Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems

Matthew Jude Egan

Green MultiGen.com, 40553 Saddleback Rd., Bass Lake, CA 93604, USA. E-mail: jude.egan@gmail.com

The world's 'Critical Infrastructure' (CI) has increased in size during the three decades between 1975–2006. CIs are those systems that provide critical support services to a country, geographic area for a corporate entity; when they fail, there is potentially a large cost in human life, the environment or economic markets. This article examines the characteristics of new technologies or services that are becoming a part of the CI, but are not yet. The article attempts to systematically define the characteristics of 'criticality' in order to better anticipate the types of vulnerabilities these new technologies or services create.

Introduction

In the early part of the 21st Century, the challenges posed by building and maintaining CI rose on policy-making agendas across the Western world. While major natural and human-made events during the 1990s and early 2000s have caused the loss of human life and damage to the environment, they have also raised questions about the reliability and security of industrial nations' CIs and their ability to provide both routine and emergency services under stress.

The 2004 tsunami in the Pacific imposed a painfully high cost in terms of human life, but from the policy and preparedness standpoints of industrialized nations, the affected nations were largely still developing their CI capacities and programs. In part, the tsunami's lesson was about what happens when there is inadequate infrastructure to respond to a major natural disaster. However, Hurricane Katrina, just eight months later, should be more troubling to policy-makers in industrialized nations because it implicated the breakdown of emergency services and public health and safety networks that were thought to be functioning and 'in place'. While the tsunami's tragedies were brought about by a relative and well-understood lack, Katrina's tragedies were shocking because they came about in a nation of plenty. Many of the Katrina-related problems arose in traditional CI areas including transportation, water and food delivery systems, sewage, environmental safety and health, and emergency management systems.

It is important to examine whether increasing reliance on large, complex systems for CI services is also increasing our vulnerability to unanticipated events. To answer this question we should know the characteristics of a technology or service that make it a 'critical' part of the CI. Are there observable characteristics such that variations will have predictable effects? This article begins to develop a tool to define and measure 'criticality' that may be useful in protecting CI from systemic breakdowns and the attendant losses to human life and the environment.

The term 'critical infrastructure' is used widely in the governmental, management and academic literatures,

but it has largely been defined by illustration and categorization rather than by a set of characteristics that can be isolated for analysis and prediction. A broad illustration of CI used by the White House includes agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and posts and shipping (White House, 2003). Another broad illustration includes: electric power, air travel, surface travel (roads and mass transit), financial instruments and corporate governance and regulation (easy credit, global banking, property rights, Sarbanes-Oxley Act), the World Wide Web and Internet, as well as, shipping, global insurance markets, day care and university systems (Schwartz, 2003).

A definition in the form of a test suggests that infrastructure elements are critical if they: '(a) provide routine functions along operational paths essential for average or routine system function, (b) no handy, rapid substitutes exist, (c) sudden dysfunction in and around these elements causes nontrivial harm, and (d) they are embedded in wide, functionally reciprocal, integrated systems' (Demchak, 2006: fn 2).

Other definitions, especially coming from the engineering literature, would limit definitions of CI to 'hard' technologies of the 'ducts, pipes and wires' variety (De Bruijne and Van Eeten, 2007). Limiting the definition of CI to hard technologies allows managers to limit their focus to particular types of vulnerabilities affecting those technological systems. CI is built with hard technologies, but as it has grown in scope and scale, its structure has transformed to include software and networks of people and machines. Thus, socio-technical systems-oriented thinkers have shown that integrating human dynamics in the study of complex systems is essential for there to be any hope for high reliability and public trust and confidence over the long term. The 'softer' systems oriented category is more expansive and complex than the hard technologies category and, thus, requires a greater investment of resources to manage reliably.

These definitions aside, even the broadest definitions of CI systems seem to be expanding. This is because: 1) systems are adding new critical elements based on technological advances to infrastructure systems, 2) systems thinkers are better mapping nodes of criticality within systems and discovering new areas of criticality, and 3) increasing globalization and the 'rafting' of CI components together to gain efficiencies are expanding the reach and the criticality of infrastructures. The focus in this article is on the set of systems that are becoming increasingly critical and 'infrastructural', systems that are not part of the CI in their current state but which may be in the years to come. Also included are systems that are currently CI but which are devolving into non-criticality and/or infrastructurality, because each of these categories of evolving or devolving criticality brings about new vulnerabilities.

Even though the CI category has expanded rapidly during the past three decades, little has been done to systematically define the characteristics of a technology or service that make it critical. Each addition of critical elements or systems to the existing infrastructure causes a variation in vulnerability to failure, making the definitions of 'infrastructurality' and 'criticality' important to anticipating future challenges.

'Infrastructurality', as it is used here, focuses on the dependency of a given system to the particular elements that support it; infrastructurality would then vary with the support technology or service's impact on system reliability. Mitigating factors could include redundancy, system design for 'elegant failure', and ability to compartmentalize support systems to ensure that failures in one sector do not 'cascade' into others. Other important distinctions can be made between urban and rural infrastructure, soft (virtual and sociological) and hard (physical) technologies, and technologies with high capital costs and those that are relatively low.

This article focuses on the 'critical', or vulnerability-inducing, elements of infrastructure technologies or services. Criticality, like infrastructurality, is relational; it largely varies with the amount it is relied upon. A consequence-oriented definition of CI suggested by Prieto includes systems whose failure would lead to unacceptable human or economic consequences, would impact rescue and response efforts and would 'severely impact' recovery efforts. There may be a tendency in the face of extreme stress to consider more things as CI than can be defended when the stress is gone, i.e. Prieto notes that immediately after the 9/11 attacks everything from footbridges to tall buildings were considered CI (Prieto, 2003).

This article uses the consequence-oriented definition of criticality as a frame of reference, expanding on it below to include some of the elements that make the consequences of infrastructure failure critical. First, the paper provides some background in the concept of reliability and the development and management of 'large technical systems' in order to show how the consequences of systemic failure can be magnified by the type and complexity of the socio-technical systems of which they are a part. Then, the paper shows how increasing usage and reliance on emerging technologies creates vulnerabilities to the shortcomings of those technologies, especially where they have not been fully tested. The paper then uses a consequence-based approach to defining criticality as a baseline. Finally, the paper expands the consequence-based approach by defining other potential areas that may increase

vulnerability as they vary. The appendices break these areas out into a rudimentary framework for analysis.

Reliability Challenges in Large and Complex Technical Systems

Since the mid-1980s commentators have been sounding an alarm about the industrialized world's increasing reliance on complex technological systems to manage highly hazardous operations. Perrow (1984) and Sagan (1993) wrote highly detailed books about the increasing probability of 'normal accidents' in large systems capable of doing grave damage, largely because the systems were growing increasingly complex and difficult for humans to manage and that under stress they were more likely to fail. Crossover books with alarming titles such as *Lethal Arrogance* (Dumas, 1996), *Inviting Disaster* (Chiles, 2002), and *Why Things Bite Back* (Tenner, 1997), have all contributed to this commentary, each showing that an increasing reliance on 'Large Technical Systems' (LTS), increases public vulnerability. A dialogue emerged in the mid-1980s with the documentation of High Reliability Organizations (HROs), large and complex organizations that manage highly hazardous operations and materials, that did not fail under extreme stress (Rochlin, LaPorte and Roberts, 1987; Weick, 1989; Rochlin, 1996). Though they identified characteristics that highly reliable organizations shared, HRO scholars argued that the success of these organizations against the odds would be difficult to impossible to replicate and maintain.

While there has been some disagreement between scholars in the LTS field, the body of work shares some characteristics: 1) creating reliability over multiple management generations in complex, tightly coupled systems is difficult and extraordinarily demanding and 2) the hope of doing so grows increasingly distant as technological systems grow larger and more complex. In addition to these two characteristics such systems also increase in criticality, they produce greater vulnerability. The proliferation of large, complex and tightly coupled systems, especially in private CI management, has led to an ongoing discussion across disciplinary lines about how to manage them for optimal reliability.

LTSs: 'rafted' networks

Many modern technologies have evolved into large and complex technical systems: 'spatially extended and functionally integrated socio-technical networks' such as electrical power, railroad, and telephone systems (Hughes, 1987: 11). These systems create vast efficiencies that have allowed for shifts in lifestyle and work especially in industrialized countries – one may even argue that the existence of such systems is what makes a country 'industrialized'. Such systems create benefits for the public and the socio-economic systems they support, often providing infrastructural support for important services and distribution networks. They also, however, create challenges for policymakers in the form of 'negative externalities, the risks of failure and disaster, management, control, and coordination problems' (Mayntz and Hughes, 1988: intro).

A LTS typically supports the missions and goals of more than one organization and is composed of complex systems of machines, humans, rules and bureaucracies that impact and are impacted by the environment around them (Grabowski and Roberts, 1996). LTSs involve 'hard' technologies ('ducts, pipes and wires'), 'soft' technologies (computer software, networks, and the World Wide Web), socio-technologies (bureaucracies, rules and procedures), human operators (including the challenging human-machine interface), and complex networks of relationships between the internal workings of the system and the outside environment in which it operates (Egan, 2005). These systems are spatially extended and functionally integrated socio-technical networks that produce benefits, risks and costs outside the system (Mayntz and Hughes, 1988). Such systems are large and demand resources. They often have multiple management nodes and a dense mix of technologies, regulations and bureaucratic procedures that require both close attention to detail and a wide lens for managing the entire system. They are also likely to undertake a variety of operations from research and development to manufacturing processes (LaPorte, 1991; 1994). This includes such traditional CI functions as transportation networks, electricity production and distribution grids, food and water distribution and telephony (Joerges, 1988; Vicente, 2004).

The LTS will have developed through a planned, or more likely unplanned, 'rafting' together of many different systems, each relying on the next for efficiency, stability and effectiveness. 'Rafting', as it is used here, refers to the joining of different elements to achieve a purpose usually unrelated to the purpose of each of the individual elements. Much like a raft made of many different foraged pieces of flotsam all lashed together with bailing wire, each of which contributes to the overall buoyancy of the watercraft, but none of which was designed specifically for flotation, a LTS is composed of many different technical and organizational elements each of which contributes to the overall function of the system, but few of which were designed to serve a larger system. A LTS adapts to changes in its environment or vulnerabilities it experiences in the form of 'reverse salients' discussed below, by 'rafting' new elements as they are needed, either by foraging for them or by creating them. The result is a device that

has both inherited the vulnerabilities of each of the elements attached to it and compensated for them with other elements, externalizing risk to the public and/or by increasing redundancy, slack, and resilience.

While this leads to efficiencies, the reliability of each element of the CI depends not only on the managerial and technological effectiveness of the LTS as a whole, but also the effectiveness of the other systems that impact it. Thus, when one part of the raft begins to sink, it may also bring down those other parts that are attached to it. LTSs are composed of many interactive and interdependent elements, increasing vulnerability; economists ('transaction costs') and engineers ('friction') alike note that each point of interaction between elements of a system is also a point of vulnerability (Coase, 1960; Cooter and Ulen, 1997; Bea, 2002). This extends reliability concerns to include the possibility that failure in one element of a rafted system can cause a cascading failure throughout the system and generate failures in otherwise stable elements. This means that LTSs are not only vulnerable to the weakest elements that support them but all elements of the LTS are vulnerable to the weakest elements they interact with.

Managing for reliability in LTSs requires managers to understand and account for all potential points of vulnerability with attention to stabilizing forces and potential breaking points. Each point of vulnerability increases management complexity by creating another potential problem for which managers have to find a solution. Stabilizing forces in a LTS can also create greater complexity in the system because managers must account for them when they make organizational and operations decisions (Rochlin, 1997). Further, complexity increases as systems are 'rafted' together with other systems with the vulnerabilities of each new system adding to the vulnerabilities of the entire 'raft'.

Interdependency and criticality externalities

When critical systems are rafted together, the critical elements of each become critical elements of all because of the possibility that failure in one part of one system will be externalized to others. Interdependence between systems and system elements also increases vulnerabilities through 'criticality externalities'. A criticality externality is where the risk of failure from one element of a system negatively impacts other elements.

For example, in a rafted distribution system such as that relied upon by the post-Katrina relief efforts, that relies on rapid and clear communications and electricity systems to allow relief workers to pinpoint those areas that need aid the most severely, a break in the communications hierarchy can place a premium on all information, including rumors and other bad information. These communication difficulties overburden the channels that are actually functioning well, causing supply and aid deliveries to be delayed. The lack of electricity and telephone infrastructure contributed to the problem by reducing the methods by which relief personnel could learn about especially hard hit areas. This overburdening of the communications network contributed to difficulties in getting supplies and aid to the places and people who needed it. Further, the National Guard's deployment elsewhere disrupted a critical part of the post-disaster peacekeeping and emergency services by limiting the number of well-trained personnel on the ground thus contributing to the information flow difficulties. This cascaded into a larger system failure in which the system relied more on its communications systems in order to fix acute problems. This emergency triage delayed aid to areas that needed attention but were not yet in crisis. Without needed services, these areas developed into crises of their own, further taxing the communications and aid distribution network and increasing delivery problems.

The likelihood of 'system failure' – a combination of smaller failures throughout the system that cascades into a larger system-wide failure for which mitigation efforts become complex and difficult – increases with the number or differentiation in the type of critical systems components. Thus, in New Orleans and the Gulf Coast of the United States after Katrina, critical systems included roads, electricity, water and food distribution, emergency and security personnel, and sanitation, including morgue services, each of which was overburdened or nonfunctional. With even one of these critical systems down for an extended period the Gulf would have experienced a systemic challenge, but the scenario that developed implicated all of them at one time, causing nearly total system failure.

Interdependent systems are subject to exogenous forces – those caused by anything outside the system in its 'ecological landscape', such as markets, regulations, competition, public perception, and natural disasters – placed upon them by changes in their environments. Two potential ways of meeting the challenges posed by exogenous forces, redundancy and emerging technologies, may add to vulnerabilities. Critical system redundancy tends not to solve the interdependency problem, in part because redundant systems add system complexity (Sagan, 1993; 2004) and private corporations that provide many CI services do not like to pay for redundant safety systems. Reliance on emerging 'critical' technologies and services presents a special problem because, as they are rushed to market to serve a specific and much needed purpose, they may not be fully tested for design or performance concerns.

If an organization can predict vulnerabilities before they emerge, it can make its own (endogenous) changes to account for them (Auerswald et al., 2006). Thus, while one element of response to changes is to create resilience in the organization – through 'slack' or by developing crisis response systems – another is anticipatory endogenous change that responds to new potentially critical system vulnerabilities.

Slack can be viewed as an organizational 'shock absorber' that ' . . . prevents a tightly wound organization from rupturing in the face of a surge in activity' (Bourgeois, 1981: 30; see also, Perrow, 1994; Rijpma, 1997). This type of buffer can prove particularly important to organizations that are highly affected by their external environment, but which have little control over unanticipated surprises it creates. For example, a power distribution network may not run its transmission lines at full capacity in order to allow for power surges or it may have emergency power generators to meet demand for local critical system function should power delivery be interrupted. This would create a buffer to protect the public in the case of an unlikely event, but it meets with efficiency challenges because slack is treated as 'waste' in most organizations.

Endogenous anticipatory change works best when the organization can predict vulnerabilities stemming from changes in its environment. Anticipatory change may require that electric power companies run lines underground in areas where hurricanes are likely, anticipating the possibility of more frequent and powerful storms.

The two are not mutually exclusive; anticipatory change can, and often should, be based on developing greater systemic resilience to surprises. Both developing resilience and anticipatory change requires taking the long view in an organization, something that is difficult in the current economic climate.

Emerging criticality and 'reverse salients'

Because large socio-technical systems haphazardly raft together support components made up of smaller systems, their expansion often requires the development of technologies and services – socio-technical 'fixes' – that link disparate support systems together. Hughes (1987) calls these socio-technical fixes 'reverse salients'. A salient, according to Hughes is a 'protrusion in a geometric figure, a line of battle, or an expanding weather front'. 'As technological systems expand', he argues, 'reverse salients develop. Reverse salients are components in the system that have fallen behind or are out of phase with the others' (Hughes, 1987: 73). If the reverse salient cannot be corrected within an existing system, it becomes 'radical' and inventors may develop new systems to resolve it (Hughes, 1987: 75). Reverse salients attract inventors, including multiple simultaneous inventions that fill the void left by the expansion. These reverse salients will become 'critical' quickly as they are relied upon by the LTS for its functionality.

Since there is both the possibility of simultaneous invention and the need for a socio-technical 'fix', the technologies or services that fill the reverse salient void usually cannot be fully tested before they are implemented. Since introducing a new technology to a system creates unpredictable interdependencies, the technology should be tested in place to ensure that they do not create vulnerabilities in the system. However, 'in place' testing has the tendency to be rushed where the need is severe. Where solutions to reverse salients are developed by in-house R&D teams, they may be rushed into service to resolve vulnerabilities in the system. Outside developers market 'beta' versions of technologies that have not been fully tested to meet the pressing demand created by the reverse salient in the LTS, often out of fear of losing market share to a competitor. This rush to usage increases vulnerability to unknown consequences of use.

For example, the mobile telephone, which entered the market as business began to demand instantaneous communication, quickly became a critical part of the business world and, eventually, a part of people's personal lives. The reverse salient came about where business and social practices required more travel and on-demand communication. The first generation of mobile phones used by average users was of very poor quality with many dropped calls and limited coverage area. To fill this increasing need for convenience and on-demand communication, the mobile phone came onto the market sooner than its networks could support it and faster than it could be fully tested. Thus, cellular transmission networks were neither completely 'built out' around the United States nor had the companies that owned them developed reliable maintenance and repair networks to keep them in service. Nevertheless, because there were no other options and the societal need for cellular phones increased the more they became available, the demand for them continued to grow. Though many cellular companies held out that their product was a telephone – drawing upon the idea of reliability that Ma Bell had created in the telephone land line – the cellular phone was not useful to most Americans for several years after the first personal plans became available.

The possibility of multiple, simultaneous invention, creates an incentive for inventors to overstate the reliability of their products and rush them to market. While untested technologies or services, which become critical support elements of critical systems, generate huge profits for their inventors and benefits for their users, they also generate negative externalities in the form of an increased likelihood of failure.

The more critical they have become, the larger the cost the failure is likely to have. Thus, benefits that accrue to users and inventors are passed along to the public and those who rely on LTSs as costs in the form of higher risk.

Such technologies may also serve as 'forward salients' (Joerges, 1996), which drive the LTS's expansion. This expansion may increase risk by increasing the potential cost of a system failure. For example, a new technology may allow dams to hold back larger amounts of water, serving a public benefit by making more water available to the public. However, since the new technology allows for greater reliability in building massive dams, it also increases the potential cost of a dam disaster. The likelihood of dam failure may decrease but the potential cost of failure of a massive dam versus a smaller dam is much higher. If some of the critical elements that support the dam's CI are not as reliable as they were believed, the cost of failure could be massive. LTSs are in many ways like increasingly large dams that hold back immense amounts of water, thereby creating the potential for enormous costs. In a perfect world, the technologies that allow for the construction of huge dams would be reliable enough that the construction of massive dams would actually decrease the risk of an accident by reducing the probability of dam failure. The challenges created by the use of technologies to fill the void created by reverse and forward salients (called in popular parlance 'killer apps'), and their quick movement into criticality, however, create a gap in our knowledge about system reliability.

Increasing Criticality

'Killer apps', like the mobile telephone, tend to create their own markets by allowing users to expand their uses beyond what was intended, but they also tend to increase vulnerability in unanticipated manners (Bijker, 1987; Bijker and Law, 1992). When there is multiple simultaneous invention or copycat invention, they will be replaced by newer, better technologies, each replacement process also creating its own share of vulnerabilities.

This occurs regularly in the pharmaceutical industry. Viagra, a drug that treats male erectile dysfunction, was a 'killer app' that immediately had a multibillion-dollar-a-year market after the Food and Drug Administration approved it. Copycat drugs emerged soon afterward, each promising to be slightly better. One of these, Cialis, lasts in the body for thirty-six hours instead of Viagra's four hours and is meant to provide the benefit of sexual spontaneity, but it also led to worries for the Food and Drug Administration, which had to take into account the increased vulnerability to the human body of a drug that persisted in the human body for so long.

In another example, where the main vulnerability for telephone users once was transmission line failure, mobile phones have shifted vulnerability to cellular towers and satellite networks. For the end user, the vulnerability is the same – their phone fails – for the company that provides mobile phone service the reliability constraints require new technological systems, service plans and security. Telephone operators had many years to develop reliability tools and maintenance for wire-based telephone systems, resulting in a telephone network that had been reliably 'built out' even to the most rural locations. Switching to mobile telephone systems requires that operators develop new systems to ensure reliability. Thus, rather than attempting to protect and maintain a 'hard' technological system of wires and switches, a system for which telephone companies had built major service networks to repair and maintain, mobile telephony networks require new systems that both integrate with land lines and require their own maintenance and protection.

The shift from a proven critical communications system with known vulnerabilities and well-established mechanisms for responding to disruption to a reliance on new technologies for the same provision of critical services also creates unproven service networks and spotty reception areas, a vulnerability for those who have come to rely on the mobile telephone. As part of its monopoly right, AT&T was required to 'build out' telephone transmission lines to rural areas to create 'universal connectivity', and a nationwide telephone infrastructure, though the profit centers for the company were in building transmission lines to higher density areas. Mobile phone companies are not required to provide 'universal connectivity', so they focus on high-density areas resulting in an unbalanced system with vulnerabilities in rural areas.

These vulnerabilities are offset by tremendous benefits for stranded motorists, travelers, and those who otherwise need to communicate when they are not near landlines. Providers enjoy enormous profits: instead of having one telephone line for a family of four, they now often have five – four mobile phones and one land line.

That new technologies, especially those in 'beta' testing versions, are prone to technological failure may be apparent; but in early phases, they are also prone to legal vulnerability in areas such as patent law, regulation, monopoly restrictions and antitrust enforcement, each of which is becoming increasingly utilized by both private parties and governmental entities. Legal challenges in any of these areas are especially powerful because the law carries with it the power to terminate, or award cost-prohibitive damages that stymie the use of the technology. Patent cases especially, as the

'reverse salient' problem encourages multiple inventors trying to solve the same problem, can force the more successful and widespread technology to shut down entirely.

For instance, the 2002 patent dispute over the Research In Motion (RIM) Blackberry data processing and delivery technology threatened a system shutdown of a major evolving technological system (mobile email retrieval and response) and the service it provides to professionals and essential government personnel. In 2003, a jury decided that RIM had infringed the patent held by NTP. NTP then filed for a permanent injunction to keep RIM from servicing the Blackberry devices it had already sold and from producing and selling further devices. The United States Justice Department filed a 'statement of interest' in November 2005 asking that any injunction issued by the district court hearing the case not include the 200,000 government workers who rely on Blackberry service. In March 2006, RIM and NTP agreed to settle the issue for over $600 million, thereby averting a possible shutdown of Blackberry service.

Though this vulnerability was not entirely unexpected and Blackberry technology, especially given the competitive market provided by other devices such as the Palm Treo, was likely only at the edge of criticality when the patent dispute emerged, shutting down the network would still have had huge consequences for both government and private entities who had relied on Blackberry technology for mission critical activities.

The technology boom in the areas of computing power and communications that has been occurring since the early 1980s has increased productivity dramatically making processes more efficient, allowing businesses to capture what was previously thought of as 'waste'. Mobile phones and portable computers have transformed previously lost travel time into productive time. Many other technologies that did not exist even two decades ago have transformed business methods and are now taken for granted for the efficiencies they create: 'wi-fi' wireless broadband Internet, ATM machines, quick credit card authorization, spreadsheet software, database technology, email and portable email devices, the transatlantic fiber optic cable and satellite communications systems, video-conferencing systems, the global positioning satellite (GPS) network, the World Wide Web and Google's tremendous searching power, as well as real-time global banking and markets data. These technologies have created an untold amount of efficiency gains and reduced vulnerabilities in a variety of manners, becoming increasingly critical elements of the public and private sectors, including the nation's, and world's, CI.

At the same time, each new technology creates new vulnerabilities, or at the very least, creates areas of unknown consequences. For one thing, these technologies have shifted the managerial burden from experts with deep tacit 'knowledge bases' regarding CI systems to computer engineers whose knowledge is based in computer technologies rather than in the systems they are increasingly responsible for managing (Demchak, 2001; 2003; Schulman and Roe, 2006). There has also been a marked shift in age and experience of managers in the computer security and communications areas. Where mid and senior managers in other divisions were largely older and well-experienced people with doctoral degrees, computer technology divisions are often populated with younger, less-experienced, and less-credentialed people. In some instances this creates an atmosphere of mistrust on both sides, another potential vulnerability (Egan, 2005).

Criticality Levels: A Consequence-Based Approach

If we wanted to change the criticality or infrastructurality of a given sociotechnical system in order to reduce our vulnerability to its failures, while maintaining the benefits from its success, how would we do it?

The article argues above that rapid reliance on emerging technologies and services increases vulnerabilities to the larger systems that rely on them. This rapid reliance also moves the technology toward criticality. One of the characteristics of criticality is how much it is relied upon by other systems. Inventions that solve some of the problems created by 'reverse salients' in LTS operations become critical parts of the infrastructure the more they are relied upon or the faster they replace existing systems.

The criticality spectrum (Figure 1) illustrates how a technology enters the market usually at the 'not critical' stage and becomes increasingly critical as it becomes an important part of the infrastructure. The World Wide Web is an example of a 'forward salient' technology for which there was little need – and which was thus not critical – until it was created; as its uses became more varied and widespread, it also grew increasingly critical. When it is 'critical' the systems that rely upon it would fail without it; thus, power grids are critical because of all of the critical systems that rely on their functionality. Certain technologies also devolve out of criticality as

Not Critical → Increasingly CI-Like → Critical → Devolving from Criticality

Figure 1. Criticality Spectrum.

Table 1. Consequences of Failure

Criticality Table					
Criticality Level	Not Critical	ICIL		CI	
Breadth of Consequences of Failure	None	Narrow or Low Impact	Broad or Moderate Impact	Widespread or Intense Impacts	Widespread *and* Death
Impacts and Cascade Effects	Little impact on either markets or critical systems	Impacts other non-critical systems; could cascade, but likely to have systems in place to reduce the likelihood to near zero.	Impacts critical systems but will not bring them down; some resiliency and redundancy in place; CI system is robust or well-partitioned so it is difficult to take down even with a series of failures	Impacts CI; Could cascade or ripple to bring down multiple elements of a single or multiple systems; very little resilience or redundancy; unique or monopolistic system provision; ubiquitous or widespread usage.	Widespread direct impacts on people or the environment; the CI in place is more containment than service provision, so when it fails, it does so with catastrophic effect; no potential replacement services
Examples	Local emergencies; failure of a non-critical product in the market	Blackberry patent litigation; shutdown of a regional public transportation system such as the Bay Area Rapid Transit (BART) train or damage to a commuter bridge.	Failure of Enron; loss of a single mobile telephony service satellite; failure of portions of the electricity grid; failure of Wal-Mart distribution system	Electricity grids; World Wide Web; Commercial aviation systems	Water and food provision and distribution networks; nuclear fallout; greenhouse gasses and severe climate change; infectious disease
Percentage of Technologies in the Market[a]	90%	8%	1.5%	.49%	$<.01\%$
Likelihood of Being a LTS	5%	5%	5%	10%	90%

[a] It is difficult to estimate the real number of each type of technology in the market. For purposes of this table, the estimates are best thought of as a qualitative description of the relationship between quantities (i.e., there are many more of one type than another) than as a true percentage (i.e., count up all technologies and multiply by percentage to get actual number).

new technologies replace them or the need for them fades; for example, the gasoline automobile engine may be at an early phase of criticality devolution as hybrid technologies begin to take their place.

For an organization, the movement from excellence to failure – or from order to chaos – is often not a catastrophic shift, but an incremental move. (Smith, 2006; cf. Kauffman, 1993). The same could be true of criticality, where incremental shifts in usage could change the criticality of the technology or service. The consequence-based approach suggested above is one method of thinking about criticality. This approach suggests that the criticality of a technology or service varies with the severity of the consequences of its failure.

Most new technologies and services that the market supports never make it past the 'non-critical' stage. Still fewer become relied upon in such a way that they can be categorized as Increasingly CI-Like (ICIL), where they become a vital part of the everyday work world for particular organizations. ICIL technologies and services often burst into the market with high expectations for resolving one of the problems created by 'reverse salients' or they may even drive markets by creating a need where one did not previously exist, such as email or the Blackberry discussed above.

Some technologies or services that are devolving out of the CI because they are either no longer necessary or they have been replaced by better technologies or services. Many organizations have developed systems to compensate for the types of vulnerabilities they create, but remain unprepared for the vulnerabilities of the newer systems that replace them, resulting in a decrease of reliability. For example, article-filing methods kept data safe under lock and key using varied storage locations. Stealing data, then, required physically entering a storage facility and carrying article documents out of it. The movement to vast electronic databases has increased efficiency by keeping data in a central location but they have raised the risk of theft because the electronic format makes theft a matter of merely moving electronic bits. The May 2006 hacker attack on a US government database, that took place while this article was being written, released classified and unclassified personal information on as many as 26.5 million US veterans. This may be the biggest single loss of data, but it is only one of many such attacks during the last decade – with this kind of information gathering capability, one may wonder if mere efficiency justifies keeping so much information in one place.

The consequence-based characterization of criticality (Table 1) expands the criticality spectrum to provide a rough framework for those who rely on new technologies to anticipate the vulnerabilities they create. Note that the number of technologies and services that support CI, and are therefore a part of the CI themselves, is quite small. The majority is not and will never move into criticality. This allows for a risk- or hazard-based approach to vulnerability management.

One method of hazard-based vulnerability management requires identification of all hazards created by the new technology, including comparisons for different levels of reliance. This entails understanding points of interactivity between the technology or service and the system it will support. Once the interaction points are well understood, the organization can better manage its vulnerabilities. Even 'mapping out' all potential points of interaction, or points where the new technology impacts the system, may be difficult in a large socio-technical system, but devising visual representations for areas that could be impacted by new technologies will aid this process.

Some understanding of the vulnerabilities and ways in which a new technology could fail will help managers decide how to respond to the hazard. Managers may choose to create partial redundancy and internal systems that will operate as backup systems. They may compartmentalize areas within the system to ensure that failure in specific technologies or services does not lead to cascading failures throughout the system. They may choose to spend resources to ensure greater reliability in the support technology or service (i.e. invest in reliability-enhancement for the critical support systems). They may do detailed background vetting to ensure that legal or operations challenges do not emerge or they may choose another technology or service altogether.

Table 1 categorizes criticality on the basis of the breadth of consequences of failure and the types of impacts it might have. Several areas that implicate criticality can be isolated from the table. Appendix I provides more detail about each of the criticality areas, while Appendix II lists the types of vulnerabilities to which systems are at risk.

Effects of Failure

Criticality increases where the failure of a technology or a service will result in the loss of human life or environmental degradation. It also increases where failure of one part of the system will result in large-scale failures for the entire system. Thus, the criticality of a technology of service varies with effects on people or the environment and the larger system the technology or service supports. The latter category can be offset by mitigation measures, but possible devastation to human life and/or the environment creates criticality in any system regardless of mitigation measures in place because it is difficult to anticipate all possible effects of failure in a complex system (LaPorte, 1978; Perrow, 1984).

Cost/benefit accounting that places a value on human life or the environment as a trade-off for provision of critical support systems requires values decisions best made by the people in a democratic society. Societies have chosen to make such collective risk-producing trade-offs in order to have the benefits of many large scale and high-hazard systems. However, most operators, though they may know that the public has made such decisions, still understand their systems to be critical and operate on the job accordingly (Egan, 2005).

A third criticality area pertaining to the effects of failure has to do with the effect of the technology or service on ancillary systems. The more failure will influence, for example, economic markets or the price of commodities, the greater the criticality level. Increasing criticality in the economic sector varies with the impact of failure; it is greater in widespread systems where failure will cause major price fluctuations or market failures.

Locality or Breadth of Consequences

Criticality varies with locality of impact or reach of a technology, service or event. While an event may have major local consequences its criticality is at least in part based on how much it impacts other jurisdictions for good or ill.

Most technologies and services in the marketplace are not critical as their impacts, for positive or negative, are largely local. The same is true with local emergencies such as traffic accidents, a local power disruption, the death of an important local figure, or record local rainfall or flooding; these may create emergencies for local citizens and managers and even have small spillover effects into other jurisdictions, but do not have widespread enough impacts to increase the criticality of a local event. This is because most technologies, services, and emergencies impact the local environment with very little 'rippling' or 'cascading' effects into other areas. Most local accidents have local causes and local impacts and rarely implicate LTSs, though while most local accidents are not the product of LTS failure, LTS failures will necessarily impact local communities. As the impact breadth of a technology expands, or as its locality decreases, it tends toward increasing criticality.

System Complexity

Increasing the complexity of a technological system alone will not increase its criticality, but LTSs tend toward greater complexity than local systems. This suggests that as technologies, services or events become less local, they also tend toward greater complexity. Further, an increasing amount of systemic 'rafting' tends to both increase complexity and decrease locality, increasing criticality.

Mitigating Factors and Trial-and-Error Learning

Decreasing locality also contributes to decreasing ability to mitigate vulnerabilities. Large, complex and unpredictable systems or events that impact multiple jurisdictions are difficult to map, and as such, are difficult to predict. In such systems, mitigation efforts may increase complexity, sometimes without decreasing vulnerabilities. Increasing criticality makes testing vulnerability mitigation efforts more difficult. In highly critical LTSs, the costs of failure make trial-and-error learning all but impossible (Rochlin, LaPorte and Roberts, 1987).

Regulation and Management

In the United States, markets alone will usually only support investment in safety up to the limits of liability established by the Hand Rule which states that: liability pertains where the cost of precaution (B) is less than the cost of an accident (L) times its probability (P) or where $B < PL$. (*United States v. Carroll Towing Co*. 159 F.2d 169 (2d Cir. 1947)). For efficiency's sake, then, corporations are only required to spend as much on precaution as the cost of failure discounted by its probability. This formula fails to account for the actual costs of catastrophic loss – a nuclear meltdown at the Indian Point nuclear power facility just thirty five miles from downtown Manhattan, for example.

Criticality often also varies with ease of regulation and enforcement. For technologies and services that have high levels of criticality, or are rapidly increasing in criticality, regulation is key to reducing vulnerability externalities. Regulators can require greater levels of precaution than the common law of torts would normally require. The regulatory burden, like the management burden, grows more intense as the system grows more complex. Regulators have the power to stop operations if they feel they are creating too much hazard, but in complex systems, regulators, like managers, may not always know where the hazards are.

Regulators attempting to regulate support systems, or technologies of LTSs, suffer from the problem of inadequate information. Organizations often have an incentive to hide or obscure information from regulators that could be damaging to their operations agenda, but in so doing, further increase the likelihood of systemic failure. Regulators examining the system for vulnerabilities will not have adequate information about potential problem areas – since they might be responsible for multiple parts of the LTS, the lack of adequate information will be compounded for each part of the system.

Criticality may not vary directly with ease of regulation or management, but they do tend to amplify it. Complex market dynamics often make regulation the only way to reduce criticality externalities that span the gap between required modernized Hand Rule precaution levels – no liability where the marginal cost of safety is equal to or greater than the marginal benefit of precaution – and the level of precaution that would be required if regulators had adequate information to take all effects, costs and externalities into account.

Legal issues may also increase criticality levels where the technology is new and bringing in large profits. The existence of reverse salients, especially in rapidly expanding markets or systems, makes it likely that multiple inventions to solve the same problem will arise at the same time, meaning that the technology or service that solves the most pressing problem is also likely to have the greatest amount of legal liability in patent, antitrust, and/or regulation. The legal truism that where there are large profits, lawyers are sure to follow, increases the likelihood of lawsuits and attempts to profit-share, which diverts resources from R&D, safety and security.

Institutional Stewardship: Reducing Criticality Externalities in Increasingly Critical Technologies

The drive to hyper-efficiency and the privatization of many CI capacities has reduced resilience in many systems, thus making the systems more vulnerable to increasing criticality. One method of responding to those types of vulnerabilities is to create systemic resilience, but markets tend not to produce this on their own because it is inefficient – corporate CEOs have argued that to spend more on precaution than necessary violates their fiduciary duty to their shareholders.

If we take the position that as new technological systems providing goods or services become more critical, they impose a cost on the public by increasing public vulnerability to their failure, then the public may seek to recoup these costs by forcing risk-producing organizations to internalize them, either by increasing their reliability or decreasing their criticality (LaPorte, 2006). By seeing network participants where once we only saw discrete products, we see that private firms have connected ('rafted') technologies together in such a way that increases their efficiency and profits. Then, it is not extraordinary to require that those who produce new vulnerabilities internalize their costs.

Central governments – which provide emergency services in the way of food and water delivery systems, security, and housing – provide social insurance against private systemic failures of all types. This means that taxpayers bear the burden of providing the CI safety net for private companies, even when they have made choices that decrease systemic reliability.

A method of encouraging private and public entities to better anticipate future vulnerability is to develop a model of risk management based on 'institutional stewardship'. This concept arises from, among other places, the legal notion that when one places another at risk, one is obligated to aid the other until they are safe. Institutional stewardship, as applied to risk management, would require that organizations perform at a higher standard of care than the Hand Rule or other liability rules (LaPorte, 2000).

Some have suggested that since markets tend to allow organizations to externalize risk, government regulation – either, *ex ante*, through regulations, rules and procedures or, *ex post*, through the tort system – should require higher levels of reliability in either increasingly critical technologies or the CI systems that are already in place (Egan, 2005; Auerswald et al., 2006; De Bruijne and Van Eeten, 2007). While stewardship-like reliability could begin to be accomplished through strict government regulation, this is not the preferred method, in part because organizations have far more access to information about their inner workings than outside regulators will have access to, making regulation ineffective.

More effective would be to establish liability rules based on the notion that organizations should internalize the costs of the risks they produce and that by internalizing them, they will make wiser choices about the technologies they use. Governments could then require that ICIL systems have built-in mechanisms that either increase their reliability, i.e. better testing or greater liability, that reduce their criticality, i.e. requiring redundancy or compartmentalization, and/or developing hazard control plans that will help users reduce their own criticality. We operate under a fiction when we treat new market entrants as though they are not a part of larger sociotechnical systems, providing benefits but also increasing vulnerabilities.

This article has attempted to provide a preliminary understanding of what elements of a technology are critical, so that managers can better predict vulnerabilities in the systems they manage. This will allow resources to be allocated to the highest hazard areas within given systems and therefore increase reliability. More work needs to be done to test whether and how variation within the areas this article labels 'critical' affect vulnerabilities and operations. It may provide a way in which the impact of increasingly or decreasingly critical technologies can be better understood. It may also allow federal or state legislation to require higher reliability and performance from organizations that reap huge benefits by making the public rely on its performance of services that have become 'critical'.

In doing this, the public bears the costs of corporate criticality externalities, something regulations could require the company to internalize under a 'stewardship' model of corporate responsibility. This model would require that some organizations that have reaped extraordinary financial gains by exposing the public to risk, have a legal obligation to go beyond 'adequate precaution' to ensure reliability for those it has placed at risk. It may also allow the public better insight into the foundation of its risk-based values decisions, or give judges better insight into corporate malfeasance.

Appendix 1: Categories of Increasing Criticality

Increases in any of the six categories below will cause an increase in the criticality of a particular technology. Increasing or decreasing amounts will impact the particular system, possibly in predictable manners. By examining especially newer technologies as they change, organizations, especially those that manage high-risk operations or have CI capacities, will be better able to predict their future vulnerabilities and take action to reduce them.

A. Intensity of Cost of Failure

Direct human and/or environmental impact
Emergency services will fail or be seriously damaged
Economic markets will fail or be seriously damaged
'Hard' or capital intensive technologies will be rendered useless or be seriously damaged

B. Breadth of Consequences

End-user device / will affect people directly
Ubiquitous usage = widespread cost
Ubiquitous usage and end-user device = widespread intense costs
Infrastructure 'backbone' for other critical systems/Part of 'rafted' critical system
'Cascading' systemic effects

C. 'Knowledge Burden' for Large Socio-Technical System Infrastructure

Complex technologies increase 'knowledge burden' (Demchak, 2001; 2003)
  Difficult to identify early stage failures heading toward crisis
  Training imperative to success
  Lack of management accountability
    Failure not known for multiple management generations
    High reliance on tacit knowledge (Schulman and Roe, 2007; Demchak, 2001)
    Performance dependent on leadership/management team or highly competent and dedicated workers (Boin and McConnell, 2007)[1]
    Institutional fragmentation and dispersed decision-making (de Brujine, 2006)
Unknown or Unanticipatable Consequences of Failure
  Warning Response systems imperative
  Threats to system are nearly infinite/Cannot prepare for all possible threats
  Need for Resilience

D. Lack of Mitigating/Limiting Factors

Design flaws increase vulnerability (Schulman and Roe, 2007)
Difficult to anticipate and recover from surprises
Little (or too much) systemic redundancy (Perrow, 1984; Sagan, 1993; 2004)
Trial and error learning is impossible because the cost of errors is too high
Interdependency between elements of the systems creates risk of criticality externalities
Increasing heterogeneity/differentiation with deceased relative redundancy

E. Complexity of Regulatory Systems

Legal concerns
  Patent
  Antitrust
Rules, regulations, and procedures are difficult to comprehend and follow (Egan and LaPorte, 2000; Egan, 2005)
Underfunded enforcement agencies
  Courts are split over rule interpretations (Egan and LaPorte, 2000; Egan, 2005)
Overreliance on quantitative or qualitative risk descriptions
  'Good numbers' problem
Turnover of political administrations changes rule interpretation and enforcement
Institutional and leadership fragmentation spreads decision-making making coordination difficult
Institutional and leadership integration decreases focus on important areas of concern (i.e. US Department of Homeland Security focus on terror at the expense of natural disaster planning)

F. Markets

'Reverse salients' rush a technological 'fix' to market (Hughes, 1987)
  CI reliance on 'beta' technologies
  Ubiquity of use – especially end-user devices
Drive for efficiency reduces socio-technical 'slack' in systems
  Reduction in system redundancies
  'Rafted' technological systems for greater economies of scale and scope
Inadequate spending on precaution
  Externalization of costs of increased risk to public
  Criticality externalities

Appendix 2: Types of Vulnerabilities

A. Adaptive Predation/Terrorism
    Cannot prepare for all possible threats (Roos, 2006)
    High community stress level/dread (Auerswald et al., 2006)
B. Natural Disaster
    Local Preparedness not possible/Safety requires large-scale transportation (Saathoff, 2006)
    High community stress level/dread
C. Accidents
    Technological Failure
    Systemic or Cascading Effects
    Human Operator Error
D. Legal Action
E. Regulatory Failure
F. Corporate Malfeasance
G. Government malfeasance[2]

Acknowledgements

An earlier version of this article was presented at the SEMA-ECMA Conference 'Future Challenges for Crisis Management in Europe', held in Stockholm, May 3–5, 2006.

The author would like to thank the Swedish Emergency Management Agency (SEMA) and the European Crisis Management Agency for travel support. He is grateful to Arjen Boin and Todd R. LaPorte for helpful comments and suggestions. The author holds a Ph.D. in Jurisprudence and Social Policy from the University of California, Berkeley and a J.D. from the Boalt Hall School of Law at the University of California, Berkeley.

Notes

1. Overreliance on the success and dedication of several team members places the organization at risk. What if there was a carpooling accident involving the dedicated workers working after hours to ensure the system's reliability? What if a terror cell targeted particularly competent and dedicated workers to attack a system?
2. The category for government malfeasance, like the category for corporate malfeasance, is emerging as citizens have begun to lose their naivety about the power of corporate lobbying and governmental complicity in corporate rule-breaking. Recent experiences in the United States and abroad have raised many questions about the power of government to institute an agenda that baldly allows corporations and governmental entities to externalize risk to the public so that corporations may garner large returns.

References

Auerswald, P., Branscomb, L., LaPorte, T.M. and Michel-Kerjan, E. (2006), 'Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge', in Auerswald, P., Branscomb, L., LaPorte, T.M. and Michel-Kerjan, E. (Eds), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, Cambridge, pp. 3–19.

Bea, R.G. (2002), 'Human and Organizational Factors in Reliability Assessment and Management of Offshore Structures', *Risk Analysis*, Volume 22, Number 1, pp. 29–45.

Bijker, W. (1987), 'The Social Construction of Bakelite: Toward a Theory of Invention', in Bijker, W.E., Hughes, T.P. and Pinch, T. (Eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, MIT Press, Cambridge, MA.

Bijker, W. and Law, J. (1992), *Shaping Technology, Building Society: Studies in Socio-Technical Change*, MIT press, Cambridge, MA.

Boin, R.A. and McConnell, A. (2007), 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience', *Journal of Contingencies*, Volume 15, Number 1.

Bourgeois, L.J. (1981), 'On the Measurement of Organizational Slack', *Academy of Management Review*, Volume 6, Number 1, pp. 29–39.

Chiles, J.R. (2002), *Inviting Disaster: Lessons from the Edge of Technology*, HarperBusiness, New York.

Coase, R.H. (1960), 'The Problem of Social Cost', *Journal of Law & Economics*, Volume 3, pp. 1–44.

Cooter, R. and Ulen, T. (1997), *Law and Economics*, 2nd edition, Addison-Wesley, Reading, MA.

de Bruijne, M. and van Eeten, M.J.G. (2007), 'Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment', *Journal of Contingencies and Crisis Management*, Volume 15, Number 1.

Demchak, C. (2001), 'Technology's Knowledge Burden, the RMA, and the IDF: Organizing the Hypertext Organization for Future 'Wars of Disruption'', *Journal of Strategic Studies*, Volume 24, Number 2, pp. 77–146.

Demchak, C. (2003), ''Atrium' – A Knowledge Model for Modern Security Forces in the Information and Terrorism Age', Lecture Notes in Computer Science Proceedings Intelligence and Security Informatics, (First annual NSF/

NIJ Symposium, ISI 2003), Springer-Verlag, Heidelberg, Volume 2665, pp. 223–231.

Demchak, C. (2006), 'Embracing Surprise in Critical Infrastructure: Lessons in Crisis Management from Military History', SEMA/ECMA Stockholm Conference discussion article, 4–5 May, Stockholm.

Dumas, L.J. (1996), *Lethal Arrogance: Human Fallibility and Dangerous Technologies*, St. Martin's Press, New York.

Egan, M.J. (2005), *The Stewardship Claim: Managing Legal and Organizational Environments at Los Alamos National Laboratory*, Dissertation, University of Berkeley.

Egan, M.J. and LaPorte, T.R. (2000), 'Two Stories of Regulatory Interpretation at Los Alamos National Laboratory', in LaPorte, T.R., Egan, M.J. and Stone, A. (Eds), *UCB-LANL Institutional Stewardship Studies, 1998-2000 Stewardship and the Design of 'Future Friendly' Technologies: Avoiding Operational Strain in Nuclear Materials Management at Scale: Final Report*, University of California, Berkeley, CA, pp. 35–77.

Grabowski, M.R. and Roberts, K.H. (1996), 'Human and Organizational Error in Large Scale Systems', *IEEE Transactions on Systems, Man, and Cybernetics*, Volume 26, Number 1, pp. 2–16.

Hughes, T.P. (1987), 'The Evolution of Large Technological Systems', in Bijker, W., Hughes, T.P. and Pinch, T. (Eds) *The Social Construction of Technological Systems: New Directions in the History and Sociology of Technology*, MIT Press, Cambridge, MA, pp. 1–82.

Joerges, B. (1988), 'Large Technical Systems: Concepts and Issues', in Mayntz, R. and Hughes, T.P. (Eds), *The Development of Large Technical Systems*, Westview Press, Boulder, pp. 9–36.

Joerges, B. (1996), 'Large Technical Systems and the Discourse of Complexity', in Ingelstam, L. (Ed.), *Complex Technical Systems*, Swedish Council for Planning and Coordination of Research, Affärs Litteratur, Stockholm, pp. 55–72.

Kauffman, S.A. (1993), *The Origins of Order: Self-organization and Selection in Evolution*, Oxford University Press, New York.

LaPorte, T.R. (1978), 'Nuclear Waste: Increasing Scale and Sociopolitical Impacts', *Science*, Volume 201, Number 4350, pp. 22–28.

LaPorte, T.R. (Ed.) (1991), *Social Responses to Large Technical Systems: Control or Anticipation*, Kluwer Academic Publishers, Dordrecht.

LaPorte, T.R. (1994), 'Large Technical Systems, Institutional Surprise and Challenges to Political Legitimacy', *Technology in Society*, Volume 16, Number 3, pp. 269–288.

LaPorte, T.R. (2000), 'Institutional Elements for Long-term Stewardship in a Nuclear Age: Views from a Stewardee', in LaPorte, T.R., Egan, M.J. and Stone, A. (Eds), *UCB-LANL Institutional Stewardship Studies, 1998–2000 Stewardship and the Design of 'Future Friendly' Technologies: Avoiding Operational Strain in Nuclear Materials Management at Scale: Final Report*, University of California, Berkeley, CA, pp. 1–32.

Mayntz, R. and Hughes, T. (Eds) (1988), *The Development of Large Technical Systems*, Westview Press, Boulder, CO.

Perrow, C. (1984), *Normal Accidents: Living with High Risk Technologies*, Basic Books, New York.

Perrow, C. (1994), 'The Limits of Safety: The Enhancement of a Theory of Accidents', *Journal of Contingencies and Crisis Management*, Volume 2, Number 4, pp. 212–220.

Prieto, R. (2003), 'Business Community Views', *Technology in Society*, Volume 25, Number 4, pp. 517–22.

Rijpma, J.A. (1997), 'Complexity, Tight–Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory', *Journal of Contingencies and Crisis Management*, Volume 5, Number 1, March, pp. 15–23.

Rochlin, G.I., LaPorte, T.R. and Roberts, K.H. (1987), 'The Self-Designing High-Reliability Organization', *Naval War College Review*, pp. 76–90.

Rochlin, G.I. (1996), 'Reliable Organizations: Present Research and Future Directions', *Journal of Contingencies and Crisis Management*, Volume 4, Number 2, pp. 55–60.

Rochlin, G.I. (1997), *Trapped in the Net: The Unanticipated Consequences of Computerization*, Princeton University Press, Princeton.

Roos, J. (2006), 'Practical Wisdom: A Philosophical and Practical Basis for Dealing Ethically with Unexpected Change', SEMA/ECMA Conference discussion article, 4–5 May, Stockholm.

Saathoff, G. (2006), 'Local Safety and Security Systems', SEMA/ECMA Conference discussion article, 4–5 May, Stockholm.

Sagan, S. (1993), *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, Princeton.

Sagan, S. (2004), 'The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security', *Risk Analysis*, Volume 24, Number 4, pp. 935–946.

Schwartz, P. (2003), *Inevitable Surprises: Thinking Ahead in a Time of Turbulence*, Gotham Books, New York.

Schulman, P.R. and Roe, E. (2006), 'Managing for Reliability in an Age of Terrorism', in Auerswald, P., Branscomb, L.M., La Porte, T.M. and Michel-Kerjan, E. (Eds), *Seeds of Disaster; Roots of Response*, Cambridge University Press, New York, pp. 121–134.

Schulman, P.R. and Roe, E. (2007), 'Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures', *Journal of Contingencies and Crisis Management*, Volume 15, Number 1.

Smith, D. (2006), 'Exploring Vulnerability Around Critical Infrastructures', SEMA/ECMA Conference discussion article, 4–5 May, Stockholm.

Tenner, E. (1997), *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*, Vintage Reprint, New York.

United States v. Carroll Towing Co. 159 F.2d 169, 173 (2d Cir. 1947).

Vicente, K. (2004), *The Human Factor: Revolutionizing the Way We Live with Technology*, Routledge, London.

Weick, K.E. (1989), 'Organizational Culture as a Source of High Reliability', *California Management Review*, Volume 24, Number 2, pp. 112–127.

White House (2003), 'National Strategy for the Physical Protection of Critical Infrastructures and Key Assets', White House, Washington, DC, Url: http://www.whitehouse.gov/pcipb/physical.html.