2011

Critical Infrastructure as Complex Emergent Systems

Lewis, Ted G.; Center for Homeland Defense and Security; Mechanical Engineering Department

Critical Infrastructure as Complex Emergent Systems

Ted G. Lewis[1]
Thomas J. Mackin[2]
Rudy Darken[1]

[1]Center for Homeland Defense and Security
Naval Postgraduate School
Monterey, CA. 93943

[2]Mechanical Engineering Department
CalPoly University at San Luis Obispo
San Luis Obispo, CA. 93402

Abstract

The United States Department of Homeland Security (DHS) is charged with "build[ing] a safer, more secure, and more resilient America by enhancing protection of the Nation's Critical infrastructure and key resources (CI/KR) …" using an all-hazards approach. The effective implementation of this strategy hinges upon our understanding of catastrophes and their potential effect on the functioning of our infrastructure. Unfortunately, there has been no unifying theory of catastrophe to guide decision-making, preparedness, or response. We do not know, for example, why some catastrophes are "worse" than others, or if the rate of catastrophes is increasing or decreasing. Furthermore, DHS has adopted a risk-informed decision-making process, but has done so without defining key terms, such as "risk", or quantifying the primary elements of risk – definitions that are badly needed before setting a course of action and allocating resources. We present a framework, based upon network science and normal accident theory that can be used to guide policy decisions for homeland security. We show that exceedance probability, which is commonly used by the insurance industry to set hazard insurance premiums, provides a unifying policy framework for homeland security investments. Furthermore, since the exceedance probability for catastrophic consequences obeys a power law, we define resilience, explicitly, as the exponent of that power law. This allows a mathematical definition of resilience that resonates with our innate sense of resilience. That is, the more resilient a given system, the larger it's resiliency exponent. Such an approach also allows one to classify hazards as 'high' or 'low' risk, according to the resiliency exponent, and to guide investments towards prevention or response. This framework provides a more rigorous foundation for Federal investment decisions and a rational basis for policies to best protect the Nation's infrastructure.

A strategy without a theory

The United States Department of Homeland Security (DHS) is charged with the responsibility of "build[ing] a safer, more secure, and more resilient America by enhancing protection of the Nation's Critical infrastructure and key resources (CI/KR) to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."[i] The homeland security strategy is considered *all-hazards* because it embraces both natural and human-made catastrophes such as Hurricane Katrina, and the 9/11 Terrorist attacks.

The effective implementation of the all-hazards strategy hinges upon our understanding of catastrophes: earthquakes and wild fires in Southern California; hurricanes in Florida; terrorist attacks on infrastructure; and pandemic threats such as the H1N1 influenza. Unfortunately, there has been no unifying theory of catastrophe to guide decision-making, preparedness, or response. We do not know, for example, why some catastrophes are "worse" than others, or if the rate of catastrophes is increasing or decreasing. Moreover, we do not know what properties of a human or natural system contribute to fragility or resilience.

This lack of understanding has led to organizational confusion (what is the goal?), duplication of effort (different agencies doing the same thing), and poor utilization of limited resources (inadequate identification of the most at-risk assets, maximal return on investment, and resourcing of adequate response capability). DHS has adopted a risk-informed decision-making process, but has done so without defining key terms such as "risk" or quantifying the primary elements of risk: "threat", "vulnerability", "resilience", and "consequence" – terms used throughout DHS policy and strategy documents. Risk-informed decisions are difficult to make without operational definitions of risk and resiliency!

For example, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets[ii] recommends, "the first objective of this strategy is to identify and assure the protection of those assets, systems, and functions that we deem most 'critical' in terms of national-level public health and safety, governance, economic and national security, and public confidence. We must develop a comprehensive, prioritized assessment of facilities, systems, and functions of national-level criticality and monitor their preparedness across infrastructure sectors." This is a laudable objective, but since 2003 DHS has not been able to define 'critical', 'prioritization', or 'preparedness' – definitions that are badly needed before setting a course of action and allocating precious resources. The authors claim this malady will continue to persist until a suitable theory of catastrophe is developed and turned into practice.

We propose a theory of all-hazards catastrophe, the results of which can be used to guide policy decisions for homeland security. Our theory is based on network science[iii,iv,v,vi,vii] and normal accident theory.[viii] In a related approach, Ramo[ix] borrows on ideas taken from physical science to explain how political disasters happen. Ramo's ideas were previously explored and illustrated by Buchanan in a broader context.[x] Similarly, Taleb's highly popular book on randomness[xi] lays the foundation for some of the ideas expressed in the author's theory of catastrophe[xii] – specifically addressing the claim that many catastrophes are the result of random processes, rather than deterministic cause-and-effects. While Taleb focuses on "black swans" – highly unlikely, highly consequential, unpredictable events, we argue that black swans are statistically predictable and follow a power law exceedence probability distribution. Lewis[34] applied the theory of complex systems to critical infrastructure and showed the relationship between power laws, black swans, and normal accident theory to critical infrastructure systems. Thus, power laws appear to be fundamental to catastrophe theory, which raises the question of "why"? Our answer: catastrophic events, including black swans, are normal accidents that increase with increasing self-organization.

Normal accidents

The authors claim that natural and human-caused catastrophes are a byproduct of routine complex system behaviors, which, ironically, contain the seeds of their own destruction. Catastrophic consequences arise when these systems operate at or near their critical state where small, otherwise insignificant perturbations give rise to unexpectedly large consequences. Perrow called these unanticipated incidents *normal accidents*.[xiii] Normal accidents have three fundamental properties: (1) small failures can lead to large consequences, (2) nearly all large failures are triggered by a cascade of small failures, and (3) failure propagation is enabled by coupling of parts within the system. These attributes are associated with systems in a state of *Self-Organized Criticality* (SOC).[xiv]

Bak, Tang, and Weisenfeld (BTW)[14] showed, through a simple sand pile simulation, how small events lead to large consequences. Bak and associates simulated and recorded carefully the size, frequency, and timing of landslide catastrophes, but concluded they could not predict the timing *nor* the size of individual avalanches. The first property of normal accidents has been observed in a variety of phenomena. For example, Ramo's recent book on social and political upheaval describe the BTW property in simple terms as "small things can have huge impact"[9]. Ramo used the BTW experiment to explain the sudden and unexpected collapse of the Soviet Union. Taleb used this theory to anticipate the 2008 financial meltdown two years before it happened, writing, "The electricity blackout experienced in the northeastern United States during August 2003, with its consequential mayhem, is a perfect example of what could take place if one of the big banks went under today".[xv] The 2003 Blackout started by a relatively small incident in August 2003, and the 2008 financial catastrophe started with the default of a small bank in southern California.[xvi]

The second and third properties of normal accidents are more subtle: Perrow suggested that incidents, such as the Three Mile Island nuclear power disaster, do not end in disaster every time a small accident occurs. Instead, such accidents must propagate and magnify through a series of connections that link small accidents, or flaws, together. Links are the vectors of contagion. They transmit faults to neighboring systems, magnifying them as

the faults spread through the system. In reference to Three Mile Island, Perrow says, "The cause of the accident is to be found in the complexity of the system…. It is the interaction of the multiple failures that explains the accident." Though Perrow explains how catastrophes happen, he does not explain why some complex systems collapse, while others do not. The difference between insignificant and magnificent collapses remained unexplained by normal accident theory until Lewis[33]. Today we know that the 'invisible coupling" in normal accident theory is actually a build up of self-organized criticality, SOC. An easy way to understand SOC is to model complex systems such as the electrical power grid, telecommunications networks, water supply systems, and supply chain networks in general, as complex networks. Nodes are the assets or components of interest and links are the connections that transmit normal accidents through a complex system. A network is a set of nodes, links, and a mapping function that expresses the topology of the network in terms of a "wiring diagram." Figure 1 illustrates the use of networks to model the mid-Atlantic power grid. Nodes are power stations, substations, and interconnections. Links are the transmission power lines connecting them.

Figure 1. Graphical mapping of a portion of the mid-Atlantic power grid showing a vast collection of nodes and links.

Risk, resiliency, and networks

Resiliency – a property of complex systems that makes them more or less tolerant of faults – may be explained by network analysis. The Network's mapping function is key to understanding the relationship between the BTW and SOC properties of the grid, and SOC is key to understanding resiliency. Specifically, it turns out that the spread or 'cascade' to other nodes in the network from a single node or link failure is magnified by self-organized criticality (SOC). The higher SOC is, the larger the effect of a cascade failure. We show that this criticality is associated with the exponent of a power law fit to the exceedance probability curve for fault consequences associated with the network. We ran computer simulations of network failures by disabling a random node in the network shown in Figure 1. We propagated that failure to neighboring nodes using a 25% probability that any node linked directly to a failed node would, in turn, fail. Counting the number of disabled nodes for each such simulation and dividing by the total number of nodes in the network produced a measure of failure consequence. Consequence percentages were tabulated for each of 10,000 computer simulations and used to construct a fault histogram. We constructed the exceedance probability, Figure 2, from those data, as follows:

1. Rank the n consequences from greatest to least.
2. Calculate the exceedance probability, EP, using: $EP = \frac{rank}{(n+1)}$

Figure 2 shows the exceedance probability plot of the simulated consequences of an attack on the Mid-Atlantic power grid shown in Figure 1. These data are well described by a power-law fit. In this plot, the exceedance probability obeys a power law: $EP(x \geq c) \sim x^{-q}$, where x and c are a measure of consequences, and q is the exponent of a least-squares fit to the data. We call q the *resilience exponent*, or simply 'resilience'. The larger q is, the higher the resilience is, because the tail of the exceedence probability distribution decreases with increasing q. In the limit, a very high q implies a very low consequence.

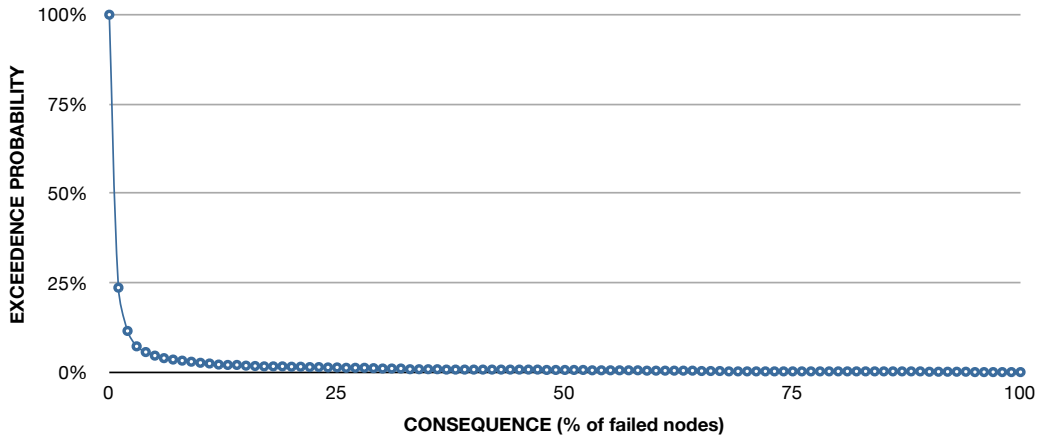

Figure 2. Exceedance probability plot for cascade consequences arising from simulations of random node failure of the Mid-Atlantic power grid. The horizontal x-axis is normalized to a percentage: 100 x #failed nodes/#nodes.

More precise functional models of the grid have been developed by Overbye[xvii] that model the physics of grid function and cascading failure. The exceedance probability curves of actual cascade failures[xviii], such as the 2003 Blackout[xix], obey a power law with exponent near 1.0. In fact, a great many natural and man-made hazards are found to obey power-laws when plotted as exceedance probabilities, EP. Table I lists a variety of typical natural and human-caused catastrophes along with the exponents, q, extracted from power-law fits of the exceedance probability for each. Power laws appear to be an integral part of catastrophe theory!

We define the probable maximum loss risk as $R = xEP(x)$.[xx] Then it is clear that R is bounded as x increases, for $q \geq 1$; and unbounded for $q < 1$, because $R \sim x^{(1-q)}$. Thus, the hazards in Table I can be divided into two categories: low-risk and high-risk, depending on the value of q. Using this definition for resilience allows one to clearly relate resilience to risk: resilient systems are low risk while 'non-resilient' systems are high risk. That is, catastrophes are either low- or high-risk depending on their resiliency exponent, q.

Though this approach allows one to classify the hazard as resilient or not, it does not explain why the resiliency exponent, q, differs for different kinds of hazards. We propose that the resiliency exponent, q, when derived from consequences associated with networked systems, is directly related to the topology of those networked systems. We illustrate this using additional simulations of various hazardous phenomena of interest to homeland security.

Self-organized criticality in networks

The authors claim that the resilience exponent, q, varies for different (network) systems because of the topologies of those systems. We tested this claim by simulating the propagation of a single-node failure throughout both random and scale-free networks over a range of average link density, shown in Figure 3. In our simulations, failure spreads to adjacent nodes, through links, with constant probability, p_f, (where, in this case $p_f = 25\%$). Consequence was calculated after each of 10,000 incidents, by recording the number of nodes affected by the propagated fault. The recorded consequences were placed into bins of increments of 1% each, tallied at the end of the simulation, and converted into an exceedence probability plot, EP(x). Finally, resilience, q, was obtained by fitting a power law to EP(x).

The experiment varied two properties of networks: the density of links, and the degree sequence distribution of each network. In Figure 3, link density was varied from a mean of 2 to 6 links per node for both a randomly linked network and a scale-free network. This plot shows that the resiliency exponent, q, decreased exponentially with increasing link density for both random and scale-free networks That is, networks with a higher density of links suffer greater loss due to link percolation.[xxi] Put more simply, the number of adjacent nodes that would fail is directly related to the number of links, n, times the probability of failure of a node, p_f, or np_f. Clearly, the more highly linked a network is, the greater the failure consequence. Link density (percolation) increases SOC, rendering the network less resilient.

Figure 3 overlays these results for both random and scale-free networks, showing a similar exponential decline in resiliency versus link density for both, suggesting that degree sequence distribution affects resilience. In addition, the plot shows that scale-free networks, regardless of link density, are less resilient than their random network counterparts. This is because of the highly connected hub, which transmits failures through more links. "Hubness" is another form of self-organized criticality that may explain why q differs for different systems.

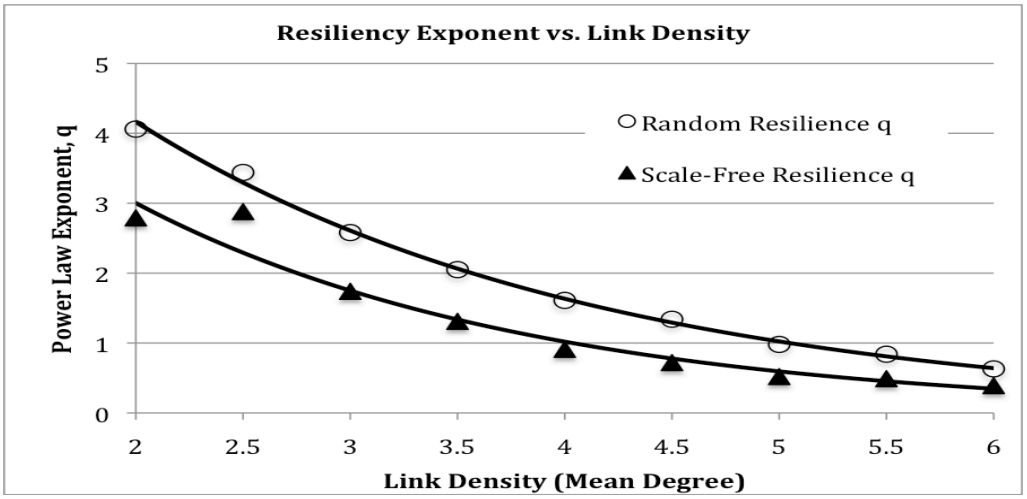

Figure 3. Resilience, defined as the exponent of the power law that fits the exceedance probability, versus the density of links in random and scale-free networks containing 200 nodes. Resilience declines exponentially as link density increases.

The authors have calculated the resilience of numerous infrastructure systems ranging from the Washington State Ferry system, Washington D.C. water network, Hetch-Hetchy water and power network, Mid-Atlantic power grid, the 9/11 Terrorist network, and major oil pipeline supply chains running from the Gulf of Mexico to New Jersey.[6] Resilience exponents can be computed for each infrastructure and compared against our low- and high-risk threshold. These simulations of real-world networks suggest that catastrophe is a combination of self-organized criticality, random incidents, and self-similar system architecture. This confirms the work by others. For example, the Amaral-Meyer network described by Buchanan[xxii] illustrates the impact of criticality in a

dynamically evolving connected system, whereby catastrophic failure is intrinsic to the system. Dynamic network systems can fail without *any* outside influence, simply by reconfiguring themselves into critical states.

These simulations also support Perrow's normal accident theory. SOC is the "invisible coupling" described by Perrow and further elucidated by Lewis[34]. Perrow's normal accident theory predicts that black swan catastrophes occur whenever a series of force-multiplying accidents unpredictably align themselves to bring down the entire system. Many of these systems obey a power law when plotting exceedence probability versus consequence.

The authors claim that financial system meltdowns, earthquakes, power grid blackouts, and epidemics are largely the result of random small failures in systems that are in a state of self-organized criticality, SOC. Alarmingly, many of our critical infrastructure sectors have reached self-organized criticality.[xxiii,xxiv] Typical signs of SOC include link density, large hubs, and betweeness (number of paths running through a node). Overly connected nodes are found in the public switched telecommunications network, high betweeness in near-capacity tie lines in the power grid, congestion on highways, lack of surge capacity in hospitals, and viruses worming their way through the Internet.

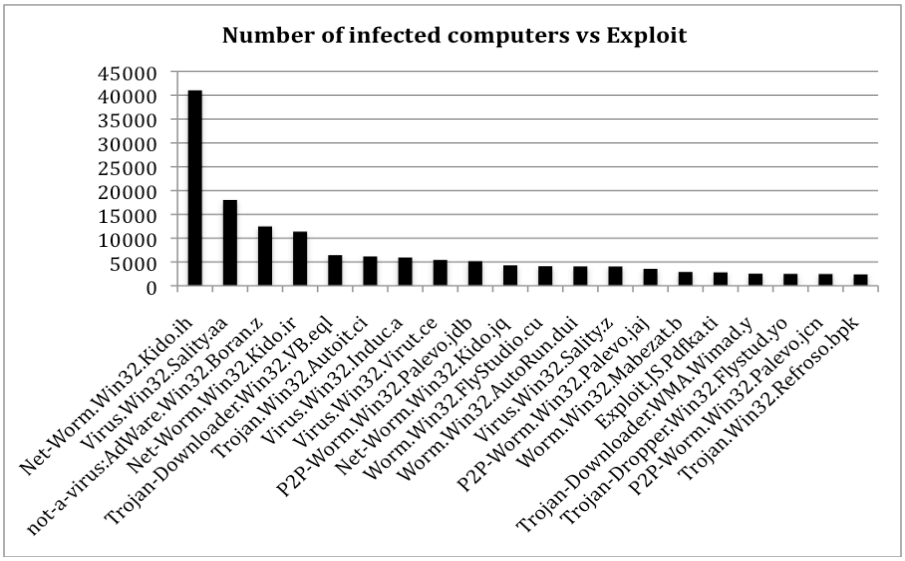

Figure 4. Number of computers infected by cyber exploits reported by http://www.securelist.com for one month during 2011.

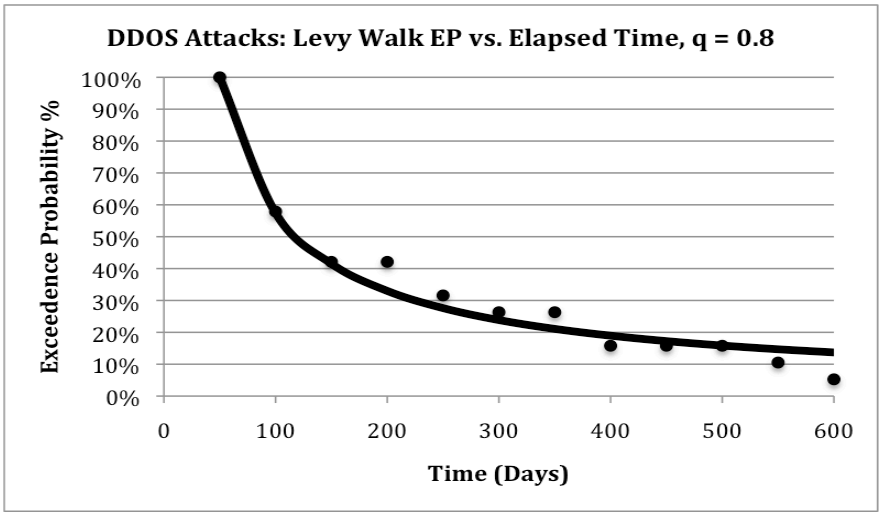

Figure 5. Levy Flight power law for DDOS exploits between August 1999 and August 2009. Time intervals between subsequent attacks follow an exceedence probability power law with exponent of negative 0.8. Data provided by Mark Schuchter, www.parabon.com/faqs/ddos-timeline.html

Application to cyber security

Does the forgoing theory of infrastructure as complex emergent systems apply to cyber security? Self-organized criticality, if it is present in networked computer systems such as the Internet, will manifest in the form of highly connected nodes (servers, autonomous systems), power law-shaped probability curves, or black swan incidents – rare, unpredictable, and high-consequence "accidents". The authors provide an initial, but perhaps incomplete, test of this hypothesis: the Internet and its corresponding infrastructure exhibits traits of a complex emergent system with self-organized criticality. It is a high-risk infrastructure, because of its exceedence probability "signature", and its high susceptibility to exploits.

For example, the Internet's web graph has been shown to be scale-free (containing major hubs) by many researchers over the past decade[35,36]. This form of self-organized criticality

contributes to its vulnerability. Additionally, the underlying telecommunication infrastructure in the US is organized around a small number of very large and critical carrier or telecom hotels[25]. These are critical to the continuity of operation of the communications backbone of the nation. The black swan event – often called the "Pearl Harbor of cyber" – has yet to happen, but its possibility cannot be ignored.

The data of Figure 4 shows the impact of cyber exploits for a one-month period during 2011. It follows the familiar power law characteristic of normal accidents and sand pile behavior. Figure 5 shows that the time interval between subsequent Distributed Denial of Attack (DDOS) exploits also obey a power law. Apparently, DDOS exploits are Levy Flights – another characteristic of sand pile behavior. These "signatures" are familiar markers of complex systems.

While the data cited here is not conclusive, it does provide a preliminary verification of the theory proposed here: that infrastructures ranging from power grids to the Internet are subject to sand pile effects. Surprising adherence to power laws, and network properties found in many self-organized systems are also present in cyber systems. The proposed theory is slowly being validated by current cyber events, but more data is needed to complete the claim.

A strategy backed up by a theory

A scientifically sound theory of catastrophe is now available for policy-makers to enable risk-informed decision-making by the department of homeland security. Rather than spending billions of dollars on securing already resilient systems, the nation's treasury should be used to increase the resiliency of high-risk sectors such as telecommunications, electric power transmission and distribution, the financial sector, and fragile public health networks. One can relate the growth of infrastructure to the growth of sand piles. When small, the infrastructure systems grow somewhat stably. However, the system will eventually reach a critical state where the addition of new demands gives rise to unpredictable consequences.

Several mechanisms can be used to reverse self-organized criticality. Of course, the problem can be solved at the engineering level: addition of surge capacity, operating systems below maximum capacity, and restructuring networks to back them away from SOC. That is, operating these systems inefficiently will keep them from becoming critical! Each of these solutions has corresponding costs, however, and is the subject of another paper. A more global solution is to change regulatory policy, affecting infrastructures across the entire nation. Re-design of regulation is a better approach because it spreads the economic burden across an entire industry.

For example, the electric power grid has evolved into a state of self-organized criticality by incremental patching of its transmission network. Regulatory policies that motivate utilities to build more transmission capacity or promote local distributed generation (reducing the need for transmission capacity) would back the sector away from criticality. A similar criticality exists in the communications sector due to the rise of telecommunications hotels.[xxv] The existence of telecom hotel hubs is a direct consequence of the 1996 Telecommunications Act that advocates peering among competitors and promotes co-location of switching equipment. This regulation needs to be changed, immediately, before a normal accident results in a national telecommunications blackout.

Similar self-organized criticalities exist in other infrastructure sectors. Financial systems tend to self-organize into criticality; public health/hospital systems have inadequate surge capacity; the World Wide Web/Internet is notoriously near its critical point with respect to denial of service attacks, worms, and cyber threats. Complex systems – whether they are financial, political, physical, human or naturally occurring – can be modeled as a network, where nodes are components and connections and relationships are links. Normal systems are rational, well designed, and perform their functions perfectly over long periods of time and under a variety of stresses. Collapse of such systems comes as a shock, not because of attacks or unnatural events, but because of connectivity and randomly occurring small accidents that, occasionally, propagate and magnify throughout the system. We should not be surprised by normal accidents. Instead we should reduce

their consequences by restructuring critical infrastructure networks to raise their resiliency exponent.

Table I.

Exceedance Probability Exponents for Low-Risk and High-Risk Incidents[1]. [xxvi, xxvii, xxviii, xxix, xxx, xxxi, xxxii]

Asset/Sector	**Consequence**	**Exponent**
		Low Risk
S&P500 (1974-1999)	$Volatility	3.1-2.7
Large Fires in Cities	$Loss	2.1
Port Consequences (MSRAM data)	$Loss	1.7
Airline Accidents	Deaths	1.6
Tornadoes	Deaths	1.4
Terrorism	Deaths	1.4
Floods	Deaths	1.35
Forest Fires in China	Land Area	1.25
East/West Power Grid	Megawatts	1
Earthquakes	Energy, Area	1
Asteroids	Energy	1
Pacific Hurricanes	Energy	1
		High Risk
Hurricanes	$Loss	0.98
Public Switched Telephone	Customer-Minutes	0.91
Forest Fires	Land Area	0.66
Hurricanes	Deaths	0.58
Earthquakes	$Loss	0.41
Earthquakes	Deaths	0.41
Wars	Deaths	0.41

Whooping Cough	Deaths	0.26
Measles	Deaths	0.26
Small Fires in Cities	$Loss	0.07

References

[i] The National Infrastructure Protection Plan (NIPP),
[ii] The National Strategy 2003
[iii] Réka Albert, Hawoong Jeong, Albert-László Barabási, The Internet's Achilles' Heel: Error and attack tolerance of complex networks, *Nature*, 406: pp. 200, (2000), http://www.neci.nec.com/~giles/barabasi/nature00.p
[iv] Barabasi, A. and Bonabeau, E. Scale-Free Networks. *Scientific American* 288, 60-69. 2003.
[v] Lewis, T. G., "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation," John Wiley & Sons, Hoboken, NJ. 2006, 500p.
[vi] Lewis, T. G., "Network Science: Theory and Applications," John Wiley & Sons, Hoboken, NJ. 2009, 510p
[vii] Strogatz, S. H., "Exploring Networks," NATURE, v. 410, 8 March 2001, www.nature.com.
[viii] Charles Perrow, *Normal Accidents*, Princeton University Press, Princeton, New Jersey, (1999): 450pp.
[ix] Joshua Cooper Ramo, *The Age of the Unthinkable*, Little, Brown & Company, New York, NY. (2009): 280pp.
[x] Mark Buchanan, *Ubiquity: Why Catastrophes Happen*, Three Rivers Press, New York, NY. (2000, 2001): 274pp.
[xi] Nassim Nicholas Taleb, Fooled by Randomness, Random House, New York, NY, (2005): 316pp.
[xii] Lewis, Ted G. "Cause-and-Effect or Fooled by Randomness?" *Homeland Security Affairs* VI, no. 1 (January 2010) http://www.hsaj.org/?article=6.1.6
[xiii] Charles Perrow, *Normal Accidents*, Princeton University Press, Princeton, New Jersey, (1999): 450pp
[xiv] Per Bak, Chao Tang, and Kurt Weisenfeld, "Self-Organized Criticality: An Explanation of 1/f Noise", *Phy. Rev. Ltrs.* 59 (1987): pp. 381-384.
[xv] Nassim Nicholas Taleb, *The Black Swan*, Random House, New York, NY, (2007): pp. 226.
[xvi] David Faber, And then The Roof caved In, John Wiley & Sons, Hoboken, NJ. (2009): 190pp.
[xvii] T. J. Overbye and J. D. Weber, "Visualizing the electric grid," IEEE Spectrum, Vol. 38, No. 2, Feb. 2001.
[xviii] Massoud Amin, "Energy Infrstructure Defense Systems," Proceedings of the IEEE, Vol. 93, issue 5, May 2005.

[xix] Massoud Amin and Phillip F. Schewe, "Preventing Blackouts", Scientific American, May 2007.
[xx] Patricia Grossi, and Howard Kunreuther, *Catastrophe Modeling: A New Approach to Managing Risk*, Springer, New York, NY. (2005): 245pp
[xxi] Duncan S. Callaway, M. E. J. Newman, Steven H. Strogatz, and Duncan J. Watts, Network Robustness and Fragility: Percolation on Random Graphs, *Phys. Rev. Lett.*, 85:25, 5468–5471.
[xxii] Mark Buchanan, *Ubiquity: Why Catastrophes Happen*, Three Rivers Press, New York, NY. (2000, 2001): 274pp
[xxiii] I. Dobson, B.A. Carreras, V.E. Lynch, D.E. Newman, "Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization", *Chaos*, vol. 17, 026103 (June 2007).
[xxiv] Malamud, B. D., and Turcotte, D. L., The Applicability of Power-law Frequency Statistics to Floods, *Journal of Hydrology*, 322 (2006), pp. 168-180.
[xxv] *NSTAC Task Force on Concentration of Assets: Telecom Hotels*, National Security Telecommunications Advisory Committee, (February 12, 2003).
[xxvi] Robin Hanson, "Catastrophe, Social Collapse, and Human Extinction", *Global Catastrophic Risks*, ed. Martin Rees, Nick Bostrom, and Milan Cirkovic, Oxford University Press, (July 17, 2008): pp. 363-377.
[xxvii] Kuhn, Richard, "Sources of Failure in the Public Switched Telephone
[xxviii] Yanhui Liu, Parameswaran Gopikrishnan, Pierre Cizeau, Martin Meyer, Chung-Kang Peng, and H. Eugene Stanley, "Statistical properties of the volatility of price fluctuations", *Phys. Rev. E.*, 60, 2 (August 1999): pp. 1390-1400.
[xxix] Weiguo Song, Fan Weicheng, Wang Binghong, Zhou Jianjun, "Self-organized criticality of forest fire in China", *Ecological Modelling* 145, (2001): pp.61 – 68.
[xxx] W.G. Song, H.P. Zhang, T. Chen, W.C. Fan, "Power-law distribution of city fires", *Fire Safety Journal* 38 (2003): pp.453–465.
[xxxi] Jie-Jun Tseng, Ming-Jer Lee, and Sai-Ping Li, "Heavy-tailed distributions in fatal traffic accidents: role of human activities", http://www.arxiv.org/abs/0901.3183v1.
[xxxii] Lewis, Ted G. "Cause-and-Effect or Fooled by Randomness?" *Homeland Security Affairs* VI, no. 1 (January 2010) http://www.hsaj.org/?article=6.1.6
[34] Lewis, Ted G., *Bak's Sand Pile*, AgilePress 2011, 380pp.
[35] Adamic L. A., B. A. Huberman, Power-law distribution of the World Wide Web, *Science*, 287:2115, (2000).
[36] A. Broder, S. R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, and J. Wiener. Graph structure in the web. *Computer Networks*, 33(1:6):309-320, (2000).