When Paul Stockton returned from the U.S. Department of Justice meeting in Washington, DC, and invited me to design the first graduate level curriculum for the first Homeland Security program at the Naval Postgraduate School, I had no idea it would take me on a decade-long journey. It was February 2002—a few short months after the 9/11 Terrorist attacks on U.S. soil—and I had just returned from a foray into corporate America. I didn’t know anything about homeland security, but then, hardly anyone did. Nonetheless, Paul and I developed a 12-course curriculum, got it approved by the Academic Council, and deployed the first-ever homeland security Master’s Degree program in America 9 short months later. The Center for Homeland Defense and Security (CHDS)––www.CHDS.us––was a huge success, and continues to be the premier program in the field, today.

From the beginning, protection of infrastructure was a centerpiece of homeland security. After all, if you don’t have food, water, energy, power, and communication, you don’t have a country. The extreme vulnerability to accidental, weather-related, and human-instigated attacks on food, water, energy, power, transportation, and public health systems was understood years before 9/11, but nothing was done about it. Americans were not consciously aware of the criticality of their infrastructure until the devastation of September 11, 2001. Even then, public concern played second fiddle to the Global War on Terrorism. But the criticality of infrastructure has since moved to center stage in the public eye as America’s roads and bridges decay, malware infects the Internet, transportation systems like air travel spreads disease and terrorism, and the very financial underpinnings of modern society comes increasingly under attack by hackers and unscrupulous speculators. Since 2001, the United States has experienced an historic series of system collapses ranging from the Middle Eastern wars to the financial debacle of 2008–2009. Some of the largest natural disasters in modern times have occurred. The Horizon Oil Spill in the Gulf of Mexico and Fukushima Dia-ichi tsunami/nuclear power disaster in Japan appear to be happening with greater frequency and consequence. Western civilization has taken on more debt than all of the previous empires combined, and most of the world’s population is no more safe than it was in 2001. Unprecedented catastrophes continue to preoccupy us even as war appears to be subsiding. And almost all of these big events involve infrastructure. The lingering question is, why?

Our milieu is punctuated by historic crashes, collapses, and disasters followed by periods of calm that suddenly and without warning break out into a series of crashes, collapses, and disasters once again. Why is this? The answer lies deep in modern life’s complexity. That is, modern society runs on complex systems that never existed prior to the last century. For example, the concept of a big business did not exist before the railroads in the 1870s, and the concept of a big system did not exist before the construction of the power grid, food and water supply chains, and global travel networks. In only 20 short years, people and communications infrastructure have become interdependent with just about all other systems as the Internet connects more people, places, and things into one big complex system. Modernity means connectivity and connectivity means complexity. As it turns out, complexity is the main source of risk and fragility in critical infrastructure and key resource (CIKR) systems. So, the short answer to the question of why collapses appear to be getting bigger and more frequent is simply complexity.

The level of complexity of systems we depend on is the root cause of extreme calamity—not some change in the climate, absence of forethought, or ineptitude. After all, buildings can be made to withstand hurricanes and earthquakes, and roads and bridges can be built to withstand ever
more severe damage. Rather than blame out failing systems on weather and terrorists, deeper analysis suggests that collapse is built into infrastructure, itself, because of its structural complexity. Risk is in the way systems are “wired together” and operated. Fragility—the opposite of resilience—is a symptom of complexity.

According to Bak’s theory of self-organization, modern society is responsible for the fragility of the very infrastructure it depends on for survival [1]. Modern designers are clever—they have optimized systems so completely that infrastructure systems have no wasteful surge capacity. Roads and bridges are built to be cost-efficient, not necessarily resilient. Water and power systems owned by both public and private corporations are built to return a profit, not necessarily to last for centuries. Power lines are much cheaper to build above ground than below, which means they become useless when a super storm such as Sandy strikes the Eastern seaboard. Public health institutions such as hospitals have no need for extra beds or 30-day power supplies, because such a lengthy outage could never happen, and the cost of resilience is simply too high. Supply chains are made efficient by centralizing distribution centers without concern for possible terrorist attacks that can take out an entire sector. Truly unthinkable events are shuffled off to insurance companies to worry about. What is the risk of an unthinkable incident of unbounded size, but near zero probability of occurring?

In the summer of 2002, when the original material for this book and its first edition was being collected, I did not understand the connection between critical infrastructure and complex systems. It seemed to me that critical infrastructure systems were largely mechanical and electrical machines. If the components worked, the entire system also worked. If something went wrong, only that something was affected. I had no concept of “system” or “complexity.” I thought the study of infrastructure was roughly equivalent to the study of processes and mechanical inputs and outputs. If students understood how these machines worked, and how they might be damaged, they could do something to protect them. Resilience is the sum of resilient components, and hardening targets against a variety of hazards removes risk. Thus, in 2003, I began writing the first edition of this book as a kind of “engineering lite” textbook.

The first edition covered the structure of water, power, energy, and Internet sectors—mostly from an engineering point-of-view. Because my students were nontechnically trained, I included some historical background, and lightly tossed in organizational things like how a sector is regulated or how regulation impacts infrastructure. From 2003 to 2006, my students struggled with the math and engineering concepts and gracially provided useful feedback. After more than two years of class testing, John Wiley & Sons agreed to publish the first edition. But by then I had the nagging feeling that I missed the mark. Why did complex systems like the power grid fail more often than they should? Why do epidemics like SARS explode onto the international scene and then vanish just as quickly? Why do terrorists attack patterns look a lot like accidents? These system questions cannot be answered by engineering or organizational psychology methods of analysis, because complex system behavior is “more than the behavior of its parts.” I came to realize that infrastructure is not designed and built, but instead, it is an emergent process that evolves. Most infrastructure sectors defined by the Department of Homeland Security are the product of hidden forces. As a result, most infrastructure has emerged as a complex system subject to unpredictable behavior when stressed.

I came to realize that the biggest threat to infrastructure systems was their topology—their architecture. Vulnerability to natural or human-made collapse is built into these systems. The secret to understanding them is buried within their very structure—largely defined by connections and interdependencies. For the most part, critical infrastructure is critical because of the way it is put together. And construction of most sectors is largely accidental or emergent. The commercial air transportation system is fragile because of important hubs (airports), the power grid is weakened by substations and transmission lines that handle more than their share of “connectivity,” and the monoculture Internet is prone to malware because it has so many connections that malicious code may travel from one side of the globe to the other with ease. It is structure—in the form of network connectivity—that makes critical infrastructure vulnerable to collapse.

I learned that Perrow’s Normal Accident Theory explained why small incidents sometimes spread and magnify in intensity until consequences are catastrophic [2]. The cause of this spread, according to Perrow, is hidden coupling—invisible links inherent in complex social and mechanical systems. Perrow’s breakthrough theory laid the blame for catastrophic failure on the system, itself. A spark may start a fire, but it is fuel, in the form of kindling, which spreads the flames and builds consequence. Per Bak—one of the founders of complexity theory—reinforced the idea that widespread collapse is inherent in the system itself. Bak went a step further than Perrow, however, and postulated the theory of self-organization. In Bak’s theory, complex systems become more fragile as they age, due to a number of factors. The most common factor simply being gradual restructuring as a system attempts to optimize performance. Bak called this self-organizing criticality (SOC).

SOC can be measured in almost all critical infrastructure systems using a mathematical quantity called the spectral radius. This may seem like an exotic quantity, but it is simply a measure of connectivity in a system. A power grid, supply chain, transportation system, the Internet, and most every infrastructure can be represented as a network. Nodes can be substations, depots, warehouses, Internet service
providers, bridges, etc, and links represent their connectivity. The pattern or “wiring diagram” of the network model is called the infrastructure’s topology. Topology has a fingerprint quantified as the spectral radius. Interestingly, spectral radius increases as the density of connections increase. It also increases as hubs form. Hubs are components that are overly connected through links to other components, such as a busy airport or central office of the telephone company.

Another metric found to be extremely useful is the fractal dimension of a system. This quantity simply measures fragility of a complex system by relating the likelihood of cascade failures (as described by Perrow in his Normal Accident Theory) to spectral radius. Interestingly, most infrastructure systems relate component vulnerability $\gamma$ and spectral radius $\rho$ to resilience $q$, as follows:

$$\log(q) = b - k\gamma\rho$$

$b$: constant

$k$: constant

This says system resilience is proportional to component vulnerability times system structure as determined by its spectral radius. That is, resilience goes down as vulnerability and spectral radius goes up (because of the minus sign). This is the fundamental equation of system resilience that applies to all infrastructure sectors that can be represented as a network of connected components. If we want to increase infrastructure resilience, we must decrease spectral radius, component vulnerability, or both.

This connectionist view of complex systems is a very handy tool for understanding critical infrastructure systems. It was an important concept mostly overlooked in the first edition. Thus, this edition places much more emphasis on networks—perhaps the simplest way to represent a connected system. By introducing formal network theory, infrastructures can be modeled and studied in the abstract. This makes it possible to understand and measure the resilience of infrastructure. Infrastructure resilience hinges on the structure of the system—not just its component’s weaknesses. Inherent weakness (vulnerability due to weak components and self-organized structure) can then be addressed on a system scale rather than a component or single-asset scale. Safe and secure policies can be designed to address the inherent risk of collapse, instead of patchwork guessing. By measuring spectral radius and fractal dimension of various infrastructure systems, we can provide policymakers with scientific tools upon which to make policy. Does changing a regulation reduce spectral radius? Does hardening of one asset make other assets more likely to fail?

This second edition first develops a general theory of risk, resilience, and redundancy, and then applies the general theory to individual sectors. After an introductory chapter, and three chapters on the theoretical foundations of risk and resiliency, the focus shifts to structural (architectural) properties of communications, Internet, Information Technology, SCADA, water, energy, power, public health, transportation, supply chains (shipping), and banking systems. Each chapter describes a sector and then applies network science and complexity metrics to an actual or hypothetical CIKR system. This should provide the reader with general tools that he or she can apply to other systems. It is a unified theory approach to the topic.

This edition stands on the shoulders of the first edition and students’ feedback. Both editions benefitted from classroom experience gained over a period of ten years.

tedglewis@redshift.com

TED G. LEWIS
Monterey, CA.

January 2014