaries between them. The result is that CI sectors tend to be very broad, to the extent that they encompass almost every aspect of daily life. And when everything is 'critical', nothing is. From certain perspectives this ambiguity could be viewed as desirable, in that it blurs responsibility and accountability for decision-making, but ambiguity is unhelpful when trying to delineate and protect critical systems.

9 James Lewis (@james_a_lewis), 'Rethinking digital development (effect of internet is to lower transaction costs; everything else is advertising). What's missing?', 9 January 2012, 1:36pm, Tweet, https://twitter.com/#!/james_a_lewis/statuses/156368736209747969.

Kenneth Kukier argues:

> *A high threshold is needed when one attempts to identify something as truly critical. For instance, many important systems are self-repairing or self-healing, such as the way that Internet traffic routes around damage, or how motor traffic still continues to flow even if traffic lights go out. Thus, even in failure, some operations can still be sustained. What is needed is a far more difficult level of judgement and calculation.*[10]

While complexity is increasing, security perceptions are shifting, further complicating attempts at conceptual clarity. Since 9/11, critical infrastructure protection in the United States and Europe has been framed largely by the spectre of terrorism (primarily non-state extremist terrorism, as opposed to state-sponsored terrorism) and tops the list of many CI threat lists. While this ranking mirrors popular fears and political priorities, it does not accurately reflect measurements of risk and probability.[11]

This is an example of 'probability neglect' where

> *in two situations involving the same dreadful possibility, one much more likely to unfold than the other, individuals may value risk elimination nearly equally even though probabilities may differ by a factor of 20 or more. People focus on the bad outcome itself, and are inattentive to how unlikely it is to occur – hence their overreaction when the risk is low.*[12]

In reality, natural disasters and accidents cause far more damage and disruption to CI than terrorism (e.g. Hurricane Katrina and the Indonesia blackout in 2005), although an observer would be at pains to discern this when observing the crafting of Western security policy over the past decade.

Interdependencies in CI have multiplied to the extent that it is difficult to define defensive perimeters. Such a concept has little meaning when connectivity is valued above security. Broad sectors such as food, water and transport are labelled 'critical', leaving ambiguity as to what needs to be prioritized. Risk assessments are often conducted with only vague metrics for threats, vulnerabilities or potential impacts.[13] This state of affairs requires close scrutiny for countries that are dependent on complex, interdependent global networks – in short, for nearly every country around the world.

---

10 Kenneth Kukier, 'Ensuring (and Insuring?) Critical Information Infrastructure Protection: A Report of the 2005 Rueschlikon Conference on Information Policy', The Rueschlikon Conference, 2005, p. 13, http://www.rueschlikon-conference.org/pressdocs/56_R_05_Report_Online.pdf.

11 The US Department of Homeland Security 'focuses all or almost all of its analyses on the contemplation of the consequences of a terrorist attack while substantially ignoring the equally important likelihood component of risk assessment as well as the key issue of risk reduction […] Political and emotional conditions do supply an understandable excuse for expending money, but not a valid one, and they do not relieve officials of the responsibility of seeking to expend public funds wisely. It is particularly important to do so with homeland security expenditures. They deal not with bridges to nowhere or with crop subsidies, but with public safety – or domestic tranquillity – the central, fundamental reason for the existence of government in the first place.' John Mueller and Mark G. Stewart, 'Does the United States Spend Too Much on Homeland Security?', *Slate*, 7 September 2011, http://www.slate.com/articles/news_and_politics/politics/2011/09/does_the_united_states_spend_too_much_on_homeland_security.html.

12 Cass R. Sunstein and Richard Zeckhauser, 'Dreadful Possibilities, Neglected Probabilities', in Erwann Michel-Kerjan and Paul Slovic (eds), *The Irrational Economist. Making Decisions in a Dangerous World* (New York: Public Affairs Books, 2010), http://www.hks.harvard.edu/fs/rzeckhau/Sunstein4-6-09.pdf.

13 As of 2007, the US Department of Homeland Security had 'received $130 billion in budget authority since 2001 and that certainly buys more security. But more security does not necessarily make the country more secure. How much risk has that $130 billion bought down? No one knows because DHS has neither a long-term, risk-based strategic plan nor a comprehensive way of measuring risk reduction. […] At first, the department crudely calculated risk by using population as a proxy. Later, figures for the extent of threat and the presence of critical infrastructure were added to the equation. Chertoff introduced a new equation: Risk is equal to threat times vulnerability times consequence. For the first time, DHS is considering probabilities in the calculations that drive grants and other security investments.' Zack Phillips, 'Security Theatre', *Government Executive*, 1 August 2007, http://www.govexec.com/features/0807-01/0807-01s3.htm.

There is also an inherent level of uncertainty in the understanding of the CI risk and threat environment. Any analysis of cyber dependencies and interdependencies must acknowledge the ubiquity of these uncertainties. They are widespread to such an extent as to obscure areas of infrastructure failure or critical tipping points,[14] and complicate attempts to measure the effects of potential disruption.[15] The ability to measure failure rates varies across sectors, though on the whole it is difficult to predict failure rates in complex adaptive systems such as supply chains.[16] In addition, these dependencies will continue to spread as long as there are sufficient political, social or economic benefits to be gained from interconnection.

> There is no avoiding the security implications emerging at the intersection of cyberspace and critical infrastructure.

What can governments and the private sector do when faced by rapidly growing complexity, lack of meaningful metrics, divergent incentives and ambiguous definitions? The common cycle of constant, incremental updates to cyber defences are a recipe for exhaustion. There is a need to step back and improve our systems of understanding – of sense-making – to conceptualize and contextualize the global changes that are reshaping both the delivery of critical services and the very definition of 'critical'.

Governments are forced to engage with these issues. It is equally clear that the ability to measure cyber security risk, success and failure is often crude – particularly when compared with equivalent metrics that have been developed in other domains. The tools that are available point towards sobering trends (e.g. persistently vulnerable infrastructure, endemic divergence of interests, lack of human talent, exponential growth in threat vectors). Better metrics are needed to judge more accurately the ramifications and trade-offs inherent in all cyber security measures. This analysis uses as a guiding principle Dan Geer's strategic-level problem statement for cyber security policy: 'To move from a culture of fear, to a culture of awareness, to a culture of measurement.'[17]

Historical perspectives

Fuelled by the growth of cyberspace, the interconnection of critical infrastructure is increasing, and with it some recognition of potential threats and vulnerabilities. But not everything is new or novel. There are historical and complicating factors that interact with the current environment. In many ways, contemporary infrastructure threats look very different from those of the late 20th century, and it is important to be aware of these differences when designing adaptable response mechanisms.

In the United States, for example, there has been a post-Cold War shift in perceptions of infrastructure security. Washington has long devoted attention to infrastructure protection, though

14 'We see the power system as slowly evolving in response to increasing load, economics, engineering and recent blackouts so as to move to a complex system equilibrium near a critical point.' Ian Dobson, Benjamin A. Carreras, Vickie E. Lynch and David E. Newman, 'Complex Systems Analysis of Series of Blackouts: Cascading Failure, Critical Points, and Self-organization', *Chaos*, Vol. 17, No. 2, 28 June 2007, p. 1, http://dx.doi.org/10.1063/1.2737822.

15 'The electricity blackout in August 2003 in the United States and Canada illustrated the interdependencies between electricity and other elements of the energy market such as oil refining and pipelines, as well as communications, drinking water supplies, etc.' John Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, Congressional Research Service, 11 July 2011, p. 1, http://www.fas.org/sgp/crs/homesec/RL30153.pdf.

16 Ben Bland and Robin Kwong, 'Supply chain disruption: sunken ambitions', *Financial Times*, 3 November 2011, http://www.ft.com/cms/s/0/6b20d192-0613-11e1-ad0e-00144feabdc0.html#axzz1gMeEQVDf.

17 'While this statement is not operationalizable per se, it demonstrates my biases that security is a means and that game play cannot improve without a scorekeeping mechanism.' Dan Geer, 'Cybersecurity and National Policy', *Harvard National Security Journal*, 7 April 2010, http://harvardnsj.org/2011/01/cybersecurity-and-national-policy/.

during the Cold War it was much more narrowly focused than today. Protection of CI was centred on preserving essential government functions and securing key facilities against nuclear attack. Anything below that was a state or federal law-enforcement responsibility.[18]

The internet has its origin in the Cold War, and was originally conceived as a US military command-and-control network that could survive multiple nuclear attacks and retain communications and retaliatory capability. This survivability – through a network of distributed nodes – provided second-strike capability and therefore hope of a credible deterrence.[19]

But large-scale nuclear war is no longer an ever-present concern, having been replaced more recently by fear of terrorism. In the cyber domain, this has manifested itself in the form of the oft-invoked yet rarely experienced evil twins of cyber war and cyber terrorism. Despite the imminent catastrophes these allegedly threaten and the way they loom large in the public imagination,[20] neither of them comes close to equalling the dangers of nuclear holocaust. However, one apt parallel with the Cold War is where a 'cyber gap' has been postulated through a process of threat inflation (spurred perhaps by the lure of funds to address the problem) combined with poor public understanding of the technical nature of cyberspace (and therefore of which threats are realistic).[21]

According to this narrative, terrorists could exploit with relative ease the high connectivity enjoyed by developed countries to launch devastating cyber attacks and cripple large portions of CI. Without precedent to guide the debate, the negative proof fallacy (i.e. assuming something to be true if it cannot be proved false or vice versa) is often relied upon to bolster assertions. Burden of proof is evaded through official statements justifying opacity on the grounds of national security and protection of 'sources and methods'. The rhetoric of imminent cyber terror against CI has become increasingly dramatic. Yet, as noted by Peter Singer, 'over 32,000 scholarly articles have discussed cyberterrorism […] and 0 people have been killed by it'.[22] Although acts of cyber-enabled terrorism cannot be ruled out, dramatic yet hypothetical scenarios tend to overshadow the more mundane but identifiable and persistent damage caused by organized crime and hacking.

This dynamic does not lessen the responsibility of owners, operators and service providers to secure their infrastructure more adequately. Potential vulnerabilities are regularly discovered, though few of these are exploited and even fewer result in disruption. However, these flaws raise pertinent questions about the extent of corporate responsibility beyond service licensing agreements, particularly in sectors and sub-sectors that are vital to a functional society. What, if any, social responsibility does the owner of infrastructure X have when providing critical services in foreign country Y? In addition, these assets may serve as critical infrastructure for multiple countries, further blurring sovereign boundaries.

18 Anthony H. Cordesman with Justin G. Cordesman (Praeger, 2002), *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*, Center for Strategic and International Studies, pp. 1–3, http://books.google.co.uk/books?hl=en&lr=&id=YliRyO6ctzMC&oi=fnd&pg=PP9&dq=nato+critical+infrastructure&ots=JfmYidiCpe&sig=CmaSqQihMR4gvj8kRxd473rkPvE#v=onepage&q=nato%20critical%20infrastructure&f=false.

19 Johnny Ryan, 'How the atom bomb helped give birth to the Internet', *ars technica*, 21 February 2011, http://arstechnica.com/tech-policy/2011/02/how-the-atom-bomb-gave-birth-to-the-internet/.

20 Ryan Singel, 'More Americans Worried About Cybarmegeddon Than Terrorism, Study Finds', *Wired Threat Level,* 11 May 2012, http://www.wired.com/threatlevel/2012/05/cyberarmegeddon-terrorism/.

21 Peter W. Singer and Noah Shachtman, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive', Brookings Institution, 15 August 2011, http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx.

22 Peter W. Singer (@peterwsinger), 'Morning security fun fact: Over 32,000 scholarly articles have discussed cyberterrorism […] and 0 people have been killed by it', 31 March 2012, 2:53pm, Tweet, https://twitter.com/#!/peterwsinger/status/186088861091377153. Eleven months after the tweet, when this Chatham House report was published, a Google Scholar search for 'cyber terrorism' produced approximately 42,000 results.

Interdependency

Through the growth of global supply chains, privatization of industry and other economic pressures, elements of critical infrastructure commonly reside far outside national boundaries and may be owned by foreign governments or corporations. This transnational dynamic was acknowledged in a roadmap to propose amendments to a European Union Council Directive asking if the EU action to protect CI was justified on grounds of subsidiarity.[23] It noted that 'on substantive grounds EU action is justified because the transnational risks of interference with European critical infrastructure can cause disruption to more than one member state.'[24]

> Participation in the global infrastructure ecosystem is inherently predicated on acceptance of a measure of unknowable risk.

The main added value of the directive is that 'it has stimulated cooperation between the Member States on the protection of critical infrastructure, the disruption of which may have effects extending beyond the Member State where the critical infrastructure is located.'[25] The risk of cross-border disruption was sufficient to justify EU involvement in infrastructure protection, in this case through coordination. These regional and global interdependencies will only increase, and can be separated into a handful of main categories:

- ***Physical.*** *A requirement, often engineering reliance between components.*
- ***Informational interdependency.*** *An informational or control requirement between components.*
- ***Geospatial interdependency.*** *A relationship that exists entirely because of the proximity of components.*
- ***Policy/procedural interdependency.*** *An interdependency that exists due to policy or procedure that relates a state or event change in one infrastructure sector component to a subsequent effect on another component.*
- ***Societal interdependency.*** *The interdependencies or influences that an infrastructure component event may have on societal factors such as public opinion, public confidence, fear, and cultural issues.*[26]

Of the categories above, physical and informational linkages tend to be the more common benchmarks of dependency. In part this is because they are more amenable to measurement (as opposed to policy or societal dependencies), and because geospatial dependencies have been reduced thanks to the near-instantaneous communication offered by cyberspace.

23 'The principle of subsidiarity regulates the exercise of powers in the European Union. It is intended to determine whether, in an area where there is joint competence, the Union can take action or should leave the matter to the Member States. The subsidiarity principle is based on the idea that decisions must be taken as closely as possible to the citizen: the Union should not undertake action (except on matters for which it alone is responsible) unless EU action is more effective than action taken at national, regional or local level.' Eurofound, 'Subsidiarity', Page last updated 30 November 2010, http://www.eurofound.europa.eu/areas/industrialrelations/dictionary/definitions/subsidiarity.htm.

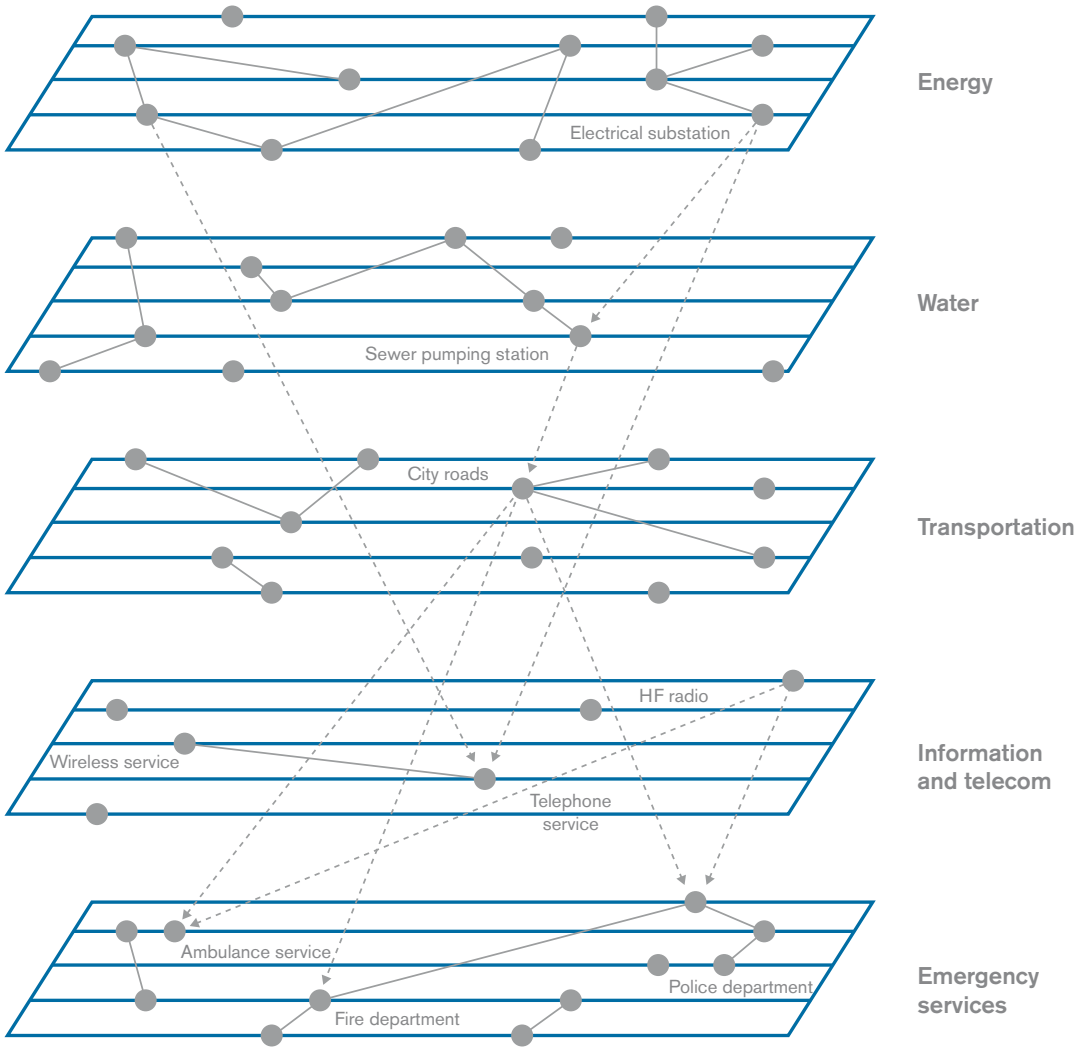
24 European Commission, 'Proposal amending Council Directive 2008/114/EC (identification and designation of European critical infrastructures)', Version 1, August 2011, http://ec.europa.eu/governance/impact/planned_ia/docs/2012_home_010_directive_critical_infrastructures_en.pdf.

25 Ibid.

26 'Again, while the dependencies within an individual infrastructure network are often well understood, the region of interest in interdependency and effects modelling is the influence or impact that one infrastructure can impart upon another. Therefore, the key effects to model and gain understanding of are the chains of influence that cross multiple sectors and induce potentially unforeseen n-ary effects […] These paths may not be unique in terms of effect, they may change over time, and their behaviour may be cumulative in nature, i.e., the end effect may be the culmination of multiple predicated events. The intertwining of networks in this fashion represents a complex system where emergent behaviours are rarely fully understood.' P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, 'Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research', Idaho National Laboratory, August 2006, pp. 6–7, http://cipbook.infracritical.com/book3/chapter2/ch2ref2a.pdf.

Figure 2 below gives a basic representation of interdependency between sectors, and demonstrates some of the critical nodes, such as telephone service, that many sectors rely upon. Though it is not represented in the figure, policy interdependency may be the most important, as it monitors, regulates or attempts to control (to the extent possible) the potential for expansion or contraction of the other dependencies (e.g. physical or geospatial) upon which a society relies. Ultimately, however, given the trend of increasing complexity, the challenge of comprehensively managing CI dependency is beyond the ability of any government. It is a fallacy to imagine that any country can accurately measure the inherent yet opaque risks to which its infrastructure is exposed.

Figure 2: Infrastructure interdependencies



Source: P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, 'Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research', Idaho National Laboratory, August 2006, p. 3, http://www.inl.gov/technicalpublications/Documents/3489532.pdf.

Entrance into, and participation in, the global infrastructure ecosystem is inherently predicated on acceptance of a measure of unknowable risk. That this participation is voluntary in order to attain significant benefit does not negate the risks. In any case, refusal to participate is scarcely

an option, given dependence on cyberspace for tasks both trivial and important. Exclusion or isolation (coerced or self-motivated) from the global internet is rare, laborious and generally self-defeating.[27] More sophisticated forms of resilience are needed, to increase security while sustaining economic growth and innovation. One cannot optimize everything at once. Prioritization – the inescapable trade-offs required between ends, ways and means – is at the heart of resilience.

27 Cyrus Farivar, 'Security researcher unearths plans for Iran's halal Internet', *ars technica*, 17 April 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/.

3 Shared Language

In the debate over prioritization, and determining what is or is not critical, terminological consistency – or 'semantic interoperability'[28] – permits greater efficiency through shared understanding. This is a priority for national coordination, and is increasingly important at the international level as critical infrastructure linkages span the globe. A useful starting point is to examine perspectives on three basic definitions: those of (a) 'critical' (b) 'critical infrastructure' and (c) critical infrastructure 'sectors'.[29] In this way, analysis begins at the macro level and then zooms in on the most crucial elements.

The following definitions demonstrate how CI is currently conceptualized, and they are supplemented by analysis showing where these definitions accurately describe the environment and where they may lack rigour, precision or, in some cases, practical applicability.

Critical

To protect the entirety of critical infrastructure has always been impossible, but it is increasingly difficult to understand what must be protected. It is more than just infrastructure; it also includes information critical to a functioning infrastructure. In some cases infrastructure may serve merely as a repository for much more valuable information.

A basic definition of 'critical' serves as a useful starting point. The Merriam-Webster dictionary offers the following: 'indispensable, vital <a critical waterfowl habitat> <a component critical to the operation of a machine>.'[30]

The *Oxford English Dictionary* defines 'critical' as 'having a decisive or crucial importance in the success or failure of something: "temperature is a critical factor in successful fruit storage". Origin: mid 16th century (in the sense "relating to the crisis of a disease"): from late Latin *criticus*.'[31]

Working from these definitions, large segments of CI (such as transport systems, power plants, or refineries) can be conceptualized as components that are critical to the operation of societal machinery.

28 'The European Interoperability Framework (EIF) defines semantic interoperability as the ability of organizations to process information from external sources in a meaningful manner. It ensures that the precise meaning of exchanged information is understood and preserved throughout exchanges between parties.' European Commission Joinup, 'Semantic Interoperability', https://joinup.ec.europa.eu/category/glossary/semantic-interoperability.

29 This report clearly contains a bias towards English-language terminology, and further study may be appropriate to analyse equivalent terminology in other languages.

30 Merriam-Webster, 'critical', http://www.merriam-webster.com/dictionary/critical.

31 Oxford Dictionaries, 'critical', http://oxforddictionaries.com/definition/critical.

Critical infrastructure

There are numerous national and international definitions of critical infrastructure. Although the similarities between definitions tend to outweigh their differences, the nuances are revealing. A report from the NATO Parliamentary Assembly notes that:

> *in some countries, those criteria stress the finality or purpose of the infrastructure (i.e. the infrastructure is critical because it performs a function that is vital to society), whereas in others they stress the severity or effects of the disruption or destruction of a given infrastructure on society (i.e. the infrastructure is critical because its loss would be extremely disruptive).*[32]

The European Union defines CI as

> *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*[33]

In the United Kingdom, the Centre for the Protection of National Infrastructure says that

> *there are certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These 'critical' assets make up the nation's critical national infrastructure (CNI) and are referred to individually as 'infrastructure assets'. Infrastructure assets may be physical (e.g. sites, installations, pieces of equipment) or logical (e.g. information networks, systems).*[34]

In the United States, the Department of Homeland Security (DHS) defines CI as

> *systems and assets, whether physical or virtual, so vital to the United States the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[35]

The US definition has been expanded beyond physical infrastructure to include 'key resources', and is now commonly known as CI/KR (Critical Infrastructure/Key Resources).[36]

---

32 Lord Jopling (Special Rapporteur), *162 CDS 07 E rev 1 – The Protection of Critical Infrastructures* (2007), NATO Parliamentary Assembly, http://www.nato-pa.int/default.asp?SHORTCUT=1165.

33 EU Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, p. 77, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

34 UK Centre for the Protection of National Infrastructure, *The National Infrastructure*, http://www.cpni.gov.uk/about/cni/.

35 107th Congress of the United States, *USA Patriot Act of 2001, Critical Infrastructure Protection Act of 2001. 42 USC 5195c*, news.findlaw.com/wp/docs/terrorism/hr3162.pdf. The US definition has broadened over time: 'Key assets, which was defined as potential targets whose destruction may not endanger vital systems, but could create a local disaster or profoundly affect national morale. Such assets were defined later to include national monuments and other historic attractions, dams, nuclear facilities, and large commercial centres, including office buildings and sport stadiums, where large numbers of people congregate to conduct business, personal transactions, or enjoy recreational activities.' Moteff, *Critical Infrastructures*, p. 10.

36 'The National Strategy for Homeland Security uses the term "key assets", defined as individual targets whose destruction would not endanger vital systems, but could create a local disaster or profoundly damage the Nation's morale or confidence. The Homeland Security Act and HSPD-7 use the term "key resources", defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government.' US Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* (2009), p. 15, http://www.dhs.gov/files/programs/editorial_0827.shtm.

In Russia, compared with the United States,

> *there is no similar formalized definition […] for critical infrastructure or critical infrastructure protection, although there are several references to the importance of specific systems in Russia that are critical to national security, economic stability, and public and social safety.*[37]

Japan's Information Security Policy Council defines CI in terms of

> *the basis of people's social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others if its function is suspended, deteriorated or become unavailable, it could have significant impacts on people's social lives and economic activities.*[38]

In Brazil, CI has been defined as

> *the installations, services or assets that if destroyed, disrupted or incapacitated will have a debilitating impact on security, the national economy, national public health and safety.*[39]

These definitions tend to be broad, covering nearly every aspect of daily life and leaving little to chance. On the whole this seems appropriate, as these definitions are meant to provide strategic perspectives that are subsequently narrowed down to critical sectors (e.g. energy, water, food, etc.). The real challenge comes in the following stages, where prioritization becomes important and difficult decisions are required.

Critical infrastructure sectors

On the basis of these broad definitions of critical infrastructure, the core components of a functioning society can be further refined into sectors. The US Department of Homeland Security lists 18 CI sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defence industrial base; emergency services; energy; government facilities; healthcare and public health; information technology; national monuments and icons; postal and shipping; transportation systems; water; and nuclear reactors, materials and waste.[40]

The US list appears expansive – almost all-encompassing – when compared with other countries. For example the Japan National Security Information Center categorizes CI into ten sectors: data communication, finance, airlines, railway, electric power, gas, government and administrative services (including municipal governments), medical, water service and logistics.[41]

37 Karl Frederick Rauscher and Andrey Korotkov, 'The Russia-U.S. Bilateral on Critical Infrastructure Protection – Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace', EastWest Institute, 3 February 2011, p. 12, http://www.ewi.info/working-towards-rules-governing-cyber-conflict/.

38 The Information Security Policy Council, *The Second Action Plan on Information Security Measures for Critical Infrastructures,* Japan National Security Information Center, 3 February 2009, p. 10, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf.

39 Emilio Tissato Nakamura, Jadir Antonio da Silva, José Manuel Martin Rios et al., 'Mobile Telecommunications Networks for the 2014 World Cup', GSM Association, 1 February 2011, p. 23, http://www.gsma.com/latinamerica/mobile-telecommunications-networks-for-the-2014-world-cup/.

40 US Department of Homeland Security, *Critical Infrastructure*, http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

41 The Information Security Policy Council, *The Second Action Plan on Information Security Measures for Critical Infrastructures,* p. 10.

The UK Centre for Protection of National Infrastructure (CPNI) identifies nine sectors that provide essential services 'upon which daily life in the UK depends'. These sectors are commonly used by many countries, with minor variations. They are communications, emergency services, energy, finance, food, government, health, transport and water.[42]

CPNI notes that 'not everything within a national infrastructure sector is "critical"', though it does not specifically identify the 'infrastructure assets' (noted above in the UK definition of CI) that are considered critical. The UK Cabinet Office provides some guidance, employing a Criticality Scale that 'includes three impact dimensions: impact on delivery of the nation's essential services; economic impact (arising from loss of essential service) and impact on life (arising from loss of essential service)'.[43]

The US Homeland Security Act of 2002 defines 'key resources' as 'publicly or privately controlled resources essential to the minimal operations of the economy and government.'[44] The notable element of this definition is the emphasis on 'minimal operation'. This can be a helpful distinction in sectors where operational levels can be clearly delineated (e.g. from minimal to optimal). The power grid is one such example, where a complex network is required to produce real-time feedback in order to balance precisely between demand and supply, often across national borders.[45]

However, if a rigorous interpretation of this definition is accepted, then, according to John Mueller and Mark Stewart,

> *it is difficult to imagine what a terrorist group armed with anything less than a massive thermonuclear arsenal could do to hamper such 'minimal operations'. The terrorist attacks of 9/11 were by far the most damaging in history, yet, even though several major commercial buildings were demolished, both the economy and government continued to function at considerably above the 'minimal' level.*[46]

This definition of 'key resources' is not particularly helpful in sectors whose operational level is highly dependent on multiple, external providers. What does 'minimal operation' mean in the context of cyberspace, where myriad autonomous actors with widely diverging incentives are linked in a loose web of cooperation (if only to avoid mutual disruption)? There is also a familiar demand on decision-makers, one that emphasizes the need to make trade-offs and prioritize scarce resources in pursuit of policy objectives. The US Congressional Research Service notes that 'a fluid definition of what constitutes a critical infrastructure could complicate policymaking and actions. At the very least, a growing list of infrastructures in need of protection will require the federal government to prioritize its efforts.'[47]

42 UK Centre for the Protection of National Infrastructure, *The National Infrastructure*, http://www.cpni.gov.uk/about/cni/.

43 UK Cabinet Office, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, March 2010, p. 25, http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-framework.pdf.

44 United States Senate, *(H.R. 5005) Homeland Security Act of 2002 (6 U.S.C. 101(9))* (2002), p. 10, news.findlaw.com/wp/docs/terrorism/hsa2002.pdf.

45 Dieter Diegel, Steffen Eckstein, Ulrich Leuchs and Oldrich Zaviska, 'Fulfillment of Grid Code Requirements in the Area Served by UCTE by Combined Cycle Power Plants' Siemens AG, Power Generation, 2004, pp. 3–4, http://www.energy.siemens.com/fi/pool/hq/energy-topics/pdfs/en/gas-turbines-power-plants/3_Fulfillment_of_Grid_Code.pdf.

46 John Mueller and Mark G. Stewart, 'Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security', prepared for presentation at the panel 'Terror and the Economy: Which Institutions Help Mitigate the Damage?' at the Annual Convention of the Midwest Political Science Association Chicago, 1 April 2011, p. 8, http://polisci.osu.edu/faculty/jmueller/MID11TSM.PDF.

47 John Moteff, Claudia Copeland, and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical*?, Congressional Research Service, 29 January 2003, summary page, www.fas.org/irp/crs/RL31556.pdf.

Critical information infrastructure

When the focus turns to critical information infrastructure (CII) the influence of cyberspace on all other sectors becomes strongly apparent. CII underpins the vast majority of physical infrastructure and is increasing as these infrastructures are linked together. The complex nature of large distributed networks makes the cyber layer extremely difficult to assess and analyse discretely, but relatively easy to compromise given the ever-expanding attack surface (i.e. connected devices).[48]

The European Commission has defined the CII layer as 'ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)'.[49]

> We may be nearing the point where distinctions between "infrastructure" and "information infrastructure" are irrelevant.

The US Department of Homeland Security defines CII as

> *any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video that is:*
>
> - *Vital to the functioning of critical infrastructure;*
> - *So vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety; or*
> - *Owned or operated by or on behalf of a State, local, tribal, or territorial government entity.*[50]

NATO's conception of CII and critical information infrastructure protection (CIIP) is nuanced yet inclusive, and gives a good overview of the scope of the issue:

> *Critical information infrastructure is a broad concept that designates both the information itself (the data flow) and the channels through which information is created and conveyed (mainly computer networks). Consequently, CIIP is usually understood as including both the protection of data (including issues of privacy) and the protection of information infrastructure (also called 'network security').*[51]

Clearly, the machinery of CI can be viewed in a variety of ways depending on its purpose (economic, social, political, etc.). Though ambiguous criteria for CI may allow for a measure of

48 Myriam Dunn Cavelty, 'Critical Information Infrastructure: Vulnerabilities, Threats and Responses', *UNIDIR Disarmament Forum,* 2007, No. 3, p. 17, http://www.unidir.org/bdd/fiche-article.php?ref_article=2643.

49 European Commission, *Green Paper on a European Programme for Critical Infrastructure Protection – COM(2005) 576 final*, 17 November 200), p. 19, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF.

50 US Department of Homeland Security, *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, November 2012, p. 10, http://www.dhs.gov/files/publications/blueprint-for-a-secure-cyber-future.shtm.

51 'The CIIP sector presents a number of particularities compared to other CIP sectors. First, it can be said that, with the spread of IT within our societies, virtually everyone has become a potential weak link of IT security. Consequently, protecting critical information infrastructure is particularly challenging, as it involves an almost infinite number of stakeholders. Secondly, information is an area where national boundaries have little relevance and interdependency is the norm. Therefore, in this sector more than in others, national protection policies will have to be complemented by co-operative multilateral efforts.' Lord Jopling (Special Rapporteur), *162 CDS 07 E rev 1 – The Protection of Critical Infrastructures* (2007).

flexibility and adaptation, this would seem to be outweighed by the potential for inefficient use of scarce resources. Public-sector clarity over what is critical will make it easier to develop and enforce security regulations for CI.[52]

We may be nearing the point where distinctions between 'infrastructure' and 'information infrastructure' are irrelevant, as the two merge into one ever-expanding circle of critical 'stuff'. As the dependence on cyber-enabled infrastructure increases, so too does the proliferation of critical 'nodes' (i.e. points in a system where failure would significantly degrade the network). This may signal a need for new methods of prioritization. This could be done by ranking critical nodes at the national and international levels. It could also be a single grouping that examines nodes at a global level and ranks them according to how disruptive their failure would be to a given nation – from 'minimally important' to 'super-critical'.

When debating the prioritization of CI sectors, it could be argued that preservation of the status quo (i.e. maintenance of societally indispensable functions) is the quintessential purpose of security. Barring sudden shocks that increase demand for a specific product or service, traditional CI sectors and basic societal needs (e.g. energy, food and water) are likely to remain largely static at the macro/national level. Evolution and innovation will take place more rapidly at the fringes – in the high-risk/high-reward space (e.g. technology start-ups, new fundraising models) – through advances that improve an existing product or service or offer something new.

The diffusion of these advances (e.g. socio-technical platforms such as social media) and the shift in societal expectations that occurs (e.g. expectations of constant connectivity) take time. What matters is the ability to adapt to these fringe changes, gradually adapting and adopting them into the centre and into the mainstream. It is an essential component of maintaining the status quo and over time enabling it to evolve in a direction deemed optimal by society.

52 John Moteff and Paul Parfomak, 'Critical Infrastructure and Key Assets: Definition and Identification', Congressional Research Service, October 1, 2004, p. 16, http://www.fas.org/sgp/crs/RL32631.pdf.

4 Prioritization

'Systems often fail because the organizations that defend them do not bear the full costs of failure.'[53]

Tyler Moore and Ross Anderson

Having outlined the increasing complexity of critical infrastructure, some current definitions and the role played by cyberspace (in facilitating and being included as part of CI), we look in this chapter at two closely connected case studies that demonstrate prioritization uncertainty. Rigorous prioritization of key assets and resources is essential. To do this effectively, a system is needed to identify, rank and resource security of the chosen assets.

This is easy to propose but difficult to implement, particularly given the political risks associated with omitting anything that – in hindsight – could be viewed as an overlooked vulnerability. Instead, the temptation is to include anything at the local, regional or national (and even international) level that could be vaguely construed as critical. Criticality inflation (a sibling of threat inflation) is a persistent problem here, as there is little political capital to be gained from a measured and balanced threat analysis.

A rigorous yet adaptable methodology is needed at the identification stage, for both information collection and analysis. It must account for infrastructure that is critical at the local or regional level, and that will feed into a national level risk analysis. The results are likely to have varying levels of confidentiality and will also require regular updating to account for national and international changes that have an impact on CI protection.[54]

US National Asset Database

The US approach to the protection of critical infrastructure over the past decade has remained fixated on the spectre of terrorism. In response, security resources have been expanded dramatically, though they are ultimately finite. In the competition for government funding, this dynamic has created incentives for threats to be framed through a dominant narrative; hence the rise of 'cyber terrorism' rhetoric.

These incentives can produce unreliable data and undesirable policy outcomes, in large part because threat inflation is a viable and profitable driver of policy. In addition, the inherent

53 'This simple insight has profound consequences for a growing number of industries, and it extends to dependability as well as security. For instance, utilities reduce direct, measurable costs by routing control messaging over the Internet; this can raise the risk of service failure, whose costs are mainly borne by its customers. Another example comes from anti-virus software; since infected machines often cause trouble for other machines rather than their owners, expenditures on protection tend to be suboptimal.' Tyler Moore and Ross Anderson, 'Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research', Computer Science Group, Harvard University, March 2011, p. 1, ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf.

54 Lord Jopling (Special Rapporteur), *162 CDS 07 E rev 1 – The Protection of Critical Infrastructures* (2007).

unpredictabilities of policy-making are multiplied in circumstances where political realities – in particular the need to be seen to be doing something – encourage *reaction* as opposed to *response*. This is a common feature of measures taken in response to a security incident or near miss,[55] and often results in an infusion of resources (e.g. the formation of a new department or increased resources), which must then be processed swiftly by the recipient.

This can result in a lack of space or political 'breathing room' for measured analysis, which places a burden on decision-makers to make sound strategic choices swiftly and with little room for manoeuvre. This pressure can result in the misapplication of incentives (e.g. allocating government security funds to states and local communities based on how vulnerable they *feel*), or in long-term delay (i.e. as hurried risk-assessment methodologies gradually evolve towards something approaching best practice).

One example of this is the US Department of Homeland Security National Asset Database (NADB), which was meant to identify and organize critical infrastructure and key resources. In the years after 9/11, as part of the effort to secure domestic assets, The DHS Office of Infrastructure Protection (OIP) was tasked with developing this. Through several phases of collection – accomplished primarily by self-reporting at the state level – the OIP gathered information on a wide variety of critical assets across the United States.

In July 2006, the DHS Office of the Inspector General (OIG) released a report on the National Asset Database and the 77,069 assets that DHS had identified thus far.[56] It reported that the database contained too many low-priority assets, and that DHS goals for building the first generation of the NADB had not been accomplished. It also noted that the database could not yet support 'effective grant decision-making' because 'managers were not familiar enough with, or did not trust the accuracy' of database assets.[57]

Media reports were less restrained, and noted the database list of assets had 'grown exponentially – from 160 (2003) to 28,000 (2004) to 77,069 (2006) – but it is filled with bean festivals, car dealerships, small-town parades and check-cashing stores.'[58] These 'assets' had been submitted by state and local officials and incorporated into the DHS database. In response, DHS officials defended their list, 'which also included petting zoos, doughnut shops, popcorn stands and ice cream parlours', saying the list had not yet been prioritized and that it needed to represent the 'universe of things' that the United States needed to worry about.[59]

55 Bruce Schneier, 'Harms of Post-9/11 Airline Security', *Schneier on Security*, 29 March 2012, https://www.schneier.com/blog/archives/2012/03/harms_of_post-9.html.

56 'According to the IG report, the first data call to the states, made by the Office of Domestic Preparedness in 2003, yielded poor quality data. The IG report described the guidance given states and localities as "minimal". The guidance apparently did tell states, however, to "consider any system or asset that, if attacked, would result in catastrophic loss of life and/or catastrophic economic loss." As a result, assets such as the petting zoos, local festivals and other places where people within a community congregate, or local assets ostensibly belonging to one of the critical infrastructure sectors, were among the assets reported. According to the IG report, many state officials were surprised to learn that additional assets from their states were added to the database, which raises additional questions about how the information was collected.' John Moteff, *Critical Infrastructure: The National Asset Database*, Congressional Research Service, July 2007, p. 6, http://www.fas.org/sgp/crs/homesec/RL33648.pdf.

57 Department of Homeland Security, Office of Inspector General, *Progress in Developing the National Asset Database*, June 2006, p. 17, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-40_Jun06.pdf.

58 Eric Lipton, 'Come one, come all, join the terror target list', *The New York Times*, 12 July 2006, http://www.nytimes.com/2006/07/12/washington/12assets.html.

59 '"What happens the very first day that al-Qaeda attacks a convenience store chain times a dozen across the country?", [Robert B.] Stephan [assistant secretary for infrastructure protection] said. "If al-Qaeda switches to golf courses or amusement parks or whatever, we better have some of those things in the database so that we know what that universe of things is that we have to worry about."' Spencer S. Hsu, 'U.S. struggles to rank potential terror targets', *The Washington Post*, 16 July 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/07/15/AR2006071500726.html?sub=AR.

Congress appeared to be unconvinced by these explanations, and several months later DHS suspended use of the NADB and replaced it with a new tool – the Infrastructure Data Warehouse (IDW). This is meant to be a more dynamic and flexible risk-management tool that will allow federal, state and local authorities to access centralized infrastructure data, which will give them a single view of multiple sources of information. In a 2009 follow-up report, the OIG noted that improvement was taking place with asset identification and prioritization, though DHS needed to communicate more effectively to state and sector partners their goals for the IDW.

It mentioned another improvement, which was the adoption of the 'critical clusters' concept. These are 'groups of related infrastructure that could be impacted by a single hazard', which cumulatively could justify the inclusion of the cluster on a national priority list.[60] DHS identified four gaps in CI risk management, which it hoped the IDW would serve to mitigate.

- *Accessible and quantifiable risk-related information;*
- *Data standards to ensure consistent data;*
- *Common information collection and maintenance processes; and*
- *Information fusion to enable current and complete analysis.*[61]

These challenges are not unique to DHS or the US government. They recall the computer science expression 'garbage in, garbage out', which denotes the impossibility of generating accurate results from inherently faulty, incomplete or imprecise data. The lesson here is that prioritization of CI at the domestic level, much less internationally, is extremely difficult. The process can be derailed or led astray at numerous stages by, for example, linking the quantity of critical local, regional or national assets too closely to government security funding. Nuanced risk analysis mechanisms are available to prioritize these assets, though increasing levels of interdependence militate against accurate prioritization by obscuring or hiding risk inside layers of complex and opaque linkages.

In the United States this process is further complicated by physical factors (scale) and political factors (e.g. the large increase in post-9/11 federal security funds). Specificity is needed in the identification phase, to harmonize the subsequent collection, aggregation and analysis phases. Without this, there is a danger of collecting too much data (e.g. the 'universe' of everything that can go wrong) and lowering the signal-to-noise ratio. This drowns the important in a sea of the trivial, and sacrifices the ability to prioritize security investment meaningfully.

In addition, a vast list of assets needs to be updated regularly to remain relevant and retain value, which requires significant resources. This strengthens the case for unflinching prioritization of CI. This cannot be solely a government exercise, given that the vast majority of CI is privately owned and operated. The private sector will naturally be engaged in this prioritization, and the general public can be kept meaningfully informed (i.e. beyond the rhetoric of rampant vulnerability and impending cyber-Armageddon). It is not just national assets that have to be considered. It is also necessary to expand the scope of enquiry and consider *international* assets that may be critical at a national level and therefore require prioritization.

60 Department of Homeland Security Office of Inspector General, *Efforts to Identify Critical Infrastructure Assets and Systems*, June 2009, p. 11, http://www.oig.dhs.gov/assets/Mgmt/OIG_09-86_Jun09.pdf.

61 Ibid., p. 6.

The rise of the network-state

Identification of critical dependencies at the international level has been equally difficult. The release by WikiLeaks in late 2010 of more than 250,000 US State Department cables shed light on a wide variety of sensitive subjects. One of these cables, classified 'Secret' and sent by Secretary of State Hillary Clinton to all US embassies in February 2009, concerned the 2008 Critical Foreign Dependencies Initiative (CFDI), a process of identifying sites around the world that were perceived as critical to the United States.[62]

The initiative is a joint DHS/State Department project to compile and annually update a 'comprehensive inventory of CI/KR (Critical Infrastructure/Key Resources) that are located outside US borders and whose loss could critically impact the public health, economic security, and/or national and homeland security of the United States.'[63] This project is part of the larger National Infrastructure Protection Plan (NIPP), and is essentially an international version of the DHS National Asset Database. In parallel with the self-reporting at the state level – as in the previous case study – US embassies around the world were asked to submit a list of CI in their host country, and categorization was to be made along three lines:

- *Direct physical linkages (e.g. pipelines, undersea telecommunications cables, and assets located in close enough proximity to the US border for their destruction to cause cross-border consequences, such as damage to dams and chemical facilities);*
- *Sole or predominantly foreign/host-country sourced goods and services (e.g., minerals or chemicals critical to US industry, a critical finished product manufactured in one or only a small number of countries, or a telecom hub whose destruction might seriously disrupt global communications);*
- *Critical supply chain nodes (e.g. the Strait of Hormuz and Panama Canal, as well as any ports or shipping lanes in the host country critical to the functioning of the global supply chain).*[64]

Embassies were not asked to consult with the host government, nor were they required to estimate second-order effects of asset disruption (e.g. cascading effects due to interdependencies). The results – in the form of 259 assets across 65 countries – are enlightening (See Table 1).

The list of dependencies – although in some cases broad, out of date or poorly defined – demonstrates the truly global nature of CI.[65] The list focuses less on military dependencies and more on energy, heavy industry and telecommunications, and reflects a process of CI interconnection that has evolved over decades and has recently been supercharged by the advent and spread of cyberspace. The prominence of pharmaceutical assets is revealing, not only for the number and range of sites scattered around the globe, but for the motivation behind their inclusion – namely that, given the extent of globalized travel and commerce, the impact of pandemics is severe enough to merit high-level consideration.[66]

62 Kim Zetter, 'WikiLeaks Releases Secret List of Critical Infrastructure Sites', *Wired Threat Level*, 6 December 2010, http://www.wired.com/threatlevel/2010/12/critical-infrastructures-cable/.

63 US Secretary of State Hillary Clinton (18-2-2009), 'Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad)', WikiLeaks, WikiLeaks cable:09STATE15113, Released 08-30-2011, http://www.wikileaks.ch/cable/2009/02/09STATE15113.html#.

64 Ibid.

65 Jane Lee, 'WikiLeaks terror target list "out of date"', *Herald Sun*, 7 December 2010, http://www.heraldsun.com.au/news/national/wikileaks-terror-target-list-out-of-date/story-e6frf7l6-1225966960066.

66 Bridgett Kendall, 'Wikileaks: site list reveals US sensitivities', BBC News, 6 December 2010, http://www.bbc.co.uk/news/11932041.

Table 1: Number and share of facilities by type

Facility type	No. of sites	% of sites
Telecommunications	74	28.57
Energy	43	16.60
Pharmaceuticals	37	14.28
Border crossing	24	9.26
Raw material	22	8.49
Port	15	5.79
Military	11	4.25
Industrial	10	3.87
Shipping	12	4.64
Dam	11	4.25
Total	**259**	**100.00**

Source: Adapted from Mark Graham, 'Map of Wikileaks list of facilities "vital to US security"', *floating sheep*, 7 December, 2010, http://www.floatingsheep.org/2010/12/map-of-wikileaks-list-of-facilities.html.

More important than individual sites, however, are the striking implications for national sovereignty in the 21st century. As Geoff Manaugh argues,

> *The sites described by the cable – Israeli ordnance manufacturers, Australian pharmaceutical corporations, Canadian hydroelectric dams, German rabies vaccine suppliers – form a geometry whose operators and employees are perhaps unaware that they define the outer limits of US national security. Put another way, the flipside of a recognizable US border is this unwitting constellation: a defensive perimeter or outsourced inside, whereby the contiguous nation-state becomes fragmented into a discontiguous* networkstate*, its points never in direct physical contact. It is thus not a constitutional entity in any recognized sense, but a coordinated infrastructural ensemble that spans whole continents at a time.*[67]

The cable appears to demonstrate a low level of asset prioritization, though it is admittedly a snapshot in time and does not represent the totality of this or subsequent exercises. Ideally, each iteration of a national 'due diligence' exercise would refresh the asset list and become increasingly specific. Merely being told that the Port of Antwerp is a critical asset is not particularly enlightening, and provides no guidance as to what steps (if any) should be taken beyond initial categorization. Identifying a point of contact at the facility, port or factory would add value, as would regular updates to core asset details (e.g. is a critical vaccine still produced at factory X?).

In terms of CI that spans the globe, the United States sits at the heavily interconnected end of the spectrum, yet all countries are forced to cope with an expanding array of national *and* international infrastructure and assets that are deemed critical. That some elements of this situation are not new or novel does not negate the fact that it is evolving at speed and is guided primarily by commercial incentives. The dominance of telecommunications sites in the cable may be sufficient evidence

67 Geoff Manaugh, *Open Source Design 02: WikiLeaks Guide/Critical Infrastructure, Domus*, Issue 948, 20 June 2011, http://www.domusweb.it/en/architecture/open-source-design-02-wikileaks-guidecritical-infrastructure/.

that the *links* between critical sites (e.g. in the form of the cyber *layer* mentioned earlier) are themselves the most critical assets. In addition, a rare public glimpse into a process such as this reinforces the notion that the United States has 'inadvertently made clear a spatial realization that the concept of the nation-state has changed so rapidly that nations themselves are having trouble keeping track of their own appendages.'[68]

This in turn raises a host of questions. Will it require a crisis to motivate policy-makers to reconsider the risks that society has implicitly accepted through the national and international growth of CI 'appendages'? How disruptive does a 'black swan' event have to be for cost-benefit analyses to swing in favour of retrenchment, on-shoring or asset nationalization? When might the expense of maintaining sovereign capability in a niche area be considered acceptable? Taking the long-term perspective, at what point do the systemic societal risks associated with global CI dependencies outweigh the benefits? These questions go to the heart of evolving network-states, and the ecosystem of critical infrastructure and assets that comprise and support them. Cyberspace is the connective tissue of these global CI connections. The benefits of this connectivity are apparent and immediate, while the risks are often opaque and deferred. The challenge is to not let the inevitable imbalances grow beyond the reach of corrective measures.

68 Ibid.

5 Pathways for Progress

'There is always an easy solution to every human problem – neat, plausible, and wrong'
H. L. Mencken[69]

Having examined varying conceptions of critical infrastructure as well as case studies demonstrating prioritization or the lack thereof, the question remains: what can be done to better delineate and defend CI, given the exponential complexity facilitated by cyberspace? This is a system like no other. It is vast, with dense interconnections and feedback loops, and is expanding to accommodate tens of millions of new users every year.

Proposals to re-engineer the internet on a grand scale to make it more secure are often offered from a parochial viewpoint, and have little chance of generating sufficient consensus.[70] Instead, layers of upgrades are piled on top of each other, with little possibility of estimating second- or third-order consequences of a failure. Improvements are made where it is possible, at the margins or in specific areas (e.g. through technical measures such as Domain Name System Security Extensions – DNSSEC).[71]

In many ways the problems of infrastructure protection parallel larger concerns about the effects of globalization. Both are driven by dynamics beyond the control of any single nation, yet both significantly affect all nations. Likewise, some pathways for progress are similar (e.g. development of norms of behaviour), though others are unique to cyberspace (e.g. coping with the large number of known and unknown actors).

Adapt

High levels of uncertainty – regarding threats, vulnerability and impact – serve to cloud nearly every aspect of discussions about cyber security as it relates to critical infrastructure protection. This places a premium on adaptable postures, policies and procedures, which can be moulded to changing circumstances. In return for its many benefits, there is a need to accept that cyberspace currently operates at a higher level of chaos than we have become used to in the more highly evolved physical domains. According to Dr Min Basadur, 'while efficiency implies mastering a routine, adaptability means mastering the process of deliberately changing

69 H. L. Mencken, 'The Divine Afflatus', *A Mencken Chrestomathy*, chapter 25, p. 443 (1949), http://www.bartleby.com/73/1736.html.
70 Ryan Singel, 'Cyberwar Hype Intended to Destroy the Open Internet', *Wired Threat Level*, 1 March 2010, http://www.wired.com/threatlevel/2010/03/cyber-war-hype/.
71 ICANN, 'DNSSEC – What Is It and Why Is It Important?', http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm.

routines. To remain viable today, organizations must mainstream adaptability thinking and get it to be part of the day-to-day fabric of the organization.'[72]

Basing cyber security risk assessments on perceived risk is a tempting substitute for quantitative analysis, largely because the accuracy of cyber risk metrics is highly variable. For example, what is the likelihood that an organization will suffer a denial of service attack, or a targeted phishing expedition aimed at extracting valuable data? And with the anonymity provided by cyberspace (at least with immediate forensic analysis), what chance is there of identifying – much less prosecuting – the attackers? The range of potential motives, means and opportunities in cyberspace are beyond the scope of any risk measurement tool, and the rapid expansion of such a complex socio-technical system makes this condition a permanent state of affairs.

It does not necessarily follow, however, that all attempts at evidence-based policy-making are in vain. Those metrics that are available, supplemented by qualitative analysis, can provide a foundation on which to design responses. However, these responses must be designed to account for the limits of knowledge, and be sufficiently adaptable to handle a range of plausible threats.

So how can adaptation be encouraged? For the public and private sectors, there is a need to acknowledge the uncertainty inherent in complex adaptive systems.[73] Efficiencies are gained through interconnection, but so are dependencies and, by extension, potential vulnerabilities. If the financial crisis of 2008 has demonstrated anything, it is that opaque or obscured risk is dispersed risk – that may ultimately be owned by everyone. Acknowledging cyber uncertainty in complex CI systems brings with it political risk (i.e. it implies lack of control), but so too does denying or ignoring uncertainty. The lack of control is real, and denial is not a strategy.

> There is a need to acknowledge the uncertainty inherent in complex adaptive systems.

The extent to which this perspective on uncertainty is embraced or meaningfully acknowledged is likely to hinge on the level of perceived control. Governments that believe they can control their cyber environment (e.g. 'full spectrum dominance') are likely to resist the realities of a domain that erodes hierarchies and devolves power. For this reason, the debate about adaptation – and about the contraction or expansion of CI dependencies (both national and international) – must be a public one. The topic is of fundamental societal importance and should not be discussed behind closed doors. Each country has to identify for itself the optimal point on the spectrum between risk and reward, and governments that can engage the public in this conversation will increase the rate at which large-scale adaptation takes place.[74]

Prioritize and bound dependence

Rigorous prioritization is needed when deciding where to invest in protection of critical infrastructure. As the case studies note, few decision-makers are willing to accept the political risk

72 Jeff Conklin, Min Basadur and G. K. Van Patter, 'Rethinking Wicked Problems: Unpacking Paradigms, Bridging Universes (Part 2 of 2)', p. 6, *NextDesign Leadership Institute Journal*, 2007, http://issuu.com/nextd/docs/conv30.

73 Dunn Cavelty, 'Systemic cyber/in/security – from risk to uncertainty management in the digital realm'.

74 Patrick Kingsley, 'How tiny Estonia stepped out of USSR's shadow to become an internet titan', *The Guardian*, 15 April 2012, http://www.guardian.co.uk/technology/2012/apr/15/estonia-ussr-shadow-internet-titan.

that comes with removing an item from the 'critical' list. The temptation is to widen the circle of things that are considered critical. This level of ambiguity is both wasteful (i.e. resources are not directed to where they can have the most impact) and strategically unwise (given the increasing rate of dependence between CI and cyberspace). There is a need to delineate or otherwise bound CI dependence in order to bring risk within quantifiable parameters.[75] Choosing not to do this is implicit acceptance of unknown amounts of risk.

According to Dan Geer,

> *The source of risk is dependence, and especially dependence on expectations of system state. My definition of security itself has co-evolved with my understanding of risk and risk's source to where I today define security as the absence of unmitigatable surprise. It is thus obvious that increasing dependence means ever more difficulty in crafting mitigations, and that increasing complexity embeds dependencies in ways such that while surprises may grow less frequent, they will be all the more unexpected when they do come, and come they will.*[76]

Benefit can also come from a closer examination of the meaning of 'minimal operation', particularly as it applies to highly networked CI. Cyberspace itself is in the process of becoming CI, but the result is that the risk parameters and understanding of what is 'minimal' are being widened to an immeasurable degree. In many ways this process has occurred by default.

As more societal functions have come to depend on cyberspace and the efficiency it brings, economic logic dictates the elimination of reversionary modes of operation (e.g. decreasing use of cheques and closure of bank branches in favour of online banking) as well as redundancy (e.g. back-up or alternative systems for continuing to bank online). In the long term, however, when 'normal accidents' happen in 'complexly interactive systems with tight coupling',[77] modes of reversion or redundancy are dusted off by grateful users.

In some sectors it may be necessary to bound or otherwise restrict cyber dependence at a predetermined level. This may involve limiting dependence on complex networked systems selectively (and accepting a measure of inefficiency) until better quantitative or qualitative measurements allow for a more complete understanding of the risks that are being accepted. There may also be a need to consider more closely what an optimum societal level of connectedness and dependency might look like, and whether this is possible to measure.

There is also a public awareness aspect of this discussion. Ambiguity or digital obscurantism may advance some interests but does not serve the public good. More specificity is needed regarding infrastructures that are defined as critical.[78] This debate would benefit from being held

75 Dan Geer, 'Criticality, Rejectionists, Risk Tolerance', *Source Boston Conference*, 18 April 2012, p. 5, http://geer.tinho.net/geer.sourceboston.18iv12.txt.

76 Ibid. pp. 3 and 11. Geer adds: 'Risk is a consequence of dependence. Because of shared dependence, aggregate societal dependence on the Internet is not estimable. If dependencies are not estimable, they will be underestimated. If they are underestimated, they will not be made secure over the long run, only over the short. As the risks become increasingly unlikely to appear, the interval between events will grow longer. As the latency between events grows, the assumption that safety has been achieved will also grow, thus fuelling increased dependence in what is now a positive feedback loop.'

77 Charles Perrow, 'Organizationally Induced Catastrophes', Institute for the Study and Environment, 29 May 2000, http://www.isse.ucar.edu/extremes/papers/perrow.PDF.

78 'None of the (US) definitions of what constitutes a critical infrastructure, given over the years, could be considered rigorous. They bound the issue somewhat, but leave plenty of room for interpreting which infrastructures fit the definition.' John Moteff, Claudia Copeland, and John Fischer, 'Critical Infrastructures: What Makes an Infrastructure Critical?', in Mathew T. Cogwell (ed.), *Critical Infrastructures* (Nova Science, 2003) p. 24.

openly. If these infrastructures truly are of societal importance, it seems natural that a society would participate in the discussion over levels of criticality. Such a discourse would serve to promote a more nuanced and widespread understanding of the level of interdependence that permeates modern life. The extent of interdependence will surprise many, but an open discussion is a necessary step towards alleviating the anxiety and misunderstanding that permeate public conceptions of technology and CI in particular.

Methods of analysing a CI sector (e.g. 'food') and narrowing it down to a manageable set of truly critical sub-sectors are even more essential now that dependencies are spreading ever further beyond borders. At the highest level of prioritization this information will be confidential, but methodologies of information collection and categorization must continually be refined in order to avoid being swamped by the 'universe' of potential vulnerabilities. An 'all-hazards' approach – that captures naturally occurring disruptions – is preferable to one that focuses on terrorism or malicious actors. In addition, a more nuanced public understanding of dependency and criticality increases the potential for individual or group resilience to inevitable disruptions.

Balance incentives

Critical infrastructure is the main area of overlap between the cyber security interests of the public and private sectors. All of society has an interest in the efficient functioning of CI, and although the vast majority is privately owned there are compelling public interest reasons for government scrutiny of security measures. This overlap of interest also prevents the public and private sectors from pursuing their goals with the relative autonomy they have in non-critical sectors, because systemic failure is too painful for too many people.

Both sectors have the same basic strategic interest: to ensure provision of CI services. However, from this point onwards there is significant divergence of incentives. In cyberspace, the majority of the commercial world tends to prioritize speed over security, for perfectly rational reasons (e.g. competitive advantage, speed to market, etc.). Yet governments have priorities that focus less on commerce and more on delivering services to society at a politically optimum level (i.e. at a level adequate to sustain political advantage).

It has been argued that the current state of cyber security – in particular cyber defence – demonstrates market failure.[79] However, it could also be thought of as market inadequacy, an inability of private-sector actors to deliver a public good (defined here as a societally optimum level of cyber security in CI) because a portion of it falls firmly outside their *raison d'être*.[80] In essence societies are grappling with a 'risk gap', whereby more security is needed than the free market can (or chooses to) supply, and the 'risks to society … are greater than the company's business model allows for'.[81]

79 James Lewis, 'Rethinking Cybersecurity – A Comprehensive Approach', Sasakawa Peace Foundation, 12 September 2011, http://csis.org/files/publication/110920_Japan_speech_2011.pdf.

80 'Security improvements are generally expensive and usually provide no added efficiency to an organization. Put another way, there is little financial incentive for private firms to invest in a socially desirable level of security, as the true cost of an attack to society is much larger than the damage this attack would cause to a private firm.' Michael Jopling, '157 CDS 08 E rev 1 – Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures', NATO Parliamentary Assembly, 2008, p. 6, http://www.nato-pa.int/default.asp?SHORTCUT=1478.

81 Bruce Schneier, Comments at the RSA Conference 2011 panel on 'Cyberwar, Cybersecurity, and the Challenges Ahead', http://www.youtube.com/watch?v=ieRLVBe3aug.

Conversely, Robert David Graham has stated that

> *the free market is what determines how valuable cyber security is in the first place. […] In other words, people claimed to want security […] they claim security has infinite importance, but behave as if it's a trade-off. The free-market captures this true value, government regulation doesn't.*[82]

This holds true at an individual level but breaks down at the national level. Some of this debate depends on the extent to which cyberspace is considered a public good. This is an environment where certain components – such as national defence and threat and vulnerability information – can reasonably be considered a public good, while others – such as many commercial transactions – are a private good.[83] The free market contributes to the development of public goods to the extent that economic actors are paid to do so. Without the potential for profit, these actors are content to sit back and let taxpayers shoulder the risk of building motorways and sanitation systems as well as the instruments of national defence.

To what extent can a distinction be made between public and private goods in cyberspace, in particular between national defence and everything else? What kind of intervention and how much is needed to adequately protect these elements of cyberspace that are public goods? Taking cues from environmental regulation has been suggested (from the perspective of cyberspace as an environment) as well as 'regulating results not technology' as the former will encourage innovation while the latter will stifle it.[84]

Greater efficiency and productivity are being extracted from cyberspace as CI expands and matures around the globe. Because of this, governments have a particularly difficult balancing act between actions to increase security (or otherwise govern aspects of cyberspace) and actions to preserve what is often viewed as an economic golden goose.[85] These dual actions (not always in contradiction) are familiar to industrial regulators.

Any policy that does not acknowledge the economic and political incentives of the actors involved will not succeed in the long run. How can cyberspace be developed into a more secure environment? Advocates of information sharing between the public and private sectors are treading a well-worn path. But why is this sharing needed now more than before? For the simple reason that situational awareness for everyone is more limited than it used to be when CI was primarily in the hands of governments – i.e. when CI was both less globalized and less privatized.

This is ultimately an argument for prioritization. A possible mission statement could be 'cooperate where it will ease the most societal harm' (with acknowledgment that 'harm' is a contested concept). By this measure, the reduction of cyber crime would seem to be a primary objective, given the damage it produces across multiple elements of society. Others will nominate espionage, though this is an area that suffers from incomplete or asymmetric information (i.e. all parties lack sufficient information to make informed decisions and/or one party holds a majority of information, allowing it to dominate the debate).[86]

82 Robert David Graham, 'Freakonomics vs Cybersecurity', Errata Security, 9 December 2011, http://erratasec.blogspot.com/2011/12/freakonomics-vs-cybersecurity.html.

83 Paul Rosenzweig, 'Cybersecurity and Public Goods: the Public/Private "Partnership"', in Peter Berkowitz (ed.), *Emerging Threats in National Security and Law* (2011), pp. 7–11, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

84 Schneier, Comments at the RSA conference.

85 Michael Joseph Goss, 'World War 3.0', *Vanity Fair,* May 2012, http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking.

86 Ross Anderson and Tyler Moore, 'Information Security Economics – and Beyond' (Information Security Summit 2008), p. 3, https://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf.

Invest in resilience

Resilience, or 'the ability of a substance or object to spring back into shape', according to the *Oxford English Dictionary*, is of increasing relevance as complex systems proliferate. In part this is because of the difficult of measuring levels of dependence. A dynamic model of dependence would be both immensely difficult to construct, and given its inherent complexity it would be out of date upon completion.[87] Resilience and redundancy both serve to bound dependence. They offer a level of insurance – though often at a non-negligible cost – to offset the dependencies that can be measured, as well as those that cannot be measured with meaningful accuracy.

Both societal and physical resilience are necessary when dealing with critical infrastructure and cyber security. The physical/logical elements of security often appear more tangible, but bolstering public confidence in the CI ecosystem and its governance is essential to avoid policy-making driven by a reactive or superficial motives.[88] A widespread infrastructure failure/crisis would certainly drive change, though decision-making in such an environment increases the likelihood of unintended consequences.

Resilience is important because interconnections create efficiency but increase dependency. When done at on a large scale this tends to bring parts of the system closer to the edge of collapse (by systemic optimization, i.e. elimination of redundancy). These connections bring significant benefits and increased efficiencies, but as always there are trade-offs. When the 'natural accident' occurs the damage can cascade in unpredictable ways, but the very connections that caused the collapse to spread will also help the system to recover. In the case of the 2003 blackout in the Northeast US (caused by cascading failures, not hackers[89]) it was noted that 'the interconnectedness of the grid makes it easier to compensate for local variations in load and generation but it also gives blackouts a wider channel over which to spread.'[90]

Resilience militates against vulnerability in complex systems (which can vary by the day or even by the hour), and helps to insure against costly damage.[91] A certain amount of this risk can be mitigated through standard insurance and reinsurance mechanisms (which are still being adapted for cyberspace).[92] Yet persistent questions remain. Where is the balance point between increased resilience and expenditure? Does a tenfold increase of expenditure equal a tenfold increase in security? It does not, and few organizations have the ability to increase cyber security expenditure by 10 per cent, much less 100 per cent. Even if this were feasible, decreasing marginal utility militates against such a large increase in consumption of cyber security products.[93] Without limiting societal dependence in critical areas, how much risk can we reasonably expect to

87 Cornish et al., *Cyber Security and the UK's Critical National Infrastructure*, p. 27.

88 The risk here is entanglement in the classic security syllogism: 'something must be done, I am doing something, something has been done.' Cory Doctorow, 'Lockdown: The coming war on general-purpose computing', Keynote speech to the Chaos Computer Congress, December 2011, http://boingboing.net/2012/01/10/lockdown.html.

89 Kevin Poulsen, 'Did Hackers Cause the 2003 Northeast Blackout? Umm, No', *Wired Threat Level*, 29 May 2008, http://www.wired.com/threatlevel/2008/05/did-hackers-cau.

90 J.R. Minkel, 'The 2003 Northeast Blackout – Five Years Later', *Scientific American*, 13 August 200, http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

91 'The threat is failure of a high-voltage transformer through a physical or cyber attack; a new transformer can take 2 to 3 months to install and has a long manufacturing lead time (often more than 18 months), and there is limited/no domestic manufacturing capability.' United States Department of Energy, *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (2010), p. 70, http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.

92 Michael Mainelli, 'Cyber Re: A Reinsurance Proposal for UK National ICT Infrastructure Security & Competitiveness', Z/Yen Group, 2011, http://www.zyen.com/PDF/Cyber%20Reinsurance.pdf.

93 'As a consumer consumes more and more units of a specific commodity, the utility from the successive units goes on diminishing.' Economics Concepts, 'Law of Diminishing Marginal Utility', http://economicsconcepts.com/law_diminishing_marginal_utility.htm.

manage? Methods of redundancy and reversion reduce efficiency under normal circumstances but mitigate the risks of things going wrong. The problem arises when applying this to cyberspace, where risk is extremely difficult to quantify, and where expenditure is difficult to justify even in the best of financial climates.

One pathway for progress is through the development of prioritization methodologies such as the concept of 'lifeline systems', 'which was developed to evaluate the performance of large, geographically distributed networks during earthquakes, hurricanes, and other hazardous natural events'.[94] This is even more important for cyber infrastructure and infrastructures that are heavily dependent on cyberspace. The discussion about CI prioritization is also about societal resilience, and could gain wider acceptance and adoption with public consultation. As noted earlier, an 'all hazards' approach is helpful and can also serve to discourage repetitive threat disorder – i.e. perpetually focusing on the next potential cyber scare (similar to the decade-long search for the next manifestation of al-Qaeda).[95]

Resilience can also be a response to lack of effective governance. Cheap technology has combined with privatization of infrastructure and other public services to create informal economies of people who organize and cooperate to survive, and in some cases invest in their own infrastructure.

As described by Robert Neuwirth, the number of resourceful and ingenious people who operate in these unlicensed and ungoverned spaces is growing. Known in French as *débrouillards*, these motivated individuals are forming their own underground economies, known collectively as *Système D*, a slang phrase taken from French-speaking Africa and the Caribbean.

> *Also known as* l'économie de la débrouillardise. *Or, sweetened for street use, Système D. This essentially translates as the ingenuity economy, the economy of improvisation and self-reliance, the do-it-yourself, or DIY, economy. […] The digital divide may be a concern, but System D is spreading technology around the world at prices even poor people can afford. Squatter communities may be growing, but the informal economy is bringing commerce and opportunity to these neighbourhoods that are off the governmental grid. It distributes products more equitably and cheaply than any big company can. And, even as governments around the world are looking to privatize agencies and get out of the business of providing for people, System D is running public services – trash pickup, recycling, transportation, and even utilities.*[96]

In many parts of the world resilience is a socially self-organized substitute for a lack of effective governance. Resilience comes in many forms, and it would be a mistake to conceive of it solely in terms of provision by a corporation or nominally sovereign entity.

94 'Lifelines are grouped into six principal systems: electric power, gas and liquid fuels, telecommunications, transportation, waste disposal, and water supply. Taken individually, or in the aggregate, all of these systems are intimately linked with the economic well-being, security, and social fabric of the communities they serve. Thinking about critical infrastructure through the subset of lifelines helps clarify features that are common to essential support systems and provides insights into the engineering challenges to improving the performance of large networks.' Thomas O'Rourke, 'Critical Infrastructure, Interdependencies, and Resilience', National Academy of Engineering, *The Bridge*, Vol. 37, No. 1, Spring 2007, p. 23, http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx.

95 Jason Burke, 'Stop looking for the next al-Qaida', *The Guardian*, 25 December 2011, http://www.guardian.co.uk/commentisfree/2011/dec/25/stop-looking-next-al-qaida.

96 Robert Neuwirth, 'The Shadow Superpower', *Foreign Policy*, 28 October 2011, http://www.foreignpolicy.com/articles/2011/10/28/black_market_global_economy?page=full. In English this concept could be roughly translated as 'make do and mend'.

6 Conclusion

The challenges of CI complexity are significant and growing, and are compounded by imprecise language and bureaucratic inertia. An outcome-based approach is likely to meet with wider stakeholder acceptance, as opposed to detailed proscriptions or regulations. The pathways for progress (detailed above and encapsulated below) attempt therefore to frame these challenges from a big-picture perspective. They provide a way of addressing the issues that cause the most pain, while leaving room for individual organizational interpretation and implementation.

- **Adapt:** Accept uncertainty where possible. Encourage and mainstream adaptability thinking within organizational hierarchies. This may involve restructuring or coordination between departments that deal with strategic direction, risk management and value chain dependencies.
- **Prioritize:** Scrutinize upstream and downstream risks. Consider restricting dependency where uncertainty is too high and unowned risk too great. Which links in a value chain are subject to the highest levels of risk, and where is risk poorly understood?
- **Incentivize:** Acknowledge the economic and political incentives that guide stakeholder behaviour. Higher levels of cyber security tend to lead to higher transaction costs in cyberspace, meaning that policy interventions should be calibrated with a long-term perspective and awareness of second- and third-order consequences.
- **Invest:** In societal, physical, and cyber resilience. Prioritize dependencies that also enhance resilience or redundancy. Exploit areas where commercial and societal resilience overlap, and gains in both areas can be made simultaneously through focused investment.

These recommendations are indicative of a complex and uncertain environment. Many governments are attempting to reduce this uncertainty and extend or consolidate their influence in cyberspace, in part by establishing a framework of international norms, values and principles. Some of them are aided by the technological and human capacity benefits provided by the 'first-mover advantage', though this qualitative edge is likely to diminish as cyber actors proliferate and contest the primacy of any single actor.[97] Although these attempts to exert influence and gain advantage are to be expected, cyberspace will continue to evolve and seek equilibrium, and may at times function at a higher level of chaos than society is accustomed to in land, air, sea and space.

97 Many complex systems have common underlying properties that permit increasingly accurate analysis of system structures and interactions between system components. 'The evolution of many complex systems, including the World Wide Web, business, and citation networks, is encoded in the dynamic web describing the interactions between the system's constituents. Despite their irreversible and nonequilibrium nature these networks follow Bose statistics and can undergo Bose-Einstein condensation. Addressing the dynamical properties of these nonequilibrium systems within the framework of equilibrium quantum gases predicts that the "first-mover-advantage," "fit-get-rich," and "winner-takes-all" phenomena observed in competitive systems are thermodynamically distinct phases of the underlying evolving networks.' Ginestra Bianconi and Albert-László Barabási, 'Bose-Einstein Condensation in Complex Networks', *Physical Review Letters*, Vol. 86, No. 24, 11 June 2001, http://www.barabasilab.com/pubs/CCNR-ALB_Publications/200106-01_PhysRevLtr-Bose-Einstein/200106-01_PhysRevLtr-Bose-Einstein.pdf.

Conceptions of critical infrastructure are trying to keep pace with this evolution, and with advancing technological change and higher degrees of interconnection. There is a risk that the current lack of conceptual clarity will give rise to ever-broader categories of what is 'critical', when in fact prioritization is essential. Organizational models that cannot reach sufficient levels of consensus, for instance the fractured debate over internet governance, will have difficulty gaining traction on a global level.[98] Given that CI in many countries has become globally interdependent, it is essential that a more public discussion takes place regarding the nature and extent of risks that have been accepted (often unknowingly) by whole countries.

Viewing a government as a unitary actor fails to understand the nature of bureaucratic politics. Issuing policy announcements and strategic communications is relatively straightforward; sustained, focused and coordinated action across multiple departments is not. Many governments are still at an early stage in their cyber security thinking. This can be seen when organizational mandates to address cyber security are lacking, and lines of responsibility are unclear. In the absence of an existential threat, 'whole of government' initiatives tend to be plagued with inertia, inter-departmental competition and the inherent disconnect between short-term political timelines and strategic initiatives capable of outlasting the current government. They are anything but unitary.

Progress is also predicated on a level of understanding that makes the problem space accessible. In other words, do decision-makers have a clear understanding of the second and third-order consequences of their actions? In some areas it is easier to answer in the affirmative, but cyber security rarely falls into this category. Robust 'red teaming' can be useful under these circumstances, to more accurately assess vulnerability and to prepare for inevitable surprises.[99] It is also helpful to bear in mind the need to reduce the 'work factor' for network defenders while increasing it for attackers,[100] a principle which could be viewed as a Hippocratic Oath for CI protection.

There is therefore a premium on designing policies that elucidate clear first principles and are designed for flexibility and adaptation. Advocating a comprehensive approach based on mutual interests and needs sounds good in principle, but tends to give insufficient weight to the transactional or temporary nature of collaboration between the public and private sectors, as well as to the widely varying incentives on both sides.

Clear first principles can help to 'do no harm' in another way, by easing the societal transition societies are undergoing. A cognitive dissonance exists between societal experiences of security in the physical world and societal expectations of security in cyberspace. People's perception of what danger 'looks like' in the physical environment has evolved over millennia to become highly nuanced. The equivalent warnings, indicators and trust mechanisms for cyberspace are at a very early stage of evolution,[101] and relatively few internet users have developed mechanisms that allow them to recognize danger.

98 Pingdom, 'The (very) uneven distribution of DNS root servers on the Internet', *Pingdom*, http://royal.pingdom.com/2012/05/07/the-very-uneven-distribution-of-dns-root-servers-on-the-internet/.

99 Steven Aftergood, 'Army Red Teams Test Communications Security', *Secrecy News*, 29 December 2011, http://www.fas.org/blog/secrecy/2011/12/army_comsec.html.

100 John Mallery, presentation at the workshop on 'Cyber Security and Global Affairs & Security Confabulation IV', Zurich, 7–9 July 2010, p. 6, icc.ite.gmu.edu/csga2010/John_Mallery.ppt.

101 Bruce Schneier, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive* (Wiley, 2012), pp. 3–5.

On the positive side, the empowerment that cyberspace brings to its many users (approx. 2.405 billion as of July 2012), generates significant innovation, resilience and self-sustainability.[102] This is happening everywhere and at all levels of society, including those countries where the government's reach is marginal at best. On the negative side, highly complex networks are being built, whose emergent properties are unknown and whose tipping points are often obscure. If the current environment appears complex now, one only has to wait until the internet adoption rate at the global level (32.7%) rises closer to that of North America (78.6%). This will amount to billions of additional users, compounded by a sea of networked devices numbering in the tens of billions.[103] With the increasing popularity of wireless devices (relative to wired devices), this growth could easily take place within the lifetime of readers of this report.

The diffusion and adoption rate of emerging technologies has significant room for upward movement.[104] The global saturation point has not been achieved, which means that opportunities will continue to increase at an exponential rate. The global ICT 'skin' – comprised of billions of networked devices – that will connect and provide feedback to these users is likely to become the most critical of all infrastructures. The network-state is on the rise. Equilibrium has not been reached in any area of cyberspace, including in the trade-offs between freedom, security and convenience. The environment continues to expand and become more complex, generating new problems as old ones persist.[105]

Certainty implies control in both physical and virtual domains, yet the internet has been called a 'global machine for springing surprises'.[106] This capacity to generate surprises is unlikely to diminish in the near future, which makes adaptability and prioritization core priorities for CI protection. Many of the most intractable cyber security issues are inherently socio-technical. They truly are wicked problems (i.e. complex, often socio-technical policy problems), yet the anxiety they provoke need not be the focal point of societal interaction with technology.[107] The possibilities are far greater than the dangers – many of which are couched in the kind of dramatic and apocalyptic language that reveals deeper fears of 'technology-out-of-control'.[108]

102 Internet World Stats, 'Internet Usage Statistics: The Internet Big Picture – World Internet Users and Population Stats', *Internet World Stats*, 30 June 2012, http://www.internetworldstats.com/stats.htm.

103 Cisco Visual Networking Index, 'Entering the Zettabyte Era', *Cisco Visual Networking Index*, 1 June 2011, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.html.

104 The Technium, 'Increasing Ubiquity', 28 May 2009, http://www.kk.org/thetechnium/archives/2009/05/increasing_ubiq.php. Adam Thierer, 'On Measuring Technology Diffusion Rates', *The Technology Liberation Front*, 28 May 2009, http://techliberation.com/2009/05/28/on-measuring-technology-diffusion-rates/.

105 'I define complexity as the density of feedback loops. A lot of people say that complexity is the enemy of security – I'm one of them – but at the same time I am here to argue that we have to learn from Nature precisely because Nature is the most complex thing we will ever see. Nature is an existence proof that complexity is not the enemy of life, but complexity is the enemy of stasis. Our problem is that we've pretty much equated security with stasis, and it is slowly getting us into trouble.' Geer, 'Keynote', p. 9.

106 'Vint Cerf and Robert Kahn created what was essentially a global machine for springing surprises. The implication of their design was that if you had an idea that could be implemented using data packets, then the internet would do it for you, no questions asked. And you didn't have to ask anyone's permission. The explosion of creativity – in the form of disruptive applications – that the world has seen since the network emerged in the 1980s may have taken a lot of institutions and industries by surprise, but it was predictable, given the architecture. There are a lot of smart programmers in the world, and the net provided them with a perfect launch pad for springing surprises.' 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.

107 'First coined in 1973 by academics Professor Horst Rittel and Professor Melvin Webber, wicked problems tend to be found in the realm of public and policy planning, where social dynamics add complexity, and progress is often incremental and slow. Examples include climate change, narcotics trafficking, urban planning, gang crime, health care and cyber security. These problems resist easy definition (i.e. there is little or no shared understanding of the problem) and are complicated by independent or interdependent stakeholders, each of which advocates their own preferred definition and "solution" to the problem.' Dave Clemente, 'Cyber Security as a Wicked Problem', *The World Today*, October 2011, http://www.chathamhouse.org/sites/default/files/TWT1011p15cyber.pdf.

108 Sean Lawson, 'Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History', Mercatus Center – George Mason University, January 2011, p. 2, http://mercatus.org/publication/beyond-cyber-doom.

Government policies can shape the landscape for better or worse, but there are no solutions that will satisfy all stakeholders, since they are shaped by the subjective perspectives and inevitably limited knowledge of decision-makers. As elsewhere, security in cyberspace – and of critical infrastructure specifically – is a means to an end; it is intended to facilitate the provision of a multitude of social and economic goods. The task facing policy-makers is to design security measures that can achieve societal consensus and preserve the ability of cyberspace to flourish, thrive and provide these goods and wider benefits. This is one of the most difficult policy challenges of the early 21st century, and those that can find an optimal balance between freedom and security in cyberspace will reap rewards that are far greater than the costs.

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