Executive Summary

Cyber Security and Global Interdependence: What Is Critical?

Dave Clemente

February 2013

Read more
www.chathamhouse.org/cyber2013
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

---

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’. 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.

---