PUBLICATION

Security, Resilience, and Communication
in Unpredictable Environments
Such as Terrorism, Natural Disasters,
and Complex Technology

P.H. Longstaff

November 2005

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

P.H. Longstaff was a communications lawyer for twenty years before joining the faculty of Syracuse University to concentrate on interdisciplinary public policy research for the communications sector. Longstaff received an M.P.A. from Harvard University in 1994 and has been a Research Associate at the Program on Information Resources Policy since 1995.

ISBN 1-879716-95-X P-05-3

Contents

Page

Executive Summary

Anyone who must manage the security of a large organization or implement security policies for a government will tell you that the number of “surprises” he or she must deal with is growing all the time. This is because many of the systems (both human and technical) that we deal with in the twenty-first century have grown more interconnected and complex, making them less predictable. This paper explores the many ways in which people deal with this uncertainty. It focuses on the concepts of *resistance* (keeping dangerous surprises away) and *resilience* (the ability to bounce back from surprises).

In many systems with high uncertainty, resistance against all possible surprises is futile and a resilience strategy will be appropriate. But there is a tradeoff. Resilience will often have a price in the form of lower efficiency. The paper explores successful resilience strategies for many systems as well as what makes a resilience strategy fail. One of the major assets of any resilient system is a trusted source of information. One of the major internal threats to resilience is the Blame Game.

The paper applies these ideas to two specific problems/opportunities: the role of the communications industries in times of uncertainty and surprise, and the application of resilience concepts to modern warfare and intelligence gathering. The final section sets out some first steps for managing security in unpredictable environments, including:

- Realign expectations about certainty
- Rethink the Blame Game
- Never overdrive the headlights
- Consider trading some efficiency for some resilience
- Recognize that sometimes security is not designed—it is discovered
- Develop more trusted sources of information.

Chapter One

Introduction

To me our knowledge of the way things work, in society or in nature, comes trailing clouds of vagueness. Vast ills have followed a belief in certainty, whether historic inevitability, grand diplomatic designs, or extreme views on economic policy. When developing policy with wide effects for an individual or society, caution is needed because we cannot predict the consequences.

Kenneth Arrow[1]

The world has always been unpredictable, yet living things manage to survive when wildfires and floods destroy habitat, volcanoes erupt, and freak storms sink invincible naval fleets. Humans have dealt with unpredictability by attributing it to the whim of the god(s), or, since the Renaissance in Western cultures, to forces of nature we do not yet understand well enough to predict. More recently, people in many disciplines and many cultures have begun to believe that some things are too complex to predict. If those unpredictable things might become dangers, individuals and groups must find strategies to deal with them even if they cannot forecast them. In both biological and human systems such strategies are designed for *resistance* (keeping the danger away) or *resilience* (bouncing back if the bad thing happens). This paper examines both, placing special emphasis on resilience because it is so often ignored in debates about important topics such as business and policy strategy and, most critically, homeland security.

Attempts to cope with unpredictable dangers are often called *risk management*. In modern times risk management usually involves sophisticated statistical analysis that yields the odds that a certain thing might happen to any individual or group. This calculation becomes more difficult when the number of variables that might influence the analysis grows. Since anything involving human behavior has many variables, very sophisticated tools for building possible scenarios[2] (including several varieties of game theory[3]) have been developed. Many of these tools have been incorporated into computer simulations that allow people to "try out" the effect of changing the variables that act on the system.

---

[1] Kenneth J. Arrow, "I Know a Hawk From a Handsaw," in M. Szenberg, ed., *Eminent Economists: Their Life and Philosophies* (Cambridge, U.K.: Cambridge University Press, 1992), 42–50.

[2] Herman Kahn was the inventor of scenario planning in the 1960s. See, e.g., Herman Kahn, *The Year 2000: A Framework for Speculation on the Next Thirty Three Years* (New York: MacMillan, 1967); and *The Next Two Hundred Years: A Scenario for America and the World* (New York: William Morrow, 1976). See also Peter Schwartz, *The Art of the Long View* (New York: Currency, 1996).

[3] For an overview suitable to nonspecialists, see, e.g., Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: Wiley, 1996), Chapter 14, 231–246.

All of these risk management tools attempt to predict unpredictable occurrences well enough to judge if the risk is worth the reward or if the risk can be mitigated through a resistance or resilience strategy. For example, insurance companies use very sophisticated analysis of mortality statistics to set life insurance rates. They cannot prevent their customers from dying, but they can develop resilience for the company by having many customers who are statistically unlikely to die at the same time or to die young. For the insured, insurance is clearly a resilience strategy: they are trying to make certain that their families can bounce back financially despite an unexpected death. Insurance works because of the Law of Large Numbers: even if individual events happen in a random way, when enough of these events are put together in a reasonably stable environment one can make predictions that have a reasonable chance of being accurate. So, for example, one cannot predict whether an individual coin toss will turn up heads or tails, but many coin tosses will follow a fixed probability ratio (an even chance).[4]

In some systems it is enough to predict where a particular variable falls within certain limits in order to make decisions.[5] But what about systems that are not large enough or stable enough for the Law of Large Numbers to operate, or where the dangerous event is *really* unpredictable because we do not know what it is or when it will strike – such as a terrorist attack?

1.1 Complex Adaptive Systems: the New Game

Complex systems are hard to make secure or dependable precisely because they are unpredictable. This idea that some systems are so complex that they are not predictable is fairly new and still feels uncomfortable, particularly in Western cultures. Economist Paul Ormerod is among those who believe it is time to admit there are things we cannot predict and to find other ways to deal with those systems.

> Governments of all ideological persuasions spend a great deal of time worrying about how the economy will develop in the short term, over the next couple of years…. But our representatives do not merely contemplate the short-term future, they seek to influence it. Elaborate forecasts are prepared, not just by governments but by academic institutions and commercial companies. Advice is freely offered as to how the prospects for the economy can be improved, by an alteration to income tax rates here, or a touch of public expenditure there. But the control which governments believe they have—in their ability to make reasonably

[4] For an excellent nonspecialist explanation of the Law of Large Numbers, see Philip Ball, *Critical Mass: How One Thing Leads to Another* (New York: Farrar, Straus and Giroux, 2004), 48–79.

[5] "That is, the same decision is appropriate for values of X between X(1) and X(2), so that all we need accurately to do is to place X between those limits." Richard Levins, John Rock Professor of Population Sciences, Department of Population and International Health, Harvard School of Public Health, personal communication with the author, March 2005.

> accurate forecasts and to understand the consequences of policy changes designed to alter their outcome—is largely illusory.[6]

Many disciplines are now developing ways to deal with complex systems, but they are doing so slowly and not without controversy.[7] Complexity theories fell into some disrepute when some management "gurus" tried to map theories about complex adaptive systems onto business management and market trading strategies, with less than successful results for investors. It now seems likely that the level of similarity in adaptation strategies between, say, populations of sharks and populations of stock-market day-traders is less than some have "seen." But the broad outlines of all complex systems appear tantalizingly analogous and can provide some clues to new approaches, even if we cannot predict in advance that these approaches will work just as they do in other systems. For example, several disciplines have noted that the level of complexity in a system is closely tied to the amount of embedded communication networking. There also appears to be a relationship between the level of complexity and the control architecture available to the system: a system becomes more complex if it involves more networking but become only as complex as its control architecture can handle. This obviously has enormous implications for designing regulatory systems for complex technical and human systems.[8] Readers unfamiliar with the ideas and terms used in studying complex systems will find a brief introduction in **Appendix A**. **Appendix B** lists suggestions for further reading.

Ideas about unpredictability may have their greatest utility in their ability to show us new ways to look at problems, new ways to plan for the deployment of resources in complex systems, and new expectations about how those systems work. But studying these systems often demands very different approaches from studying simpler systems. Their nonlinearity and long lag times make it difficult to track from actions to consequences. This means that case studies and the ability to work backward from undesirable outcomes and "learn" about the system become some of the most important ways to understand and manage these systems. Doing so requires accurate information about what the system actually does and the distribution of this information to everyone who must adapt to any surprises in the system. Throughout this study we will encounter the importance of trusted sources of information for successful individual and group actions in times of uncertainty.

---

[6] Paul Ormerod, *Butterfly Economics: A New General Theory of Social and Economic Behavior* (New York: Basic Books, 1998), 76.

[7] For two very readable treatments of the changes in how we see predictability and science, see Philip Ball, *Critical Mass: How One Thing Leads to Another* (New York: Farrar, Straus and Giroux, 2004) and F. David Peat, *From Certainty to Uncertainty: The Story of Science and the Ideas of the Twentieth Century* (Washington, D.C.: John Henry Press, 2002).

[8] See, e.g., Johannes M. Bauer, "Harnessing the Swarm: Communications Policy in an Era of Ubiquitous Networks and Disruptive Technologies," *Communications & Strategies* **54** (2nd quarter 2004), 19–43.

Most of us rely on some form of computing for virtually all of our communications, not only for email and Internet access but also because computers run critical elements of mass media such as newspapers, broadcasting, and cable companies. As our computer systems become more complex they become more "fragile" and prone to surprises. Some engineers believe the answer to this problem is to gain a better understanding of all the possible conditions under which the system will operate and then carefully craft the system to operate under all those conditions. They see surprises as flaws or "bugs" in the systems that could have been avoided with better planning. But some computer scientists have begun to see these bugs as the product of "subtle interactions between many components or layers in the system."[9] Some circles accept the concept that complex computer systems are inherently unpredictable and that the best engineering designs will allow them to "fail gracefully" and without too much damage.

Unpredictable human problems are almost never solved by simply throwing technology at them. Most technology succeeds in a system where 1 plus 1 always equals 2. It is often less successful in systems where the control variables or the emergent properties of the system are unpredictable, particularly if human beings are part of the process. Technology can be part of a resistance or resilience strategy for unpredictable dangers, but it is almost never the whole answer. In some cases technology would be counterproductive if it made a system more complex and less reliable.

Just because some systems are complex does not mean they are unmanageable or ungovernable. Managing them just takes different forms and rests on different assumptions. Where we had come to expect certainty, we now (sometimes reluctantly) must accept the necessity of dealing with uncertainty. This is not a new idea. One of the best known statements of this concept came from military theorist Carl von Clausewitz, who described the "fog of war."[10] The U.S. Marines (an organization with some experience in competition and running complex operations) also recognized the need to acknowledge and manage unpredictability:

> All actions in war take place in an atmosphere of uncertainty—the *fog of war*. Uncertainty pervades battle in the form of unknowns about the enemy, about the environment and even about the friendly situation. While we try to reduce these unknowns by gathering information, we must realize that we cannot eliminate them. The very nature of war will be based on incomplete, inaccurate, or even contradictory information.
>
> We must learn to fight in an environment of uncertainty, which we do by developing simple, flexible plans; planning for contingencies; developing

[9] Steven D. Gribble, "Robustness in Complex Systems," in *Proceedings of the 8th Workshop on Hot Topics in Operating Systems* (New York: IEEE, May 2001), 22.

[10] Carl von Clausewitz, *On War*, M. Howard and P. Paret, trans. and ed. (Princeton, N.J.: Princeton University Press, 1984).

> standing operating procedures; and fostering initiative among subordinates.[11]

Readers will notice several concepts from this Marine Corps doctrine that have become well accepted in both modern military and business strategies. But the underlying message of accepting uncertainty and learning to manage it is not always honored in business or in government. It is easier, especially in times when things are going well, to claim that a system is operating just the way we planned it to operate. Still, most experienced managers recognize that they operate in the fog of business or the fog of politics created by increasingly complex situations. It is not known if the authors of *FMFM-1* knew much about ecological systems, but their analysis could have come directly out of an ecology textbook that explains how populations of plants and animals survive in unpredictable environments.

Many people in business and government circles have begun to talk about managing systems they cannot predict. Some have gone so far as to declare that people who pretend to control complex systems actually make those systems more insecure.[12] Increasing evidence indicates that an adaptive management strategy that acknowledges complexity and uncertainty is more effective than a rigid command and control strategy, particularly in organizations that must deal with unpredictable events such as natural disasters and terrorism.[13] In 1977 Burton Klein was one of the first economists to note that firms facing high uncertainty (such as new technology) must be managed differently than traditional firms.

> Highly adaptive organizations are required if the best use is to be made of a technology…. However, the more structured and predictable firms become, the less adaptive they are likely to be. Generally speaking, highly structured organizations are inefficient when dealing with changes in their environments.[14]

Similarly, Anthony Oettinger suggests that the best way to manage in complex and unpredictable environments is to adapt by continually rebalancing the tradeoffs being made and give up the

---

[11] John Schmitt, *FMFM-1: Warfighting*, Foreword by Gen. A. M. Gray, Commandant, U.S. Marine Corps (Washington, D.C.: Department of the Navy, 1989), [On-line]. URL: http://www.clausewitz.com/CWZHOME/Warfit1.htm (Accessed on Sept. 27, 2005.)

[12] For example, Lee Clark of Rutgers University calls planning documents that try to cover any possible adverse event in complex systems "fantasy documents" and asserts that they give everyone a false sense that things are under control and prevent people from preparing for real dangers. See Lee Clark, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago and London: University of Chicago Press, 1999).

[13] See, e.g., Alexander Kouzmin and Alan Jarman, "Crisis Decision Making: Towards a Contingent Decisions Path Perspective," in Uriel Rosenthal, Michael T. Charles, and Paul T. Hart, eds., *Coping With Crisis: The Management of Disasters, Riots and Terrorism* (Springfield, Ill.: Charles C. Thomas Publishers, 1989), 397–435.

[14] Burton Klein, *Dynamic Economics* (Cambridge, Mass.: Harvard University Press, 1977), 56–57.

idea that you can predict everything: "[E]ven though you prepare for surprise, you must be prepared to be surprised, nonetheless. The aim is to be less surprised than the other guy!"[15]

If we must make predictions about systems that involve uncertainty, it is worthwhile to study people who do it better than most. Weather forecasters must deal with a truly complex system and yet their short-term predictions are right more than 70 percent of the time. Some evidence suggests that this is because they have years of hands-on experience, guidance from computer models, and ample feedback about their predictions, and, perhaps most important, because they function in organizations that reward them for candor.[16]

This paper will examine the strategies developed in a variety of unpredictable environments, that is, systems subject to "surprise." This discussion requires the adoption of very specific meanings for words that are used in many ways and by many disciplines. Some of these terms and the meanings assigned to them in this paper are listed below. Each of these terms is further defined and discussed in **Chapter Two**. Specialists who are familiar with the terms may want to turn directly to **Chapter Three**.

- Uncertainty: Where the action of a system is not predictable or is predictable only within broad ranges.
- Risk: An unacceptable outcome in a system and the calculation of its likelihood.
- Security: Not a state of being but a probability calculation of the likelihood of a dangerous surprise.
- Danger: An unacceptable condition that reduces security. This can be an immediate physical hazard or a longer term deprivation of resources. Dangers can be known or unknown. They can be actual, threatened, or perceived.
- Black Swan: A particular type of surprise that is theoretically possible but statistically so unlikely that it is not predicted to happen.
- Crisis: What happens when a surprise reveals an unambiguous failure of the rules, norms, behavior, or infrastructure used to handle the surprise.
- Efficiency: A characteristic or goal of a strategy that seeks to obtain the maximum output for the minimum input.
- Resilience: The strategy that develops the ability of a system to bounce back from a surprise.

---

[15] Anthony G. Oettinger, *Whence and Whither Intelligence, Command and Control? The Certainty of Uncertainty*, P-90-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=339 (Accessed on November 7, 2005.)

[16] Max Henrion and Baruch Fischoff, "Assessing Uncertainty in Physical Constants," *American Journal of Physics* **54**, 9 (1986), 791–798.

- Resistance: A strategy designed to keep a danger away or stop it from developing. Figuratively, building a wall around the things you want to protect. This includes “detection and response.”
- Robustness: A characteristic of a resistance or resilience strategy to perform in the face of a wide variety of challenges.
- Surprise: A discrepancy between what is expected and what is perceived. These can be unexpected discrete events, discontinuities in long-term trends or the emergence of new information.

1.2 Caveat

This paper represents only part of *the beginning* of the work, both conceptual and practical, that researchers in many disciplines must carry out to give us tools for building strategies to cope with unpredictable environments. Some readers may hope for formal models that can be tested and will lead to new, globally effective strategies for national security or business competition. Perhaps that will happen. But beware the simple answer! Be skeptical of the diagram with circles and arrows that indicate simple causes and effects. There is a real danger that the jargon of complex adaptive systems research will be used merely to dress up old ideas in new clothes. The problems are too important to have resources diverted to the management or policy fad *du jour*. There is probably not one answer, but many. We will not find the answers by trying harder to do the old things.

Chapter Two

Terminology

Because the readers of this paper (and the authors from whom we draw our terminology) come from many disciplines, we have carefully selected the terms used here. The terms and definitions chosen are consistent with their use in most disciplines and with common usage among nonspecialists, but their use in some professions may be slightly different or more specific.

2.1 Uncertainty

In some cases, "uncertainty" describes a situation where something is totally unpredictable: it could be anywhere in its possible range at any given time. This is also referred to as a "stochastic" situation. In other situations, an event is more likely to occur in particular places and the probability of its happening in a certain place can be calculated, but its exact location or timing remains uncertain.

Individuals and organizations reduce uncertainty by gathering information (or "news") about their system that allows them to make predictions. If they cannot find accurate information about certain topics, they transform this residual uncertainty into "risk" calculations that allow them to bet on probable outcomes.[1] For example, a person considering an investment in orange juice futures will want, and be able to find, information about current supplies and the condition of the current crop, but will not be able to find accurate information about hurricanes that might ruin the crop and drive up the price of the futures. In many situations, information about the intentions of others is missing, which results in high uncertainty.

We assume throughout this study that merely calculating the odds does not make the system less uncertain, but does make it more manageable because we can deal with the risk. Systems thus have various levels of uncertainty. At one end of this continuum are systems in which all the variables are predictable (A always follows B). Then there are systems that have low uncertainty (A almost always follows B) and medium uncertainty (we can calculate the probability that A will follow B). At the far end of this continuum are high uncertainty or stochastic systems (in which we cannot even predict a probability that A will follow B). In systems where uncertainty is relatively low it is easier to plan for any possible dangers, while in highly uncertain systems security becomes more problematic. It should also be noted that the ability to calculate probabilities that something will happen does not necessarily mean that we can also calculate the effects that this event will have.

---

[1] This use of these terms was developed by Arthur L. Stinchcombe, *Information and Organizations* (Berkeley, Calif.: University of California Press, 1990).

Clearly, we do not all view risk in the same way. There is evidence that tolerance for uncertainty is closely linked to culture. In countries with high aversion to uncertainty industrial sectors where information is not readily available or is hard to interpret grow more slowly.[2] The lack of information makes movement in these sectors seem very risky.

2.2 Risk and Risk Perception

We often use probability calculations to assign various monetary values to the probabilities that something will happen. This is often referred to as "risk management." It is how the premiums for all types of insurance are set and how people decide how much to bet at a casino. In practice, this type of risk can only be calculated where the Law of Large Numbers operates; that is, where a large number of independent entities can be observed and counted. We could not calculate the risk of a particular ship's being lost at sea if we knew about only a few ships that had sailed in that sea or if all the ships we knew about traveled in a convoy.[3] Insurance is a way of spreading risk across all the policy holders and the stockholders of the insurance company. Methods of discovering possible risks in the face of uncertainty include failure mode effects analysis, fault trees, and event trees, but most of us rely on "heuristics": what we have experienced before or hear about from trusted sources.[4] Thus, we are not prepared for New Surprises, where neither we nor anyone else have experience. However, risk management can give us a false sense of security and shift dangerous activity to new areas. For example, when the government mandated seatbelts in cars some people drove more recklessly,[5] and some arguments against government-funded terrorism insurance claim that it would make noninsured assets the preferred targets.[6]

Risk is clearly associated with lack of control in many areas of life. In a study of 700 business managers, almost three-quarters of them believed that all risks are controllable and that controlling risks is what managers do.[7] Some commentators have noted that the belief that one can control systems with more than modest levels of uncertainty may be why fads in technical

---

[2] For a recent application of this idea see Rocco R. Huang, "Tolerance for Uncertainty and the Growth of Informationally Opaque Industries," presented at the University of Amsterdam 2005, [On-line]. URL: http://papers.ssrn.com (Accessed on November 8, 2005.)

[3] For more examples of risk and how humans have dealt with it, see Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: Wiley, 1996).

[4] See James R. Chiles, *Inviting Disaster: Lessons From The Edge of Technology* (New York: Harper Business, 2001), 134–138.

[5] For other examples of this, see Bernstein, 334–337.

[6] Darius Lakdawalla and George Zanjani, *Insurance, Self Protection, and the Economics of Terrorism*, Working Paper of the RAND Institute for Civil Justice, WR-123-ICJ (Santa Monica, Calif.: The RAND Corporation, December 2003).

[7] Zur Shapira, *Risk Taking* (New York: Russell Sage Foundation, 1995).

analysis and analytic decomposition are so popular: people will reach for anything that gives them the appearance of control.[8]

In fact, decision makers (whether individuals or organizations) seem to have several blind spots when confronted with dangers in their environments, which makes their decisions about risks less than optimum.[9] These include limited awareness of alternatives, misperception of the probabilities of an event (e.g., assuming too much from a small sample), misperception of causation from correlation (i.e., assuming that if A and B usually happen together, then one must cause the other), and an inability to integrate information from multiple sources.[10]

Research indicates that perceptions of risks are not uniform in a given population and may vary (along with trust in risk management) according to factors such as experience, gender, social status, and worldview.[11] Some limited generalizations have been drawn, including:

- The public seems willing to accept voluntary risks roughly 1,000 times greater than involuntary risks at a given level of benefit;
- The acceptability of risk is roughly proportional to the real and perceived benefits; and
- The acceptable level of risk is inversely related to the number of persons participating in the activity.[12]

Since perception is often more important than reality when one examines what people are likely to do, this research has important implications for building strategies that will encourage people to deal appropriately with security-related issues. It also offers clues to improved communication in times of uncertainty or surprise and to the need for various trusted sources that will be acceptable to different individuals and groups (see **Chapter Six**). To achieve both of these goals, it is especially important to note the variability in and among populations and the reduced likelihood that "one strategy fits all."

2.2.1 Security

Security does not mean a complete absence of risk. Precious few things in life are 100 percent certain. Most of us are happy with an acceptable level of risk, usually discounting the

---

[8] Robert Jackall, *Moral Mazes: The World of Corporate Managers* (New York: Oxford University Press, 1988).

[9] For a critique of the efforts of local governments, see, e.g., Robert P. Wolensky and Kenneth C. Wolensky, "Local Government's Problem With Disaster Management: A Literature Review and Structural Analysis," *Policy Studies Review* **9**, 4 (Summer 1990), 703–725.

[10] See, e.g., Paul Slovic, *The Perception of Risk* (London and Sterling, Va.: Earthscan Publications, 2000), 1–31.

[11] Ibid., xxxv.

[12] Ibid.

[12] Slovic, 26 (citing C. Starr, "Social Benefit Versus Technological Risk," *Science* **165** (1969), 1232–1238).

harm by its likelihood of occurrence.[13] Information security expert Bruce Schneier reminds his readers that, “like any adjective, ‘secure’ is meaningless out of context.” An operating system for a computer that is not safe from hand grenades is not insecure.[14]

Security often adds to the cost of a system, and may be balanced against qualities such as efficiency. Efficiency is almost always the enemy of security (both resistance and resilience). Because it is almost always a tradeoff, security is not a state of being but a probability calculation: How probable is one possible scenario, and how probable is it that the potential danger will be more devastating than “normal” risks of this type? The important but difficult question is “How safe is safe enough?”[15]

2.2.2 Dangers

As a general rule, we think of security as freedom from some kind of danger or hazard. This danger could be one of two types or a combination of the two. An immediate physical danger will immediately injure or kill people (or their assets), while a deprivation of resources will injure or kill them (or their assets) over a longer period of time. A fire puts people in a burning building in immediate physical danger, whereas burning a village’s crops deprives the villagers of a critical resource and can lead to starvation. Poisoning a water supply would both put the local population in immediate physical danger and deprive them of a critical resource. Both physical harm and deprivation of resources can be known or unknown to the endangered individuals or groups.

Known dangers can be actual, threatened, or perceived. Someone may shoot a gun at you or threaten to shoot you, or you may perceive that someone is about to shoot you when the person suddenly reaches into a coat pocket. A terrorist organization may have captured a hostage, threaten to capture hostages, or engage in “chatter” about hostage-taking that makes intelligence agencies perceive this as a danger. Known dangers are easier to respond to and plan for, and the risks are easier to measure. For example, virtually all humans know that fire can both pose an immediate danger and lead to deprivation of resources, and so we have set up specialized organizations to fight actual fires, train people about the dangers of fire, and sell insurance to manage the risks associated with fires.

Some dangers are known to us, but we cannot predict where or when they will happen. We would not be surprised that there are icy roads in cold climates during winter but we might be surprised to find them on a particular day. We also do not know how severe these dangers might be when they happen: the roads could be only slightly icy or icy only in spots. We can calculate the chances of their being dangerously icy by looking at past weather data, but it is important to

---

[13] Bernstein, 70–71.

[14] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: John Wiley & Sons, Inc., 2000), 13

[15] Slovic, 80–103.

note that the iciness of the roads tomorrow is not absolutely predictable. A known danger whose timing or magnitude we cannot predict has also been called a "known unknown," or an UNK.[16]

There are dangers that we do not know about and will not know about until they hurt us (unknown unknowns—UNK UNKs). In some cases we do not see them in advance, because they operate at a different time scale than we are used to looking at. In other cases enemies design UNK UNKs to be new and unique so that they cannot be anticipated and will foil any resistance strategy that has been put in place. A plane flying into a skyscraper was, to most of us, an UNK UNK. Their very nature means it is not possible to plan for or perform risk analysis for UNK UNKs. This type of danger always comes as a surprise.

2.2.3 Surprise

Surprise has become a subject of much study and debate in the early twenty-first century.[17] In human systems surprise has been described as "the discrepancy between what is expected and what is experienced. It is of central importance in dislodging individuals from a previously adopted set of beliefs or models."[18] Several typologies of surprise have been developed: unexpected discrete events, discontinuities in long-term trends, and emergence of new information.[19] These have also been called local surprise, cross-scale surprise, and true novelty.[20] We will the term *surprise* to denote many types of unexpected occurrences and the term *New Surprise* (see **Section 2.2.5**) to denote unprecedented conditions or occurrences.

---

[16] UNK and UNK UNK have been standard slang in military circles for many years. One of the first uses of these terms in popular media seems to have been in Harold B. Jyers, "For Lockheed Everything's Coming Up Unk-Unks," *Fortune* (August 1, 1969), 77.

[17] See, e.g., Peter Schwartz, *Inevitable Surprises: Thinking Ahead in a Time of Turbulence* (New York: Gotham Books, 2003). For a discussion of surprise in many complex systems, see, e.g., John L. Casti, *Complexification: Explaining a Paradoxical World Through the Science of Surprise* (New York: Harper Collins, 1994) and other books noted in Appendix B.

[18] This definition comes from the Resilience Alliance, [On-line]. URL: http://www.resilience.org (see Key Concepts on that site). See also Carl Folke, Fikret Berkes, and Johan Colding, "Ecological Practices and Social Mechanisms for Building Resilience and Sustainability," in *Linking Social and Ecological Systems: Management Practices and Social Mechanisms for Building Resilience*, Fikret Berkes and Carl Folke, eds. (Cambridge, UK: Cambridge University Press, 1998), 36–37.

[19] Harvey Brooks, "The Typology of Surprises in Technology, Institutions, and Development," *Sustainable Development of the Biosphere*, W.C. Clark and R.E. Munn, eds. (Laxenburg, Austria: International Institute for Applied Systems Analysis, 1986), 325–3-47.

[20] Lance H. Gunderson, "Adaptive Dancing: Interactions Between Social Resilience and Ecological Crises," *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change* (Cambridge, UK, and New York: Cambridge University Press, 2003), 33–52.

2.2.4 Black Swans

Every once in a while, a severe storm strikes that forecasters did not anticipate. Even if we can usually predict local temperature and precipitation, there are those few times when things do not happen as our prediction tools tell us they should. This is because the weather is the classic complex, unpredictable system. The stock market has also seen its share of unpredicted rises and falls. Author and investment strategist Nassim Taleb calls these sorts of statistically unlikely (but possible) events *Black Swans*.[21] This refers to the dilemma posed by philosopher John Stuart Mill: no amount of observation of white swans can allow the inference that all swans are white, but the observation of a single black swan is sufficient to refute the conclusion.[22] Taleb suggests that failure to take the possibility of Black Swans into account can lead people to think their short-term predictions are infallible because they have not yet seen an unusual event. Like Paul Ormerod, Taleb believes that humans delude themselves about their ability to predict complex systems such as stock markets.

2.2.5 New Surprises

The category of genuine novelty, or the emergence of new information, is limited to situations that humans have never experienced or are "at least outside the breadth of captured experience for a culture in a new situation."[23] This might include the evolution of a new virus or the emergence of totally new technical, social, political, or economic phenomena. As people, businesses, cultures, countries, and economies become connected in new ways, the chances increase that New Surprises will emerge. Many of these New Surprises will present opportunities for some or for all, but others will only be dangers that no one has ever faced before. Because they are unprecedented, these surprises are nearly impossible to predict or prepare for, but systems can survive (or take advantage of) these surprises by having a broad inventory of resilience mechanisms in place.

2.2.6 Surprise and Crisis

Crisis occurs when a surprise reveals an unambiguous failure of the rules, norms, behavior, or infrastructure used to handle that type of surprise.[24] A crisis is often precipitated when the resources considered important in the system change dramatically (e.g., resources for security often become more important after an attack).[25] Thus, a crisis is more likely to happen where

---

[21] Nassim Nicholas Taleb, *Fooled by Randomness: The Hidden Role of Chance in Life and the Markets* (New York: TEXERE, 2004).

[22] Ibid., 110.

[23] Ibid., 33, 37.

[24] M. Janssen, "A Future of Surprises," in *Panarchy: Understanding Transformations in Human and Natural Systems*, L.H. Gunderson and C.S. Holling, eds. (Washington D.C.: Island Press, 2002), 241–260.

[25] From a presentation by D. Linda Garcia, at the Center for Communication, Culture, and Technology, Georgetown

these resources are not flexible or are designed to handle specific, predictable surprises. A crisis will precipitate a change in the rules that takes into account the newly discovered surprise and the change in resource priorities. The New York City Fire Department (NYFD) had rules, norms, behaviors, and infrastructure that were useful for dealing with surprise fires in a dense metropolitan area, but what they lacked on 9/11 were rules for coping with a fire so hot that it buckled a tall building's support structure. There is debate on whether this tragedy could have been predicted (or prepared for), but there is no question that the collapse of the World Trade Center buildings precipitated a crisis and a review of the NYFD rules and procedures. Can the NYFD make rules that will protect every firefighter in every situation? Can we make technology that never fails? Can we protect citizens from all of the possible types of terrorist attacks?

> Even if it were possible to reach perfection, it wouldn't matter for more than a short time, anyway. All complex systems mutate under pressure of technology and business, so what was good last week is different now. Every launch of the space shuttle is a little different from the last one because there are hundreds of suppliers in the chain, and they all have to change materials and techniques now and then. It's probably better not to believe in our own perfection, anyway, because it's such hubris that leads to the belief that failure is impossible.[26]

2.3 Coping Strategies

2.3.1 Resistance

Resistance is a strategy that attempts to keep the danger away from the system in the first place. Building a wall around a city is a resistance strategy if the city is likely to be attacked by large groups of people. Evolving a woolly coat in a northern climate helped some animal species to resist the cold. Screening people who come into a building is a resistance strategy. Even very simple organisms such as bacteria can evolve a resistance strategy as they become increasingly impervious to certain recurring (and thus "known") dangers such as antibiotics. Over many generations more of the bacteria that have the resistance factor (e.g., a particular shape of receptors on cell walls) survive to reproduce and eventually their descendants replace the nonresistant types.

2.3.2 Resilience

In situations where (as the Borg on *Star Trek* say) "resistance is futile" or will reduce access to other critical resources, building resilience is the next best thing. Resilience has been defined

---

University, Washington, D.C., December 17, 2004.

[26] James R. Chiles, *Inviting Disaster: Lessons From the Edge of Technology* (New York: Harper Business, 2001), 285.

as the "capacity of a system to absorb disturbance, undergo change, and still retain essentially the same function, structure, identity, and feedbacks."[27] If a system has resilience capacity it is more likely to be sustainable over a long period. Note that resilience does not necessarily mean that the system will look just as it did before a surprise. Often the system must adapt to new situations, but it will survive. Thus, a resilience strategy does not guarantee short-term stability, but a system that exhibits resilience is more likely to be stable in the long term.[28] However, stability is not always better than chaos and some level of chaos may protect certain systems from larger chaotic disruption.[29]

Resilience is often an *emergent*[30] property of the system and therefore is difficult to predict and manage. There is an ongoing debate in the biological sciences about whether diversity (the number of different entities in a system) increases or decreases resilience and stability.[31]

Resistance and resilience, and the technologies designed to enable them, are both important in defensive and offensive situations. An army attacking a walled city would prefer to resist (to have shelter from) the rocks and arrows coming from above rather than to have resilience (good medical care) after the missiles struck its fighters. **Chapter Four** deals with resilience in much greater detail.

2.4 Robustness and Fragility

In this study we adopt a slight different definition of robustness and fragility than has become common in engineering circles.[32] We use these terms to denote characteristics of both resistance and resilience strategies. Strategies (and their technologies) are *robust* if they continue to perform in the face of a wide array of challenges to the strategy; for example, backup electric

---

[27] Resilience Alliance.

[28] The term "resilience" is being used to refer to government goals for responding to emergencies in the UK. That nation has set up a special Resilience Center that is administered by Cranfield University and the Defense Academy of the UK.

[29] "… it should not be thought that stability is necessarily good and chaos bad. Some cardiologists believe that the young heart is chaotic and then loses complexity and becomes more vulnerable to pathological fibrillaton." Richard Levins, John Rock Professor of Population Sciences, Department of Population and International Health, Harvard School of Public Health, personal communication with the author, March 2005.

[30] Phenomena are said to be emergent when they arise from the collective actions of many uncoordinated agents. See, e.g., Steven Johnson, *Emergence: the Connected Lives of Ants, Brains, Cities, and Software* (New York: Scribner, 2001).

[31] See, e.g., Shahid Naeem, "Biodiversity Equals Instability?" *Nature* **416** (2002), 23–24.

[32] Robustness has been described as "the ability of a system to continue to operate correctly across a wide range of operating conditions, and to fail gracefully outside that range." This seems to be similar to the idea of keeping away dangers (resistance) but does not include the idea of adapting and bouncing back from a system failure (resilience). See, e.g., Steven D. Gribble, "Robustness in Complex Systems," in *Proceedings of the 8th Workshop on Hot Topics in Operating Systems* (New York: IEEE, May 2001), 21.

generators provide broadcasters with a robust resilience strategy for systems that may be surprised by power outages. A resistance strategy is robust if it keeps out a wide variety of dangers. A strategy is *fragile* if it works only under a small number of possible scenarios. Fragile strategies are not necessarily bad, and are often adopted for known dangers because specific tactics can de developed in advance that deal with those dangers efficiently and effectively. Tactical training for first responders (fire, police, emergency medical services, etc.) to deal in very specific ways with known dangers or UNKs will make these responders efficient and effective in those situations, but this same training can cause them to fail (and perhaps put them in danger) in the face of a Black Swan or a New Surprise.

Chapter Three

Surprises in Uncertain/Unpredictable Environments

3.1 What Is an Uncertainty?

As noted in Chapter Two, systems have various levels of uncertainty, from low to high. Some are predictable, some can be managed with probability calculations, and some are simply unpredictable—often because they are so complex.

Think of throwing a handful of buttons on the floor and then connecting them in various ways: some by heavy string, some by magnets, and others only by dotted lines on the floor. All the red buttons are connected to each other, and some of the red buttons are connected to blue buttons. Most (but not all) of the blue buttons are connected to one yellow button, while all of the red buttons are connected to another yellow button. The group of buttons lies on top of an active earthquake area. Could you predict what will happen to any one of the blue buttons if an earthquake struck or if someone pulled the string connected to one of the yellow buttons?[1]

This analogy can be used for many systems in the twenty-first century, including technical, economic, political, and cultural systems. They have intricate interdependencies, unequal strengths of the forces operating in them, and some of the forces acting on the system (such as weather) are not predictable. This makes the whole system unpredictable, at least on some scales.

Of course, some systems, both simple and complex, are designed to be unpredictable in order to foil resistance strategies. Participants in activities such as tennis, chess, and warfare will do something unexpected if they do not want an opponent to succeed by using a defensive strategy that has worked well in the past.

3.2 Coping with Surprises

Any system that involves uncertainty will produce surprises. Some of these surprises may present opportunities and others will only be dangers. Understanding surprise is critical for managing these systems. Surprises include natural disasters, economic fluctuations, epidemic diseases, and technological revolutions.[2]

The role of surprise in business management was first noted by Frank Knight in 1921 and echoed by John Maynard Keynes in 1936. Both rejected the possibility that the variables acting

---

[1] This is an adaptation of the “Buttons and Strings” metaphor used to explain complex systems in Stuart Kauffman, *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity* (New York: Oxford University Press, 1995), 55–58.

[2] M. Janssen, “A Future of Surprises,” in *Panarchy: Understanding Transformations in Human and Natural Systems*, L.H. Gunderson and C.S. Holling, eds. (Washington D.C.: Island Press, 2002), 241–260.

on a modern business can be measured and put into a universal mathematical formula or probability calculation. Knight reasoned that uncertainty was common in business systems because surprise was so common, even in the face of much calculation of probabilities. He believed these calculations were not helpful because the business world changes constantly and no two transactions are exactly alike. Therefore, it is not possible to obtain enough examples of independent actions necessary for the Law of Large Numbers to operate.[3]

In an increasingly interconnected world, most human systems are constantly co-evolving (one system changes in reaction to a change in another), making surprise more common than predictability. This is particularly true in technical systems that are interconnected with other technical systems as well as with the human systems that use them. We now have ample evidence of the uncertainty inherent in complex human and technical systems, and yet we are still surprised when these systems do not do what we predict. Sometimes we are surprised because we have been looking at the wrong scale. Sometimes something happens that has never happened before because several things are put together in a new way. Black Swans might be either local/global or slow/fast scale surprises. In either case, looking at all the history of one scale (all the white swans) will not predict the Black Swan that may appear if one looks at a longer or larger view of the system.

3.2.1 Local- and Global-Scale Surprises

Local surprises, or unexpected discrete events, can sometimes be understood, and made less startling, when they are seen in the context of a larger scale process. Local political variables can have surprising effects when they interact with global ones. A terrorist bomb would be a local surprise but not a surprise to those who knew what was happening at an international scale. We can prepare for these surprises (even if we cannot predict their time and place) by making sure that local levels are kept informed about what is happening at the global level.

Individuals can sometimes prepare for surprises at the local level. Preparations would include "…adaptations to risk that are amenable to economic rationality at the local level, including risk-reducing strategies and risk spreading or risk pooling across independent individuals."[4] So, for example, as electrical systems become more complex and less predictable, individuals could build resilience at the local level by buying generators for use when the power fails. Global weather patterns may affect communities in the form of storms or droughts. Recent evidence indicates that maintaining healthy ecosystems at the local level and building on local

---

[3] For a summary of Knight's and Keynes's views, see Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: Wiley, 1996), 215–230.

[4] Carl Folke, Fikret Berkes, and Johan Colding, "Ecological Practices and Social Mechanisms for Building Resilience and Sustainability," in *Linking Social and Ecological Systems: Management Practices and Social Mechanisms for Building Resilience*, Fikret Berkes and Carl Folke, eds. (Cambridge, UK: Cambridge University Press, 1998), 414–436.

knowledge were important for communities in Southeast Asia that bounced back quickly from the December 2003 tsunami.[5] Individuals can choose to purchase insurance against some surprises like this, but governments generally do not mandate insurance.

When the surprise occurs at the regional or global scale, it often results from links between local, regional, and global scales. In these cases, adaptations may require the coordinated effort of many individuals and institutions. Wars and revolutions often grow out of local or regional problems that become linked with and involve regional or global systems.

3.2.2 Slow/Fast Scale: Temporal Surprises

Some surprises are caused by failures to notice or appreciate an interaction between variables that usually operate at different time scales. These unexpected discontinuities in a long-term trend can occur when a fast variable interacts with a slow one. The Greeks saw two different kinds of time: *kairos* (opportunity or the right moment) and *chronos* (eternal or ongoing time).[6] Stewart Brand has described the operation of these different time scales this way:

> Some parts respond quickly to the shock, allowing slower parts to ignore the shock and maintain their steady duties of system continuity. The combination of fast and slow components makes the system resilient, along with the way the differently paced parts affect each other. Fast learns, slow remembers. Fast proposes, slow disposes. Fast is discontinuous, slow is continuous. Fast and small instructs slow and big by accrued innovation and occasional revolution. Big and slow controls small and fast by constraint and constancy. Fast gets all of our attention. Slow has all the power. All durable dynamic systems have this sort of structure; it is what makes them adaptable and robust.[7]

Fast-developing new technologies caused considerable surprise in the communications sector when they started to interact with the more established and stable media technologies. What surprised many people (perhaps even Brand) was that the small and quick technologies did not destroy the older, slower technologies, but instead instructed them. The new technology received all the attention, but in the end the old media retained great power and were necessary for the spread of the new technologies and ideas. “The new always acts through the old.”[8]

---

[5] Ibid.

[6] See, e.g., P.F. Brown, *Venice and Antiquity: The Venetian Sense of Past* (New Haven, Conn.: Yale University Press, 1997).

[7] Stewart Brand, *The Clock of the Long Now* (New York: Basic Books, 1999), 34.

[8] “No matter how strange the perturbation, its effects depend on the network. Inputs that are unique as they enter from the outside become more familiar as they spread through the system along preexisting pathways. *The new always acts through the old*.” Richard Levins, John Rock Professor of Population Sciences, Department of Population and International Health, Harvard School of Public Health, personal communication with the author, March 2005.

Surprises that result from interactions among systems that operate at different time scales could be predicted in a broad way (not for specific individuals or groups, or for specific time frames) by paying attention to these cross-scale temporal interactions. It is important to note that such systems may produce small surprises, but over the long term are more stable, and less surprising in big ways, because the slow parts can adapt to input from the fast parts.

While fast responses to surprises are generally preferred, they are sometimes too expensive, so they are backed up by responses that act on a slower scale. Professor Richard Levins of the Harvard School of Public Health has noted that some fast responses to surprise are too costly over the long term because they place what is known as an allostatic load on the system. For example, the human system known as homeostasis keeps our body temperature within a certain range, but this does not happen without cost. Over time the homeostatic system can erode, sometimes leading to increased variance in blood pressure in older adults. To prevent wearing out fast (but expensive) defense mechanisms, some systems have developed slower responses that step in when the surprise lasts a long time or recurs frequently.

Levins has developed what he calls Schmalhausen's Law: systems in extreme or unusual conditions, near the boundary of their tolerance, are more vulnerable to changes in every one of life's requirements. He notes that "As a result of allostatic load, we depend on a hierarchy of different defenses on different time scales, where short term responses that may be harmful if carried on too long will be replaced by slower responses that are less harmful."[9] The concept that slow response mechanisms can play an important role may offer insights in designing security for systems that produce many surprises. The slow response mechanisms might include changes in paradigms under which people manage these systems.

3.3 Managing Uncertainty?

We will always need to manage systems that are uncertain. Several factors have been observed to have an impact on risk in unpredictable systems, and thus to be relevant in making plans for managing complex situations and complex human organizations.

- Positive and negative feedback (and feed-forward) loops of different lengths. Long feedback loops, with communication traveling through many agents or subsystems, tend to be more complex and more likely to make the larger system unpredictable.
- Connectivity. The extent to which agents or units are all connected or are connected through hubs increases both the efficiency of the communication and the complexity of the system, perhaps making it more susceptible to cascading failure.
- The presence of "sinks" that absorb external impacts or "buffer" systems that mitigate unwanted variations in subsystems. Both sinks and buffers make the system

[9] Ibid.

> less susceptible to surprise and reduce the need to build complex responses. For example, immediately passing on the increased price of an input to a product to consumers acts as a sink that protects the firm from the impact of the price increase, and makes it unnecessary for the firm to build a complex system for response.[10]

In systems where no surprises can be predicted (or where they are deliberately ignored) strategies that incorporate these three features can protect individuals or groups. These strategies will work most of the time, which is to say, to the extent that the risk/benefit analysis dictates. More freedom from surprise (benefit) requires more feedback, more connectivity, or more buffer mechanisms (costs). If the price for greater predictability in the short term is more complexity, the ultimate price may be greater unpredictability in the long term. When it comes to security in complex environments, many engineers have come to the conclusion that "there is no free lunch":[11] there are always tradeoffs.

3.3.1 The Blame Game: Play With Caution

We cannot manage systems with high uncertainty unless we receive accurate feedback. If surprises are concealed because they are seen as "failures" of the system, the system can not adapt. Blame is often appropriate where known dangers have been ignored, but it is not appropriate as a reaction to Black Swans and New Surprises. In all cases, the energy it takes to fix and apportion blame is diverted from the adaptation process. This tradeoff must be acknowledged, especially in systems with high uncertainty. Will punishing someone because a surprise occurred keep a similar surprise from happening again, or will the people in the system try to resist such surprises by creating new restraints that will rob the system of efficiency or resilience—and ultimately be more expensive than the surprise? There is an important difference between identifying the potential causes of a surprise and finding somebody to punish. This is a significant problem in many countries and corporate cultures and deserves a broad and open debate.

---

[10] Levins, written comments and telephone interview with the author, July 2003.

[11] For more information on the "no free lunch" theorems see, e.g., Yu-Chi Ho, Qian-Chuan Zhao, and David L. Pepyne, "The No Free Lunch Theorems, Complexity and Security," *IEEE Transactions on Automatic Controls* **48**, 5, (May 2003), 783–793.

Chapter Four

Resistance and Resilience

What can we do if the possibility of surprise makes resistance futile or too expensive? In many systems with uncertainty, the answer is: become resilient. This chapter examines the concepts of resistance and resilience more deeply and links them to several other concepts often used to analyze systems with high uncertainty, including redundancy, efficiency, complexity, scale, tight/loose coupling, and networks. The chapter also describes how resilience strategies can fail.

4.1 Resistance: Keeping Everything Safe

Resistance strategies are appropriate for dangers that can be anticipated, that are likely to happen with some frequency, or that, when they do happen, impose higher costs than the system can endure. For example, fire-resistant building materials are undoubtedly appropriate in places where the risk of fire is fairly high or where many people, or vulnerable people, are likely to be found. They are less appropriate when they reduce the opportunities to resist other dangers (a woolly coat can lead to heat exhaustion in warm weather), restrict other survival options (a wall keeps local defenders from sending calls for reinforcements or reaching water supplies), or give a false sense of security (screening everyone entering by the front door, but leaving back windows open to let in air, will not protect a building against burglars). Classic resistance strategies include prevention and detection/response.

Prevention is resistance that keeps the bad thing(s) from happening. This can be an effective strategy if we know about the danger, but it is not effective against Black Swans and New Surprises. A “fortification” strategy (e.g., building a fortress) means that we must be able to defend the fortress at all points and at all times. We can build a fortress to protect a city or a firewall to protect a computer network, but any gaps in the perimeter put us in danger of creating a false sense of security and making us unprepared for surprises. Another type of prevention/resistance strategy is to build something to be unbreakable, such as a building that can withstand every imaginable earthquake. However, the earthquake might be the Black Swan that nobody imagined.

If barriers and heroic engineering cannot keep danger away, the next best strategy is to detect the dangers as soon as possible so that we can respond before too much damage occurs. *Detection/Response* strategies assume that we cannot keep all dangers from happening, but that we can detect danger and respond appropriately. Such strategies are usually necessary when the dangers must move through some sort of barrier. Detection can be accomplished by surveillance (watching all things moving in and through the system) or audit (watching all things that have moved) and then dealing with any detected dangers by removing them. We would prefer to keep thieves out of buildings that store valuables, but we cannot construct useful buildings with no

windows and doors. We therefore set up systems—human and/or technical—to detect intruders so that they can be arrested. We try to detect people carrying weapons onto planes. We try to detect computer viruses before we let them into local networks or local computers.

The human body contains perhaps the most complex detection/response system in existence. The human immune system is a diffuse, or distributed, informational and command network with no central control function. It simultaneously pursues overlapping and contradictory goal,[1] in part by layering new systems onto old ones (giving the new ones "scaffolding"), parallel processing by several systems, dynamic engagement (immune cells act for a short period of time and are then replaced by other cells), and variable network connectivity.[2] These types of distributed systems are powerful and flexible in dealing with known dangers, but they need time—often too much time—to respond to new surprises. These design principles are being studied for clues to security for computers and may have applicability for security in other distributed human systems.

Even if we cannot detect and respond to every instance of a danger, we can build resistance strategies that attempt to make an attack too expensive (e.g., the attackers will lose too many lives, or risk a lengthy prison sentence) or ensure certain retaliation will be directed at the invader's home base (in business terms, "If you come into my market I will go into yours"). The former resistance strategy is not effective if the enemies do not count the cost (e.g., they have many more suicide bombers or do not believe they will be caught); the latter will not work if the defender cannot inflict serious damage (e.g., take significant market share).

Camouflage strategies allow individuals and groups to resist danger by hiding from it. In some animal species, individuals or groups that are threatened find a way to make themselves inconspicuous, for example by becoming very still or by changing color to blend in with their environment. Other species take the opposite tack and apply enlargement strategies: they puff themselves up to appear larger or gather in large numbers to become more conspicuous as they confront the danger. At least one historian has argued that many countries, including the United States, typically respond to danger with expansion in the form of preemption, unilateralism, and hegemony.[3]

---

[1] Lee A. Segel, "Diffuse Feedback From a Diffuse Information Network: The Immune System and Other Distributed Autonomous Systems," in *Design Principles of the Immune System and Other Distributed Autonomous Systems*, Lee A. Segel and Irun R. Cohen, eds. (Oxford and New York: Oxford University Press, 2001), 203–226.

[2] Charles G. Orosz, "An Introduction to Immuno-ecology and Immuno-informatics," in Segel and Cohen, 125–149.

[3] See John Lewis Gaddis, *Surprise, Security, and the American Experience* (Cambridge, Mass.: Harvard University Press, 2004).

4.2 Resilience: When Resistance Is Futile or Too Expensive

The term *resilience* has slightly different meanings in the various disciplines where it has been used, but it always includes some concept of an individual's, group's, or organization's ability to continue its existence, or to remain more or less stable, in the face of a surprise, either a deprivation of resources or a physical threat. Unpredictable systems with low resilience have high vulnerability to surprise. The surprise may be partly predictable and come from a long-term trend (e.g., climate change), or a local Black Swan (hurricanes in the Caribbean). In the first case we can plan for specific resilience strategies (e.g., by creating adaptable artificial climates in buildings), but for a recurring surprise of unprecedented magnitude resilience means an ability to move appropriate resources quickly (e.g., emergency services and stockpiles of emergency supplies). A New Surprise will challenge entities that were well prepared for particular surprises, because efficient responses to what they knew about may lack the adaptability needed to deal with events they did not plan for; in other words, their resilience strategy lacked robustness. Resilience to New Surprises will be found in highly adaptable systems (those not locked into specific strategies) that have diverse resources.

As noted in Chapter Three, resilience does not mean stability. In most cases resilience will be the preferred strategy where stability is not possible or not desirable; in other words, when we want the system to adapt). In fact, many who have studied resilience in ecological and human systems see it most vividly in systems that undergo cyclical changes or life cycles.[4] Two different ways of thinking about stability and resilience—engineering resilience and ecological resilience—seem appropriate to different types of unpredictable systems.[5] Each may be appropriate at different points in the life cycle of a product, an industry, or an economy.[6]

Engineering resilience results from an effort to make a system return to one pre-designed state or function after it is disturbed. We want our computers to bounce back and do what they were designed to do. Resilience in these systems is measured in the time it takes to return to operation within system specifications. This type of resilience generally emphasizes efficiency and optimal performance. It is often suitable for systems with low uncertainty, but it can be inappropriate and even counterproductive when used in systems with high uncertainty, because it requires regulatory functions to reduce the uncertainty and these will often make the system more tightly coupled and brittle. Engineering resilience frequently makes very efficient use of

---

[4] See C.S. Holling and L.H. Gunderson, "Resilience and Adaptive Cycles," in *Panarchy: Understanding Transformations in Human and Natural Systems*, L.H. Gunderson and C.S. Holling, eds. (Washington, D.C.: Island Press, 2002); and Charles L. Redman and Ann P. Kinzig, "Resilience of Past Landscapes: Resilience Theory, Society, and the *Longue Durée*," *Conservation Ecology* **7**, 1 (2003), [On-line]. URL: http://www.consecol.org/vol7/iss1/art14 (Accessed on November 8, 2005.)

[5] See Lance H. Gunderson, C.S. Holling, Lowell Pritchard Jr., and Garry Peterson, "Resilience in Large-Scale Resource Systems," in *Resilience and the Behavior of Large-Scale Ecosystems*, Lance H. Gunderson and Lowell Pritchard, Jr., eds. (Washington D.C.: Island Press, 2002), 3–20.

[6] Gunderson and Holling, 25–62.

resources, but it would not be an appropriate goal if the system is intended to generate innovation and new opportunities.

Ecological resilience is found in systems that have high uncertainty and must focus on persistence and adaptation. The system can have several (or many) possible stable states and might flip from one to the other when disturbed. The key knowledge needed for designing ecological resilience concerns what happens at the boundaries of these states. For example, water flips to become a solid at a certain temperature and a gas at another temperature. Human systems (economic and political) have been known to flip from ordered to chaotic and then to a new order, when they are disturbed by war or lack of resources. In a system capable of flipping into new states (without perishing), the objective of returning it to any particular state may be unattainable if the variables acting on the systems have changed. It would be senseless to try to rebuild a buggy whip business after the introduction of the automobile flipped the primary mode of transportation. It would be difficult to replicate all of the systems and values of old institutions after a society has been changed by new ideas about human rights, democracy, or technology.

Ecologically resilient businesses and institutions will adapt to new variables that are active in their environment. This strategy is easier to recommend than it is to implement. As organizations set up ever more sensitive tools to give them feedback about changes in their environment they trigger ever more readjustments and "interlinking balancing acts," including the desire to reduce complexity and increase adaptability, resulting in "simultaneous sensations of progress and *déjà vu*."[7] But there is some evidence that the most resilient organizations are those that have some experience with surprise and have adapted in order to survive.[8] This view of successful organizations requires a new attitude about change; managers would assume that things will change and explain stability rather than assume stability and explain change.[9] A new view about resilience does not involve a massive revamping of expectations about what it takes to safeguard the investments of shareholders and the interests of other stakeholders, but new resilience strategies can be added to those already in use.

Many management theorists advocate expending more resources on resilience strategies by identifying potential risks and taking steps to deal with them.[10] This approach is also known as

---

[7] Anthony Oettinger, *Whence and Whither Intelligence, Command and Control? The Certainty of Uncertainty*, P-90-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=339 (Accessed on November 7, 2005.)

[8] Dennis S. Mileti and John H. Sorenson, "Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events," *Columbia Journal of World Business* (Spring 1987), 14.

[9] See Fikret Berkes, Johan Colding, and Carl Folke, "Synthesis: Building Resilience and Adaptive Capacity in Social-Ecological Systems," in *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change*, Fikret Berkes, ed. (Cambridge, UK, and New York: Cambridge University Press, 2003), 352–387.

[10] See, e.g., Gary Ahlquist, Gil Irwin, David Knott, and Kimberly Allen, "Enterprise Resilience," *Best's Review* (July 2003), 88.

risk management. These steps include making these goals part of the reward systems for managers.[11] Traditionally, risk management in the form of hedging bets (betting on several possible outcomes) and buying insurance was considered prudent in unpredictable environments, even though neither action contributes to revenue or profit.

4.2.1 Resilience and Redundancy

Another typical strategy for resilience in unpredictable systems is to build in *redundancy*: backup capabilities or whole separate systems that can take over when a surprise makes the main system inoperable or unavailable. Thus, many engineered systems, such as airplanes, have redundancy in all of their systems (mechanical, electrical, computer) to ensure that they can survive a surprise to the main systems. Some evidence indicates that in animal and human systems the redundant systems should not be copies of the original but should be able to re-create the capability in different ways to ensure that the system will have flexibility in its response.[12] In economics, redundancy often takes the form of substitutes for a particular good or service. The availability of substitutes serves to give a firm or an economy some stability because "…the greater the degree of redundancy in the form of substitutes, the more constrained price increases are likely to be."[13]

On the other hand, resources devoted to building redundancy must be taken from current efficiency. Building up resources that may never be used is expensive, and diverts assets from immediate efforts aimed at growth (getting more market share). If we save resources for a rainy day we cannot use those resources in the sunshine of today. If the management's bonus depends on how efficiently they ran the company this quarter, they are less apt to worry about any Black Swans that may be just over the economic horizon.

Building resilience through redundancy is thus often considered an inefficient use of resources, because it lowers returns and might force a firm to raise prices in the face of stiff competition. For firms whose customers have high expectations of reliability, large investments in redundancy can lead to disaster if the firm is confronted with a Black Swan or New Surprise that cannot be handled with redundant capability. In addition, redundancy and/or diversity could be counterproductive if they increase the complexity of the system, make the system more opaque and difficult to understand for the people who must operate in it, or lead people to place too much confidence in the system and forget to watch for surprises.[14] Heavy layers of redundancy or

---

[11] "Strategies for Weathering the Corporate Storm, *Financial Times* (20 August 2004), 7.

[12] For more on redundancy in various systems, see Bobbi Low, Elinor Ostrom, Carl Simon, and James Wilson, "Redundancy and Diversity: Do They Influence Optimal Management?" in *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change*,

[13] Fikret Berkes, Johan Colding, and Carl Folke, eds., *Navigating Social-Ecological Systems* (Cambridge, UK, and New York: Cambridge University Press, 2003), 83–114.

[14] These and other considerations when planning for surprises in high-risk situations are set out in Charles Perrow,

diversity can also make it possible to conceal errors and surprises (fearing the Blame Game), which results in less accurate information about how the system is operating.

All companies or institutions should adopt resilience measures that are justified by the level of surprise they face and the price they will pay for any surprise. MIT professor Yossi Sheffi suggests that resilience investments can often be justified "…by their contribution to flexibility—creating a competitive advantage for the company.[15] However, there is no one-size-fits-all resilience jacket.

Resilience strategies also differ when several organizations must work together. Tightly coupled organizations, such as military and public safety organizations, must bounce back to their previous roles when surprised. They must also deal with populations that may respond to the dangers of war or natural disaster by flipping into a new form of organization that will allow them to survive the danger. Recognition of this difference by all participating organizations would facilitate cooperation and communication.

4.2.2 Tradeoffs: Efficiency as the Enemy of Resilience

Plant and animal communities that experience frequent dangers often develop resilience. Individuals in these communities have high biotic potential (they can quickly regenerate new individuals) in the face of dangers such as drought, fires, or floods, provided the basic resource they need (e.g., nitrogen in the soil) is not destroyed in the surprise. Such communities are made up of many small individuals that reproduce quickly. In human systems, this is analogous to local economies that have many small firms (e.g., farms) that can return to production relatively quickly if the resource they need (arable land) has not been destroyed. The local aggregation of many small farms is almost certainly not as efficient as several very large ones would be, but this configuration will allow the system to bounce back more quickly, because it does not require rebuilding all the coordination functions necessary for reconstituting the larger organizations.

Modern telecommunications firms offer another example of how efficiency can become the enemy of resilience. Most of these firms have attempted to increase efficiencies through the use of fiber optics and "digital loop carriers" between central offices and homes—functions that used to be performed with copper wires that also carried low-voltage electrical power. Digital telephony technologies often reduce costs and increase capacity, but their deployment comes with a resilience trade-off: when electric service fails, these telephone services will fail as well. Telephony services offered by cable companies also lack a separate power source and are not

---

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

[15] Yossi Sheffi, *The Resilient Enterprise: Overcoming Vulnerability for a Competitive Age* (Cambridge, Mass.: MIT Press, 2005), 279.

operable during power outages, but they make efficient use of the cable infrastructure and are often cheaper than services offered by telephone companies.[16]

In some biological communities, resilience comes from the ability of individuals to move away from the danger. Deer survive a forest fire more often than shrubs because they can run from the approaching flames. However, shrub species survive if they can regenerate new individuals quickly after the fire. Thick bark often gives trees a resistance strategy, but if the fire penetrates this defense the tree species will find it difficult to come back because the reproduction cycle is so long. In human communities, plans for freedom of movement are often built into local systems. Transportation systems designed to take many people from one place to another, such as high-capacity roads, enable people to get away from danger without creating local bottlenecks. In architectural design, this translates into a requirement for exits that allow all the people in the building the freedom to get out in a short period of time, but there are always design tradeoffs. Giving the building better operating efficiency reduces this freedom of movement. For example, it is tempting to devote less space to corridors and stairwells that are seldom used, raise heating/cooling costs, and may increase the need for surveillance to detect intrusion, but in the event of a Black Swan or a New Surprise this design decision will demonstrate once again that efficiency is the enemy of resilience.

In yet other biological communities, resilience rests on the ability of individuals to tolerate a broad range of conditions. Sometimes this means that individuals can obtain the resources they need (water, food, shelter) from several different sources. For example, wolves can eat mice if their usual prey is not available, giving them a broad range of resource options. In other situations broad tolerance means individuals are designed to adapt themselves to changing conditions. Some species can go into hibernation when water supplies are low; others can change their breathing pattern to a “pant” to cool themselves if the temperature becomes too hot. But if an animal species evolves to be maximally efficient in its current environment, it can lose the ability to eat other foods or adjust to changes in the environment. The predator that evolves to become the best rabbit hunter in an environment with many rabbits risks losing its resilience if the rabbit population plunges and the predator must hunt for other types of food.

Humans’ ability to find new ways to meet their needs in the face of surprise greatly increases broad-tolerance resilience. We can figure out alternative ways to procure water, food, and shelter because we can plan in advance. We expect to be surprised, and the more likely the surprise (or the more likely that it will have severe effects), the more likely it is that individuals or groups will adopt a strategy for broad tolerance. In economic systems, broad tolerance can be thought of as “dynamic” efficiency that gives a system adaptability, but not “static” efficiency

[16] Peter Grant, “Phone System’s Weak Link: Storms Cause Greater Outages in New Fiber-Optic Networks as Bell South Races to Recover,” *Wall Street Journal* (September 19, 2004), B1.

that would allow better use of resources in a stable business environment where adaptation by firms is not necessary.[17]

4.2.3 Resilience and Diversity

When a group (whether a species or a business organization) must operate in an environment where resources are unpredictable and competitors or predators are common, one strategy that often gives the group resilience is to try many things—lay many eggs, develop many new products—and hope that some of them can survive whatever challenges they encounter. Thus, *diversity* can be a tool for resilience. It does not mean that the group will not suffer a loss, but it does mean that the group will not lose everything. However, when a system becomes more diverse it tends to become more complex, as interaction networks spread unevenly and the forces working on the system have different effects on the diverse population.[18] Some evidence suggests that, at least in biological systems, an increase in the number of species will increase the efficiency and stability of some system functions but decrease the stability of the populations of all the species. Thus, what might increase stability at one scale might decrease it at another scale. There remains a serious debate in biological science about the relationship between diversity and stability. Some argue that diversity enables stability, because it acts as insurance: if danger appears, a system is more likely to recover if it contains species with various strategies or tolerances. On the other hand, some experiments have indicated that low-diversity systems regain more biomass faster.

These insights about diversity in biological systems are beginning to be applied to human organizations and to generate similar controversies.[19] Some have argued that organizations with diverse structural components and/or resources are more likely to keep working in the event of economic or technical surprise.[20] This has been specifically recommended for planning telecommunications services.[21] Certainly, diversifying, or hedging, one's investments when the outcome is uncertain is a strategy as old as mankind. However, it has also been noted that diversity is not, and should not be, a static phenomenon. Organizations or subunits must be allowed to fail in order to sort out successes and enable the organization to adapt, thereby

---

[17] Burton Klein, *Dynamic Economics* (Cambridge, Mass.: Harvard University Press, 1977), 35–67.

[18] Shahid Naeem, "Biodiversity Equals Instability?" *Nature* **416** (2002), 23–24.

[19] See, e.g., Ian McCarthy and Jane Gillies, "Organizational Diversity, Configurations and Evolution," in *Complex Systems and Evolutionary Perspectives on Organizations: The Application of Complexity Theory to Organizations*, Eve Mitleton-Kelly, ed. (Oxford, UK: Elsevier Science, 2003), 71–97.

[20] M.T. Hannan, "Uncertainty, Diversity, and Organizational Change," in *Behavioral and Social Sciences: Fifty Years of Discovery*, N.J. Smelser and D.R. Gerstein, eds. (Washington D.C.: National Academy Press, 1986).

[21] *BITS Guide to Business-Critical Telecommunication Services*, Washington, D.C.: BITS, 2004), [On-line]. URL: http://www.bitsinfo.org (Accessed on November 8, 2005.)

reducing diversity at least temporarily.[22] The opportunity that the debate gives to reexamine ideas about organizational resilience may make the journey worth the effort, even if one discipline does not closely inform the other.

We see at least some evidence that the strategy of "try many things and let the failures go" might hold true in human systems. For example, businesses have been told that they can build resilience by developing "a broad portfolio of breakout experiments with the necessary capital and talent"[23] that will include winners and losers. "Most experiments *will* fail. The issue is not how many times you fail, but the value of your successes when compared with your failures."[24] If a business has high uncertainties, diversity becomes even more important.

> The more uncertainty individuals or organizations must deal with, the broader must be their concept of diversity. In a certain world diversity is defined most narrowly and consists of known alternatives. Ina world of weak uncertainties it consists of alternative probability functions….In a world of strong uncertainties, it consists of more or less randomness in hints.[25]

Few industries must deal with as much uncertainty as the U.S. film industry. Many films are released every year, but only a few are major successes, and nobody can consistently guess which ones they will be. Instability at the level of the individual movie does not mean instability at the level of the industry.[26] These examples from business seem to be consistent with other systems where resources are unpredictable and follow a power law distribution: one in which the distribution of individual units (movies, products, offspring) does not follow a bell-shaped curve with most of the units appearing in the middle, but instead has most of the units in the first part of the graph and a "fat tail" at the end. The key to the success of these systems seems to be accepting many failures at one level to find the one thing (movie, body type, etc.) that will bring significant gains.[27]

---

[22] See, e.g., David Stark, "Heterarchy: Distributing Authority and Organizational Diversity," in *The Biology of Business: Decoding the Natural Laws of Enterprise*, John Henry Clippinger III, ed. (San Francisco: Jossey-Bass, 1999), 153–179.

[23] Gary Hamel and Liisa Valikangas, "The Quest for Resilience," *Harvard Business Review* (September 2003), 54.

[24] Ibid., 60.

[25] Klein, 51.

[26] P.H. Longstaff, Raja Velu, and Jonathan Obar, *Resilience for Industries in Unpredictable Environments: You Ought to Be Like Movies*, P-04-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=595 (Accessed on November 7, 2005.)

[27] For how funded research results in many failures but some big successes, see F. M. Sherer and Dietmar Harhoff, "Technology Policy in a World of Skew-Distributed Outcomes," *Research Policy* **29**, 4–5 (April 2000), 559–566.

Both ecology and network science provide evidence that some members of a diverse group seem more important than others. Members that are highly connected to all the others may be "keystones" or "hubs" that support many others.[28] Some species become critical by moving between systems (mobile links), connecting them in space and time, and thereby making the connecting systems more resilient.[29] Removing these connecting individuals or species from the system causes much greater loss of diversity that removing less connected individuals or groups.[30] Resilience would improve if these keystones had some functional redundancy with other individuals or groups: if they are removed from the system, some other thing or function would perform their role. For example, telephony is a keystone communications function in developed countries. If something happened to make it unavailable, the system would be more resilient if an alternative communications system could take over this function. This became clear in the electrical blackout on the east coast of the United States and Canada in August 2003. Cell phones could not operate because of high demand that caused overloading of the system, but people caught in the blackout could use pay phones and the wired telephony system. In most cases, however, this did not give them access to the mass media that could tell them about the situation. Most people did not have wireless or battery-operated radios or television sets, but some were able to gather around cars that powered their radios from the car battery.

4.2.4 Resilience and Complexity

The world and the projects we undertake are continuously becoming more complex. This complexity has come about in large part because people and businesses are more closely linked to each other both physically and virtually through transportation and communication networks. Being connected to more people and more places means there are more forces that we can affect and that can affect us. The more forces at work, the more complex the system becomes, and the more complex it becomes, the more uncertainty there will be.

Does more complexity make the system more or less resilient? There was a longstanding belief in ecological circles that the complexity of an environment—more species, greater connection among them, and stronger links—would make the environment more resilient or more stable in the long run; that is, less likely to change radically in the face of some surprise. This

---

[28] The idea that connection counts has been clearly demonstrated in studies of the diffusion of technology and is known as "network effects." See M. L. Katz and C. Shapiro, "Systems Competition and Network Effects," *The Journal of Economic Perspectives* **8**, 2 (Spring 1994) 93–115.

[29] Jacob Lundberg and Fredrik Moberg, "Mobile Link Organisms and Ecosystem Functioning: Implications for Ecosystem Resilience and Management, *Ecosystems* **6** (2003), 87–98.

[30] Lance H. Gunderson, C.S. Holling, Lowell Pritchard Jr., and Garry Peterson, "Resilience in Large-Scale Resource Systems," in *Resilience and the Behavior of Large-Scale Ecosystems*, Lance H. Gunderson and Lowell Pritchard, Jr., eds. (Washington D.C.: Island Press, 2002), 8–9. A similar idea has been developed in "network science." See, e.g., Albert-Laszlo Barabasi, *Linked: The New Science of Networks* (Cambridge, Mass.: Perseus Publishing, 2002); and Mark Buchanan, *Small Worlds and the Groundbreaking Science of Networks* (New York: W.W. Norton, 2002).

theory has now been called into question and some evidence indicates that simple systems that have robust resilience strategies (because they operate in unpredictable environments) will meet surprises more successfully than complex ones. In some experiments, resilience seemed greatest when the system was made up of simple organisms with short life spans and population turned over rapidly. Foxes tend to be longer lived than fruit flies and the population does not turn over as fast; thus, the fruit fly population is more likely to bounce back quickly.[31]

The complexity of technology—particularly technology aimed at ordinary consumers—has raised increasing alarm in many circles. People do not know how to operate all the features of a system and become frustrated by system failures that they can neither predict nor remedy. Sooner or later this frustration will reduce trust in these technologies. *The Economist* (no technological Luddite) has called upon businesses to rethink the value of complexity in products and pricing plans, and pointed to new commitments to simplicity by computer and information technology firms.[32] Aside from the difficulty of learning to operate (or cope with) these complex technologies there is the very real, but generally unacknowledged, problem that engineered complexity increases uncertainty. This can have terrible consequences if we depend on certain responses from a technology to keep us safe (resistance strategy) or help us bounce back after a surprise (resilience strategy).

4.2.5 Resilience and Scale

There is almost universal agreement that the best starting point for trying to manage an unpredictable system is to identify the various temporal and organizational scales involved. Surprises that manifest themselves over a long period of time require different strategies than Black Swans that can pop up at any time.

In systems that operate at more than one scale, resilience may operate at each scale and across the scales. For example, in the human body, the immune system acts first at a local scale to confront an infection by sending a variety of forms of immune cells (within-scale resilience through diversity). But if this strategy fails, the system responds by "scaling up" its response and inducing fever. When similar functions (not necessarily similar mechanisms) operate across scales, they make the system more resilient because they are redundant: if one fails, the other goes into action. For example, it has been noted that al Qaeda was resilient despite the arrests of many top members, because it operated on two separate levels: one with a traditional top-down

---

[31] See Michael Begon, John L. Harper, and Colin R. Townsend, *Ecology: Individuals, Populations, and Communities*, 3rd ed. (Oxford, UK, and Cambridge, Mass.: Blackwell Science, 1996), 838–860; and Robert E. Ricklefs and Gary Miller, *Ecology* (New York: W.H. Freeman & Co., 1999), 368.

[32] *The Economist*, U.S. ed. (October 30–November 5, 2004), editorial, Special Survey of Information Technology, "A Byte's-eye View of Complexity," 8–9.

structure and one with “freelance franchisees.” These two levels of organization gave it resilience when the first level was degraded by arrests and by being cut off from its resources.[33]

Each level of these systems operates separately, and often each level has its own emergent properties and/or operates over different time scales and responds to different cycles. The majority of interactions usually take place within a scale, but scales often interact. To understand how the whole system functions it is necessary to look at all of the scales at which it operates. It is unlikely that there will be only one appropriate perspective from which to view the entire system. Two types of cross-scale interactions have been identified: *revolt*, when events at a smaller scale trigger change at a larger scale, and r*emembrance*, when events or conditions at a larger (or longer) scale limit the options at smaller (or shorter) scales.[34]

Some forces have an impact at all scales, but the impact will be different at each level. In the early twenty-first century, some of these meso-scale drivers of instability, or change, include demographic changes (e.g., age distribution, migration to urban areas or wealthier countries) and globalization (greater connectedness through advanced communication and transportation networks). As noted above, greater connectedness often makes a system more complex and less resilient.

Many authors have noted that slower parts of systems act as resilience mechanisms for the faster parts because they can “remember” how to handle certain surprises. In return, the faster parts of the system give the slower parts information about changes taking place and allow the system to adapt at its own time scale. The Federal Emergency Management Agency and nongovernmental organizations (NGOs) such as the Red Cross are good examples of systems that operate at a different scale from local emergency responders and are most helpful in situations where they “remember” surprises that the local levels have never seen before.[35]

4.2.6 Resilience and Tight/Loose Coupling

In times of surprise individuals and groups often tend to come together and move in lock step to resist the danger—like a phalanx of infantry arrayed against an invading army. For some kinds of surprises, such as epidemics of infectious disease, this tight coupling is more dangerous. If the epidemic is a Black Swan or New Surprise, we may want to try a variety of resilience strategies. The benefit of tight coupling is often illustrated by tying together a number of wooden

---

[33] Robert Block and David Cloud, “Experts Reassess al Qaeda’s Strength,” *Wall Street Journal* (August 16, 2004), A4.

[34] See, e.g., Fikret Berkes, Johan Colding, and Carl Folke, eds., *Navigating Social-Ecological Systems* (Cambridge UK: Cambridge University Press, 2003), 19.

[35] For a history of disaster management in the United States, see, e.g., Roy S. Popkin, “The History and Politics of Disaster Management in the United States,” in *Nothing to Fear: Risks and Hazards in American Society*, A. Kirby, ed. (Tucson, Ariz.: University of Arizona Press, 1990), 101–129.

twigs that can be snapped easily; as a bundle they cannot be snapped. But what happens if the danger they face is a fire? Now if one catches on fire they will all go up in smoke.

Like the system of variously connected buttons mentioned in Chapter Three, the components (or individuals) in most systems have connections that vary in strength. Robert Glassman, who originally wrote about loosely and tightly coupled systems in biological systems, saw that the concepts he developed could be applied to many organizations. His ideas have been applied to military organization,[36] organizational development,[37] cooperation among business firms,[38] and many other fields.[39] Glassman described the fundamental process of organization this way: "As soon as the relation between two entities A and B becomes conditional on C's value or state, then a necessary component of organization is present."[40] He then noted that the strength of that relationship (whether it is loose or tight) is important to understanding how the system reacts to stimuli. Several similarities in loosely coupled and tightly coupled systems have been identified and are used to help understand these systems, even if they cannot always predict their behavior precisely.

In *tightly coupled organizations* any change in one component (individual or subsystem) of the system engenders an immediate response from the other component(s). Any organization that requires an organization-wide rapid adjustment to new conditions is likely to be tightly coupled. A system could be tightly coupled if its components share many variables or the link between the variables is very strong. Engineered systems with automatic controls are said to be tightly coupled (if A happens, then B is the automatic and immediate response). These systems often have very tight feedback and feed-forward loops that attempt to control all variables. Since anything that affects one part of a tightly coupled system affects all parts, these systems are often unstable because the individual parts cannot adjust to maintain their local stability. They are not associated with persistent behavior because they adjust as a unit to changes in the environment.

In *loosely coupled systems* the components have weak enough links that they can ignore small perturbations in the system. The components have more independence from the full system than tightly coupled components, since they can maintain their equilibrium or stability even when

---

[36] Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton, N.J.: Princeton University Press, 2000).

[37] John W. Meyer and W. Richard Scott, *Organizational Environments: Ritual and Rationality* (Beverly Hills, Calif.: Sage, 1983).

[38] Marc J. Dollinger, "The Evolution of Collective Strategies in Fragmented Industries," *Academy of Management Review* **15**, 2 (1990), 266–285.

[39] For a comprehensive review, see J. Douglas Orton and Karl E. Weick, "Loosely Coupled Systems: A Reconceptualization," *Academy of Management Review* **15**, 2 (1990), 203–223.

[40] Robert B. Glassman, "Persistence and Loose Coupling in Living Systems," *Behavioral Science* **18** (1973), 84. For an excellent overview of these ideas, see Karl E. Weick, "Educational Organizations as Loosely Coupled Systems," *Administrative Science Quarterly* **21** (March 1976), 1–19.

other parts of the system are affected by a change in the environment. They are also better at responding to local changes in the environment, since any change they make does not require the whole system to respond. This has been seen in research on effective strategies for managing emergency response organizations: a "problem solving" approach has been called superior to a command-and-control style because it encourages local answers to emerge.[41]

Thus, if innovation or localized response to particular problems is a goal, then loosely coupled systems would seem most appropriate. A more tightly coupled system could lead to premature convergence on a solution, as all the components would respond more or less in unison. However, if the goal is standardization across the entire system, then a tight coupling of the entire system (including all subsystems) is more likely to yield the desired outcome.

The various scales of a system can also be tightly or loosely coupled. In some cases, when the slower parts lack information about surprises (or changes) at the local level, they are liable to drastic, cascading effects when the changes reach a critical level, particularly when the entire system becomes tightly coupled. The very connectedness that makes it efficient can amplify internal weaknesses or external shocks. This has been seen in many systems.

> When the system is reaching the limits to its conservative growth, it becomes increasingly brittle and its accumulated capital is ready to fuel rapid structural changes. The system is very stable, but that stability derives from a web of interacting connections. When this tightly connected system is disrupted, the disruption can spread quickly, destabilizing the entire system. The specific nature and timing of the collapse-initiating disturbance determines, within some bounds, the future trajectory of the system. Therefore, this brittle state presents the opportunity for a change at a small scale to cascade rapidly through a system and bring about its rapid transformation. This is the "revolt of the slave variable."[42]

Managers of functions that have reached this tightly coupled, highly interconnected stage should thus be looking for small, local changes or small errors that can cascade through the system. If this is a real danger, the best strategy may *not* be to get even more tightly coupled but to start a decoupling process that allows the errors to die out locally before they spread in undesirable ways.

It must be emphasized again that resilience is not the one answer to all planning problems in systems with high uncertainty. In fact, resilience can harm a system if it allows a bad condition to

---

[41] Russell R. Dynes, "Community Emergency Planning: False Assumptions and Inappropriate Analogies," *International Journal of Mass Emergencies and Disasters* **12**, 2, 141–158. For another point of view, see Robert P. Wolensky and Kenneth C. Wolensky, "American Local Government and the Disaster Management Problem," *Local Government Studies* (March/April 1991), 15–32.

[42] Gunderson et al., 12–13, citing Diener and Poston, 1984.

persist. Some of the most maladaptive practices, the worst managers, the most ineffective governments, and the most murderous terrorist organizations are very resilient. In the long run, a resilient system will protect its functions, not its functionaries. It must be able to generate novelty that will reject what works badly and discover things that work better.

4.2.7 Networks and Resilience

A new, and growing, body of work examines the connections between things that function as a network. Network science came to the attention of those outside the academic community as the "small world" problem and, more recently, the "Kevin Bacon game." The former is the puzzle of why most people in the U.S. seem to be separated from one another (in terms of social linkages) by only six other people, or six degrees of separation. The latter uses movie actor Kevin Bacon and his connection to other people in the film industry to test the degrees of separation between them.[43]

This new research on networked systems emerged from a branch of mathematics known as graph theory. It is now being examined by many disciplines including political science, biology, sociology, and computer science. In some of the networks studied, the distribution of entities in the network (e.g., wealth, Web links) follows a "power law," and the place of any particular entity in that distribution is difficult to predict. As noted above, networks that exhibit a power law distribution are characterized by a continuously decreasing curve, with many small entities coexisting with a few large ones; for example, many people with small amounts of money and a few with large amounts, or many Web sites with a few links and a few with many links. This contrasts with systems where the distribution follows the typical bell curve, with a few entities at either end of the spectrum—for instance, a few small ones at one end and a few large ones at the other—but most clustered in the middle.

Networks following a power law may develop differently from other systems. They seem to grow one node at a time: one Web page at a time, or one person at a time. Some nodes have preferential connections, because the more connections they have the more they will get. These superconnected nodes are called *keystones* or *hubs*. For example, some nodes become hubs when they are connected to more nodes, often by others, because they were the first to fill a connection role or because they have more resources to devote to connections. Thus, the first EBay-type Web site or a very large company such as Microsoft (with perceived resources to devote to connection) is more likely to become superconnected. In these systems the connected tend to become more

[43] For a more comprehensive discussion of the game and why it is important even outside of Hollywood, see, e.g., Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (New York and London: W.W. Norton & Co., 2003), 92–100.

connected not necessarily because they are better, but because they got there first or were bigger to start with.[44]

Some networks have what is known as a "scale-free" topology: that is, many small nodes connect to a few larger nodes that in turn connect to still larger nodes in a hierarchical configuration. The lower level nodes have no way to connect to other nodes in the system except through their local hub. The telephone network does not allow us to connect directly to anyone except through our local exchange, which acts as a hub for our area. Unfortunately, we are now discovering that this type of network will often

> …perform terribly under conditions of failure. For the same reason they are vulnerable to congestion-related failure (because they are too centralized), if any of the hierarchy's top nodes do fail, they will isolate large chunks of the network from each other. It is here that connectivity at all scales really comes into its own, for in multiscale networks there is no longer any "critical" nodes whose loss would disable the network by disconnecting it. And because they are designed to be decentralized not only at the level of teams but also at larger scales, they can survive bigger failures.[45]

Multiscale networks allow nodes to connect across scales without requiring them to go through a hierarchical routing system. While this may not be the most efficient configuration, it does make the network resilient; that is, allows it to survive failures, because taking out the one hub to which the node is connected, or those that it connects to, will not deny access to the whole system.

In some networks the "winner takes all" if one node has all the connections and there is one giant hub with many nodes.[46] When nodes can choose which hub they will use to connect to the system they will choose the hub that gives them the most connections. The more connections a hub has, the more likely it will be chosen, and eventually the system will tip and all will choose the most connected hub.[47] In fact, there is strong evidence that the Internet is a winner-take-all network and only a few sites will have superconnections.[48] Any time a hub is added to a random network of individuals or groups the result is likely to be this "plutocratic" (the rich get richer)

---

[44] See, e.g., Albert-Laszlo Barabasi, *Linked: The New Science of Networks* (Cambridge, Mass.: Perseus Press, 2002), Chapter Six.

[45] Watts, 285.

[46] Ibid., Chapter Eight.

[47] A similar thing happens when people must choose a technology to connect to the system. They will choose the one that gives them the most connections to things in the system. The battle between VHS and Betamax was an example of this. The system tipped to VHS when consumers perceived that it gave them access to more movies.

[48] See, e.g., Barabasi, Chapter Eleven.

configuration, where power and scarce resources are drawn to the spot with the most resources.[49] Networks where superconnected hubs form are often very resilient at lower levels, because destroying any of the less connected nodes will have little impact on the system. This strength is also their Achilles' heel, because destroying a superconnected hub can destroy the entire network. In a business context, for example, any firm that becomes a superconnected hub for its sector presents both an opportunity for efficiency and a danger, because it can bring the entire industry down with it.

As with other complex systems, research on networks also indicates that the strength of the ties between elements is critical for understanding, if not always predicting, the operation of the networked systems. Good evidence shows that weak ties, or loose couplings, are often more important than strong ones when dealing with a new opportunity or problem. If two groups are strongly linked (or tightly coupled) to each other, they are probably also strongly linked to each other's links, so what happens to one will affect all of them. Strong links work very efficiently as long as the groups (individually or collectively) do not face unique challenges or encounter new opportunities. If something unexpected happens, the weaker links of each entity will be bridges to other systems with other resources or ideas that can be used when they face a new problem.[50] Thus, the long-term stability of a group or an entity may actually increase if the group or entity has many weak ties, even if this means it is less predictable or less efficient in the short term. This has led to speculation that a balance between the need for stability and diversity is necessary, and the appropriate strength will depend on the number of connections available. "[T]he superconnected few should be linked to others mostly by weak links, while those with few links to others should be connected by strong links."[51]

Network resilience also improves if hubs have some functional redundancy. If they are unexpectedly removed from the system, there is something or some function that will perform their role in the system. For example, if telephone communication becomes unavailable due to the damage to a switch at a hub, the system would be resilient if there was a backup switch or if there were some other way to perform this function.

While this work on resilience in complex networked systems is still preliminary, Duncan Watts, one of the original researchers in this area, stated:

---

[49] This "rich get richer" phenomenon is observable even in physical systems with no "choice." For example, snowflake growth is often governed by this rule. If one of the plates of a developing snow crystal is a bit longer than the other, it will pick up more of the scarce water vapor and grow faster. The longer it gets, the more water vapor it gets, and eventually one plate will "win" over the other. See Kenneth Libbrecht, *The Snowflake: Winter's Secret Beauty* (Stillwater, Minn.: Voyageur Press, 2003), 78.

[50] See, e.g., Mark Buchanan, *Nexus: Small Worlds and the Groundbreaking Science of Networks* (New York and London: W.W. Norton & Co., 2002), Chapter Two, "The Strength of Weak Ties."

[51] Ibid., 149.

> Already we can understand that connected, distributed systems, from power grids to business firms to even entire economies, are *both* more vulnerable and more robust than populations of isolated entities. If two individuals are connected by a short chain of influences, then what happens to one *may* affect the other even if they are completely unaware of each other. If the influence is damaging, then each is more vulnerable than they would be if they were alone. On the other hand, if they can find each other through that same chain, or if they are both embedded in some mutually reinforcing web of relations with other individuals, then each may be capable of weathering a greater storm than they would be by themselves.[52]

Most people who must deal with security in uncertain environments would probably agree with these sentiments, even if they do not understand the science behind them.

4.3 When Resilience Fails

Resilience fails when the system loses its capacity to absorb disturbance or undergo change while still retaining essentially the same functions, structures, identity, and feedbacks. The individual dies or the group reorganizes, but looks completely different before. This happens when the danger is "too novel, too fast, or too abundant."[53] The system does not have response capabilities that are diverse enough, it cannot marshal these responses quickly enough, or the danger is so great that all responses are overwhelmed. The danger may become overwhelming if the system has been weakened by previous dangers and has not had time to recover. The system may also fail if those managing it impose a response that is not consistent with the local system's own trajectory or "path dependence," such as the growth patterns of a city[54] or the attempted containment of fire ants.[55] This reminds us that there is unlikely to be a single resilience strategy that works for all systems made up of many units with different histories and different local resources. If a global strategy is imposed, the resilience of some local groups will fail.

The next chapters address the "So what?" question and examine how these ideas about resilience play out when considering strategies for human resilience.

---

[52] Watts, 303.

[53] C.R. Allen, "Ecosystems and Immune Systems: Hierarchical Response Provides Resilience Against Invasions," *Conservation Ecology* **5**, 1 (2001), 15, [On-line]. URL: http://www.consecol.org/vol5/iss1/art15 (Accessed on November 8, 2005.)

[54] H.A. Makse, S. Havlin, and H.E. Stanley, "Modeling Urban Growth Patterns," *Nature* **377** (1995), 608–612.

[55] J.A. Zettler, T.P. Spira, and C.R. Allen, "Ant-Seed Mutualisms: Can Fire Ants Sour the Relationship?" *Biological Conservation* **101** (2001), 249–253.

Chapter Five

Human Resilience Strategies

We can now apply these theories to human individuals and organizations that experience surprises. We will look at the various levels of an organization or community and what each needs in order to have a good resilience strategy for imminent, short-term, and long-term surprises that present some danger. At the outset, it should be noted that individuals and organizations do not often engage in adaptive behavior as their first response to surprise.

> In their immediate environment such as family, workplace, and leisure activities, people do all they can to build around themselves a cocoon of certainty in the form of repetitive or slightly variable (torus) behaviors. When they are troubled by changing circumstances they make every effort to return to their former regular, reliable ways of functioning. When the organizations they belong to are perturbed by fluctuations, people turn to stricter enforcement of rules, regulations, and norms of behavior.[1]

This is a resistance strategy: trying to keep the danger away by denying that it exists and/or using tight coupling to keep it at bay. It is certainly natural to "wait and see" if the surprise is temporary or has made some fundamental change in the environment that requires the formulation of a resilience strategy that will involve change and adaptation.

Change is more difficult than is sometimes acknowledged in the management fad *du jour* books. Resisting change is not irrational, because many people seem to know instinctively that changing some things in their complex lives or organizations will have unpredictable effects on other things. Anyone who has ever tried to manage organizational or even personal change can attest that this is invariably true and that dealing with surprises caused by the change is very time consuming. This cascading surprise is part of the landscape when attempting to adapt something from the top down. If the adaptation occurs from the bottom up, the surprises are dealt with at the scale where they occur, but there is a good chance that the end product will not look exactly like what the manager had in mind. It may also take more time to allow an organization to adapt from the bottom up—and with surprises that involve imminent physical harm, time is not an available resource. Where these types of situations are likely (e.g., for emergency first responders) the individuals in the organizations charged with managing them must see adaptive and creative response as the "way it is" and not as change at all. The organizations are loosely coupled, and any tightly coupled response is delayed until it becomes clear that it is appropriate to the surprise.

There is growing agreement among many organizational theorists that the best responses to challenges often come from the bottom up and not from the top down.[2] This idea is difficult to

---

[1] Uri Merry, *Coping With Uncertainty* (Westport, Conn., and London: Praeger, 1995), 128.

[2] See, e.g., Peter Schwartz, *Inevitable Surprises: Thinking Ahead in a Time of Turbulence* (New York: Gotham

convey to people at the top of the organization charts in business and government. However, when the consequences of a surprise occur at the individual level, it actually makes more sense for the resilience strategies to come from individuals, since they will have the most incentive to get it right. There is likely to be wide variability in individual resilience based on such factors as experience with similar dangers, perception of the danger, perceived control, sense of community, available resources, and willingness to see the advantages in any surprise.[3] In fact, some research indicates that the centralized and tightly coupled organization of community emergency services may actually be counterproductive when individuals attempt to be resilient.[4]

For governments, this bottom-up approach is absolutely consistent with the idea of democracy and the consent of the governed. The genius of democratic forms of government is that they expand individual freedom (and risk) and allow many things to be tried. Why should we suppose that an authoritarian (or top-down) approach will be the answer to civilian security issues? Even if it is still appropriate for some organizations (e.g., the military) to maintain a top-down and tightly coupled organizational structure to face another top-down, tightly coupled organization (another army), it may also make sense to respond to surprises that occur at the individual level by relying on bottom-up strategies that give individuals the flexibility they need to be resilient.

In the twenty-first century, most Western nations have made a strong commitment to the idea that collective "goods" emerge from the aggregated actions of individuals, not from the omniscient vision of central planners. Adam Smith noted that a collective good such as prosperity requires that individuals be free to pursue their own interests in an open market. To force everyone to act in the same way in a situation where people have different needs and different opportunities is to deny them "liberty" and to hobble the system that they are capable of building.[5] In times of surprise it would be foolish to constrain the ingenuity of each citizen by a tightly coupled response. People will look for the right resilience strategy for themselves, their families, and their neighbors. Governments and NGOs have many ways to help them in this process, but decreeing the right or best thing would not be helpful in most instances.

One of the tradeoffs that open, loosely coupled societies make for their individual adaptability is an increased vulnerability to rogue individuals and groups who do not play by the rules or are intent on the destruction of individuals or institutions. Identifying and dealing with rogues will continue to be one of the critical roles of collective actions taken by governments.

Books, 2003), and John Seely Brown and Paul Duguid, *The Social Life of Information* (Cambridge, Mass.: Harvard University Press, 2000).

[3] Douglas Paton, Leigh Smith, and John Violanti, "Disaster Response: Risk, Vulnerability and Resilience," *Disaster Prevention and Management* **9**, 3, 173–179.

[4] See, e.g., Russell Dynes, "Disaster Reduction: The Importance of Adequate Assumptions About Social Organization," *Sociological Spectrum* **13** (1993), 175–192.

[5] Adam Smith, *An Inquiry Into the Nature and Causes of the Wealth of Nations* (New York: Modern Library, 2000).

The hardest part of this governmental mission is to incapacitate the rogues without destroying the openness of the society that makes the nation successful and resilient.

5.1 What Individuals Need for Resistance and Resilience

Individuals in biological systems who cannot escape a dangerous environment (known dangers) have several strategies for resilience, including having many offspring (greater chances that some will survive) and broad tolerance for many possible changes in the environment. A mobile individual can flee from danger, but must first become aware of the danger in time to flee. Humans practice the “many offspring” strategy in countries with high infant mortality. To cope with other known dangers that involve changes in local conditions, humans build broad tolerance by constructing shelters that allow them to deal with many types of weather or by purchasing insurance.

In the event of Black Swans and New Surprises, such as massive failure of the electrical grid or unimagined new ways to attack civilian populations, resilience is enhanced if individuals have the ability, or the freedom, to flee from the danger and/or to adapt and reorganize their resources. Flight is a resistance strategy for imminent physical danger in that its goal is to avoid an impending injury, but preparations for this resistance make individuals resilient as well, since avoiding injury to themselves will allow them to bounce back faster from damage to their resources .

In situations involving imminent physical danger individuals need information about the danger, flight options (freedom of movement) that will get them away in time to avoid injury, and information about those options (including what others are doing). Thus, if the building is on fire, they need to know there is a fire. They need exits, and they need to know where the exits are and which ones other people are using successfully. If a hurricane is approaching, they need details about the storm (How strong is it? Can I survive by making my house more resistant to the danger?) so they can decide whether or not to flee. Moreover, they need this information about conditions at both local and larger scales. (Is the whole region going to be affected or just one community?) The community needs to have roads that allow people to leave in a short period of time, and individuals need to know about the evacuation routes and whether any are blocked. In the event of a Black Swan or a New Surprise, people need to know if and how they can flee a danger they have never encountered before. (If it is a biological attack by terrorists, can they get away from it by getting out of the city?)

Strategies that enable adaptation or broad tolerance are appropriate for dangers that do not require flight, such as electrical grid failure, or appear over a longer time scale, such as reduced access to cheap oil. For these types of surprises people also need as broad a range of options as possible, and they need to know what those options are if they are to build a resilience strategy. They need information about a potential or current surprise (What caused it? How bad is it? How long will it last?) and about how others are adapting or reorganizing. Again, they need this

information about conditions at both local and larger scales. (Is the whole power grid down or just in one neighborhood?) All this information must be available fast, be as accurate as possible, and be placed in a context that has meaning to the user. People need all this information so that they can choose the best way to bounce back from current or anticipated surprises. **Chapter Six** focuses specifically on information and communication.

If there is a danger that the power grid will fail more often and for longer periods of time—apparently a growing likelihood in the United States and the European Union[6]—citizens need a broad range of options for energy (perhaps including wood stoves and gasoline generators for emergency electrical power, etc.). They need to know what those options are as well as where and how to obtain the resources. They need to know how likely power outages are and how long they might last, and how other people are adapting or shifting their resources in response to the potential loss of power. (Do all the neighbors have generators? How big are their generators? How much does a generator cost?). They need all these pieces of information to decide whether or not to shift part of their resources from some other use to buying a generator. As they ponder their options they need to use creativity to match the level of novelty in the environment. New Surprises will require more creativity.[7]

In many cases people cannot obtain what they need on their own, and must depend on cooperation with others. This cooperation may be organized at many levels, but it works best at the scale where the resources are likely to be. Neighbors would be the best resources for some immediate needs, such as a flashlight battery or help in digging a car out of a snowdrift. Local government can enforce building codes to ensure that citizens have several exits from buildings. Regional government agencies would be better placed than local ones to tell citizens about the potential for power outages and how to buy a generator. National government agencies may be the only ones who can tell citizens if the price they pay for heating oil is likely to increase to the point where they would want to investigate other energy options.

In most cases governments would not insist on tight coupling—that all citizens act in the same way—but would allow individuals or groups the freedom to discover options and refine their strategies. Larger groups, including governments and the news media, could then fill a clearinghouse function to distribute information about what succeeds and what does not. In some cases individuals can also learn from "experts," although they are often not very helpful for Black Swans and New Surprises. Besides, experts are usually more concerned with understanding the components of a problem than with seeing the whole. Learning—putting data in an appropriate context—allows individuals to refine their strategies and their tactics. Long-term surprises often

---

[6] See, e.g., Peter Fairley, "The Unruly Power Grid," Spectrum Online, http://www.spectrum.ieee.org; and US-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the US and Canada: Causes and Recommendations* (Washington D.C.: U.S. Department of Energy, April 2004).

[7] See, e.g., Merry, 121–154.

require changes in perceptions of how things work. These changes often emerges spontaneously and attempts to impose them from above will be difficult.

5.2 What a Group Needs for Resilience

There are differences between groups, crowds, mobs, and herds. We will assume for purposes of this discussion that *groups* are collections of individuals who act in concert for some purpose, although they may also be acting individually for other purposes at the same time. Groups may be tightly or loosely coupled, and may have a top-down control structure, a bottom-up structure, or a combination of the two. The main purpose of a group is to perform some function that the individuals who belong to it cannot (or do not wish to) accomplish by themselves. The individuals in groups continue to make individual decisions about their own behavior; even in authoritarian groups they still have free will. To maintain their cooperation they must each have confidence that group efforts are more effective than acting alone. Trust in the effectiveness of the group is thus critical for its continued existence.

A group becomes a *mob* or a *herd* when it comes together in one physical and temporal space and something happens to weld individuals into a tightly coupled One Thing. This One Thing may "panic"—exhibit terror, confusion, or irrational behavior—if the individuals believe they are in danger and are not free to escape it (e.g., from a burning building): in other words, if they feel they have no options. It could also rise with spontaneous applause at a great performance: the group members simultaneously come to one conclusion.[8]

Officials charged with security, who always deal with danger and too seldom receive applause, are often afraid that groups will become mobs and have been known to forbid gatherings of more than a few individuals. They may also fear mob behavior that might be contrary to the planned response to danger. This may be explained by theories that collective panic behavior is often "unregulated competition" and that it emerges in groups when individuals believe they must compete for a scarce resource that affects their immediate survival, such as physical safety or access to food. These incidents can be seen as

> …individualist crowds responding to a situation in which the social order has broken down. Behavior can then become highly selfish and aggressive, not as a result of irrational panic, but of emergent definitions of the situation as one in which the norms of civility no longer apply, and to compete for individual advantage is legitimate.[9]

---

[8] For a review of the work that has been done on crowds, mobs, and herds, see Philip Ball, *Critical Mass: How One Thing Leads to Another* (New York: Farrar, Straus and Giroux, 2004), 118-155.

[9] Norris R. Johnson, "Panic and the Breakdown of Social Order: Popular Myth, Social Theory, and Empirical Evidence," *Sociological Focus* **20**, 3 (1987), 172.

This seems to be a good description of a crowd trying to escape a burning building. People perceive the bottleneck at the exit and decide that escape is a scarce resource for which they must fight. They would be less likely to panic (and more likely to cooperate with each other) if they knew there were other exits and everyone could get out safely.

Some authors have noted that widespread panic is not the usual pattern following a surprise. The observed pattern looks more like "[T]error, accompanied by a moment of stunned reflection, or even anomie, followed by fairly orderly response."[10] Other research indicates that members of the public are usually quite resilient.[11] We have all seen instances where individuals or groups endanger their own lives to save strangers when that was not part of anybody's plan. This altruistic behavior seems to blossom even in the most horrific surprises, such as the attack on the World Trade Center. There was little evidence of mob behavior in New York on September 11; apparently there was no perception that safety was a scarce resource or that the normal rules of civility no longer applied. In fact, New Yorkers were said to be noticeably more civil to each other during the crisis and remained so for months afterward.

As cooperative units, groups can be the most effective resource for individual resilience. In addition, their communication with other groups helps to spread the word about the kinds of cooperative behavior that are effective.[12] Groups that are important for resilience may be temporary and may form just to deal with the current surprise, such as a group of subway riders stuck underground because of a power failure, or they may be continuing groups that adapt their agendas to the surprise, such as a neighborhood social group that pools resources after a bad storm.

Both short-term and long-term groups need several things to enhance their ability to build resilience for their members. They need a mechanism to adapt, for instance, someone who calms the stranded subway riders by pointing out their options and organizes them for the walk back to the surface. The adaptation device could also be a process whereby the group agrees to share a scarce resource (Neighbor A gets the electric generator from eight o'clock to ten o'clock, Neighbor B gets it from ten o'clock to noon, etc.). This adaptation may be temporary or may become a permanent change in how the group functions if the surprise is likely to recur.

---

[10] Lee Clark, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago and London: University of Chicago Press, 1999), 179.

[11] See, e.g., Russell Dynes, "Disaster Reduction: The Importance of Adequate Assumptions About Social Organization," *Sociological Spectrum*, Vol. 13 (1993), 175–192.

[12] Like virtually all aspects of human behavior, there is no clear agreement about why people cooperate with each other—particularly in times of surprise. For some recent ideas, see Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984); Elliot Sober and David Sloan Wilson, *Unto Others: The Evolution and Psychology of Unselfish Behavior* (Cambridge, Mass.: Harvard University Press, 1998); and P.H. Longstaff, *Competition and Cooperation: From Biology to Business*, P-98-4 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=374 (Accessed on November 7, 2005.)

The group also needs information about the surprise it must deal with, particularly about possible harm to individuals and any group resources, and information about the local environment and the resources available to the group and to individuals. Finding this information may be one of the reasons that the group forms, and the information may become one of the group's most important shared assets. The group thus needs a mechanism to gather and share information outside and inside the group. This information can be shared using a communication system that is put together with assets that happen to be available (for example, cell phones or car radios) or special communication plans that the group has set up in advance (for example, meeting at a certain neighbor's house, or using a bulletin board at a school).

Members of longer term groups need a compatible (not necessarily identical) schema, that is, their belief in how things work (Is "God" controlling the situation? Is the best plan likely to come from authority figures?) Shared schemata allow a group of individuals to process information and make plans without irresolvable disagreements about how the plans are likely to unfold. A shared schema about unusual things such as Black Swans does not emerge automatically, even in a group of neighbors who often work together. Thus, they need a mechanism to test for shared awareness of both their individual schema and the data they bring to the problem. In some cases they also need a mechanism to test for synchronization among themselves and with other scales. Are they acting in a way that works with what other groups and umbrella groups are doing? For example, should they turn off most appliances before the power is restored to avoid a power imbalance in the system?

It is sometimes essential to have a mechanism for communication about a threat that dangerous individuals and groups cannot learn and hijack. The communication mechanism must allow access to those who need it but deny access to the enemy. In some situations, this would argue against a central depository, or hub, for information, since enemy access to this information would be devastating. A more distributed information network would be secure if information collected locally is shared only with trusted local nodes and with other nodes only if trust can be established.

Many of the most efficient communication strategies involve networks of individuals and groups. In both biological and human systems that have many interacting individuals (or groups) there are often super-connected individuals who have weak links to many other individuals and groups.[13] They become the hubs that enable the many interactions that keep the system operating. Removing one of these hub species (or people, or firms) means that the system will experience rapid (and often unpredictable) change. Adding a hub to a random network of individuals you are likely to get a "plutocratic" (the rich get richer) configuration where power and scarce resources are drawn to the hub. These networks where super-connected hubs form are often very efficient

[13] For a discussion of this in human systems see Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston: Little, Brown and Company, 2000).

and robust at lower levels because destroying any of the less connected nodes will have little impact on the system. This strength is also their Achilles' heel. Any part of the system (a person or a group) that becomes a super-connected hub will present both an opportunity for efficiency and a danger to resilience, because if it is disabled it can bring down the whole system.[14]

5.3 What a Coalition Needs for Resilience

A *coalition*, also called an intergroup network, is a group of groups that comes together for specific purposes and is not a permanent larger group.[15] It has all the needs identified above for a group, but building systems for these needs becomes more complex.[16] The effectiveness of coalitions in times of surprise can be enhanced by each of the following:

- Boundary-spanning personnel who interact with other organizations as part of their duties or belong to several of the coalition groups;
- Coalition-wide groups or committees;
- Frequent and reciprocal interaction between groups;
- Communication patterns that are characterized by clarity, openness, and breadth, perhaps using joint data banks; and
- No member group fears loss of autonomy as a result of participation in the coalition.[17]

The information needs of coalitions are similar to those of the component groups, but often the critical communication functions noted above will be complicated by incompatible language or technical systems that have evolved within the individual groups.[18] For joint efforts, all the members of the coalition need information about a danger (possible harm to individuals and

---

[14] See, e.g., Duncan Watts, *Small Worlds: The Dynamics of Networks Between Order and Randomness* (Princeton NJ: Princeton University Press, 1999).

[15] Coalition builders include canids (dogs and wolves), lions, hyenas, dolphins, and primates (including humans). Only dolphins and humans form coalitions of coalitions. For more information about coalitions in other biological systems, see, e.g., Esta Ranta, Rita Hannu, and Kai Lindstrom, "Competition versus Cooperation: Success of Individuals Foraging Alone and in Groups," *American Naturalist* **142** (1993), 42–58.

[16] Collaboration between groups is so crucial for response to surprises such as terrorist attacks and natural disasters that the National Science Foundation has funded a study of how insect behavior might give us insights for managing first responders and designing telecommunications and transportation infrastructure that is useful in times of surprise. See, e.g., "Insects, Viruses Could Hold Key for Better Human Teamwork in Disasters," *Medical News Today*, March 1, 2005, [On-line]. URL: http://www.medicalnewstoday.com (Accessed on November 8, 2005.)

[17] See, e.g., Dennis S. Mileti and John H. Sorenson, "Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events," *Columbia Journal of World Business* (Spring 1987), 13–18.

[18] Overcoming these communication barriers has been the subject of much effort for military coalitions. See, e.g., Anthony W. Faughn, *Interoperability: Is It Achievable?*, P-02-6 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=555 (Accessed on November 7, 2005.)

groups), a way to communicate about the danger with individuals (that the dangerous people cannot learn and hijack), information about environment and resources available to groups and to individuals, and trusted information to confirm the belief that coalition efforts are more effective than operating alone. All of these needs were highlighted in the 9/11 Commission report, particularly the need for radios capable of enabling multiple agencies to respond and communicate local conditions of danger.[19]

Coalitions are sometimes, perhaps often, vulnerable to surprises because of the various scales involved and the difficulty of communicating across those scales. Slow scales in one group do not communicate with fast scales in another. Local scales in one group do not communicate with local scales in another group. Cross-scale interactions can cause surprises, which might take the form of friendly fire casualties or the inability to offer assistance for resistance or resilience strategies. If one coalition partner has experience with a surprise over a longer time scale (for example, dealing with local insurgency in a particular culture), it often cannot communicate that knowledge to lower levels of coalition partners who are dealing with this type of surprise for the first time.

5.4 Resilience Strategies for Deprivation of Resources

Some surprises do not involve imminent physical danger but the gradual or abrupt loss of important resources used by individuals and groups. The response of biological and human systems to uncertain or unpredictable access to resources seems to fall into two groups: diversification and intensification. If there is an unexpected reduction in a necessary resource (a surprise), the initial response is likely to be diversification into smaller, less costly, and more reversible alternatives to that resource. This requires that diverse or redundant sources be available. For example, if oil becomes scarce because of a natural or political surprise, resilience requires oil reserves, because it is not possible to switch cars to another fuel in the short term. If the resource becomes scarce more gradually, people and businesses will find ways to use less oil or to use an alternative, but make adjustments that can be reversed if the price comes back down to expected levels. This “wait and see” response will change to intensification in the use of the alternatives if it becomes widely accepted that the original resource will not become abundant again.

Often the use of alternatives requires a long-term commitment of resources and is unlikely to be easily reversible.[20] If oil remains costly, individuals and organizations will invest more deeply in alternative energy sources or abandon activities that require high energy use. Water is another resource that may become scarce in many places, including the Great Plains in North

---

[19] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary* (Washington D.C.: U.S. Government Printing Office, 2004).

[20] See B.J. McCay, “Systems Ecology, People Ecology, and the Anthropology of Fishing Communities,” *Human Ecology* **6** (1978), 387–422.

America and many parts of Africa. Understanding the possible resilience strategies for these areas will be important for any political response or for economic planning. In cases such as these, where the resource deprivation is gradual, it need not be a surprise and the local populations can be encouraged to adapt by making information about alternatives available. Often these gradual reductions in resources are not perceptible at local scales, and local populations need ways to be in touch with what is happening at much larger (often global) scales to build local resilience. This requires communication between and among scales. Thus, effective communication systems are necessary for any resilience strategy.

Chapter Six

Communication for Resilience to Surprises

How can we design, or redesign, a communication system if we want to build resistance and/or resilience for individuals or groups? The following discussion endeavors to be applicable to all cultures to the extent possible, but readers should keep in mind that every culture and every country have different traditions with regard to communication. They will differ with regard to such factors as the trusted senders of information and access to communication channels. U.S. planners sometimes forget that communication channels developed very differently in the rest of the world, and this gives Americans very different expectations about communication than, say, citizens of a country with a long history of government control and limited access.[1]

6.1 The Importance of Being Accessible, Trusted, and Local

In many animal species, and even among some plants, all individuals use information about opportunities and dangers in the environment. They obtain this information by observing what works for others. If everyone is using trial-and-error tactics to find something that works, this observation reduces the number of failures and increases the number of successes for the group. Some species that live together use deliberate signals about where to find food (for example, the famous bee dance) or about the presence of predators (specific noises made by many species to signal danger).[2]

This information exchange only increases survival chances for individuals if the information is accurate and correctly transmitted. In systems where individuals cannot verify the information before acting on it, this requires that the sender of the information be trusted. False information would send the hive bees in the wrong direction, induce the herd to flee from rich grazing land, or cause the human population to behave in a way that will harm it.

Sometimes public information (i.e., information available to all) is not compatible with individual survival, especially if it concerns a limited resource that cannot satisfy all individuals. In that case individuals may benefit by hiding where they found nectar or not signaling the presence of a lion at the edge of the herd. This zero-sum game (I win if you lose) is not applicable in most cases of surprise in human groups, and working together usually proves to be the best resilience strategy.

---

[1] For a very readable history of U.S. control of communications, see Paul Starr, *The Creation of the Media: Political Origins of Modern Communications* (New York: Basic Books, 2004).

[2] See Etienne Danchin, Luc-Alain Giraldeau, Thomas Valone, and Richard Wagner, “Public Information: From Nosy Neighbors to Cultural Evolution,” *Science* **305** (23 July 2004), 487–491; or any of the ecology texts listed in **Appendix B**.

The necessity of a trusted source for individual and group risk assessment has been well established.[3] Information functions that must be trustworthy include scanning for changes in resources and in trustworthy individuals, and detecting damage, intruders, and dangerous trends.

6.2 Communicating About Known Dangers

Some dangers are not surprises, at least not to most people. Most of us know we can cause serious harm to ourselves if we light a match near a flammable liquid or touch a live wire, but people do both of these things every day and suffer the consequences. Some of them (children, for example) did not know about the danger; others performed a risk/benefit analysis that did not recognize the actual potential or scope of the risk, such as talking on a cell phone while driving.

The typical strategy for communicating about known dangers is education about the dangerous activity, which attempts to stop the damage before it happens—a resistance strategy. We tell people about dangers to themselves or to society at large and assume they will refrain from dangerous activities. However, the impact may be blunted, because we tell them that many things are dangerous. As life becomes more complex many more things can be dangerous, and every nightly news show seems to trumpet some newly discovered danger. A time may come where individuals get “danger fatigue” and no longer listen, even to trusted sources of information.

Most individuals know on some level that things that pose a danger in some situations present an opportunity in other situations. Thus, educational resistance strategies fail in cases where individuals bet that the benefits will outweigh the dangers in their case. They are particularly likely to make this decision if the danger will appear at a different time scale (e.g., smoking cigarettes today can cause lung cancer years from now) or a different population scale (e.g., polluting the ground water near our homes will not hurt us but may hurt many others in ways we cannot predict).

Thus, we are not capable of total resistance even to those dangers that almost everybody knows about. In addition to communication strategies for resistance we need communication strategies for resilience. Both will be primarily local, because known dangers are often local surprises, and the most effective resilience mechanisms are local. For example, at the level of the individual, we might seek resilience by giving people information about buying insurance and seeking emergency medical services.

Interestingly, most resistance strategies also involve local communication. It is necessary to know about the presence of a danger to initiate systems that keep it away. This is true even at the level of the human immune system. Local communication between cells signals local white blood cells to attack a problem such as a local bacterial infection. Local information about the success

---

[3] See, e.g., Paul Slovic, *The Perception of Risk* (London and Sterling, Va.: Earthscan Publications, 2000), 316–326.

of that attack is also critical when higher level mechanisms (such as fever) are brought into the battle.[4]

Most people pay closer attention to those around them than they do to people in faraway places with whom they have no connection. Most of us also pay closer attention to the opinions of our family and neighbors than we do to information from more distant sources such as news media or government officials. Communication about dangers that comes from a larger scale is more likely to be ignored as not relevant to the individual's special circumstances. Many of us stopped smoking not because we finally became convinced it was dangerous, but because the people around us were stopping. We are more likely to examine our homes for fire hazards if a neighbor's house catches fire. Successful strategies for both resistance and resilience are therefore likely to involve local communication and to rely heavily on reports about what is working for people near us rather than on messages about what a distant government assures us is the right thing to do.

The importance of timely and accurate local information became tragically apparent in the evacuation of the World Trade Center towers. One government report concludes that more people would have survived in the second tower if they had known that the first tower had collapsed.[5] It was also evident in the use of cell phones by those trapped in the London Underground rail system after the bomb attacks in 2005. Most people called their friends and relatives to find out what happened and to let them know what was happening to them. In both cases there was no government source for the critical local information and no place for individuals to give information to government.

6.3 Communicating About Known Unknowns and Black Swans

Some known dangers do not involve individuals engaging in dangerous behaviors, but are surprises from another scale. We can predict that these surprises will happen, because they have happened in the past. We do not know where, when, or how hard the next dangerous storm will strike, but we know there will be a next one. We do not know when there will be a terrorist attack or what form it may take. Communications strategies for these types of surprises are complicated, because they must be executed at the right scale (organizational, geographic, temporal, etc.) to be effective.

It would be very expensive for all local communities to have resistance or resilience plans for all the possible types of multiscale, and possibly catastrophic, events that they know might happen. These risks are often aggregated by larger scales of government. The responsibility for

---

[4] Lee A. Segel, "Diffuse Feedback From a Diffuse Information Network: in the Immune System and Other Distributed Autonomous Systems," in *Design Principles for Immune System and Other Distributed Autonomous Systems*, L.A. Segel and I.R. Cohen, eds. (New York: Oxford University Press, 2001).

[5] The NIST report is available on-line at URL: http://wtc.nist.gov (Accessed on November 8, 2005.)

bringing in resources that will allow the local population to bounce back is often taken by state or national agencies. The higher the cost of that help, and the more often it is needed, the more likely it is that the higher level government will insist on some local-level risk management in the form of resistance (e.g., not building in flood-prone areas) or resilience (insurance) planning. If higher scales of government are not able or willing to take this responsibility, local communities are forced to make a cost/benefit analysis to determine how much of their resources they want to invest in resistance or resilience strategies. Two of the most important considerations in this decision will be the amount of resources available locally and the local perception of the risk. Since these two things will not be the same in every community, it is unlikely that one global strategy will be maximally effective or be welcomed in all communities.[6]

One of the tradeoffs in local resistance and resilience communication about UNKs and Black Swans is that multiple strategies are not as efficient (cost-effective) as standard, globally imposed ones. Communication is also less likely to be able to take full advantage of nationally coordinated procedures. Local resources for communication vary widely. For example, many communities that are prone to weather surprises have established active communication systems that distribute information about local conditions regarding such topics as evacuation routes and available shelters. In other communities, emergency communication systems may have atrophied from lack of use or become dysfunctional, because local changes in technology or personnel mean that several systems that need to talk to each other no longer can do so.

Unique local variables may also come into play in a decision to communicate about any particular possible surprise. For example, consider a case where national intelligence officials become aware that persons with known ties to terrorist organizations have recently frequented a very popular local casino and there are some vague indications that these people were assessing the value of the casino as a target. Any public alert about the activities of these persons could have ruinous implications for the casino if people chose to stay away, believing it would be dangerous to be there. The decision about how to alert the public would be difficult, to say the least, and the person making it would want to know about both the local populations and the nature of the evidence gathered by the national authorities.

It is thus critical that any local strategies have the ability to access information about the UNK or Black Swan at all appropriate scales, from other places, other times, other groups, and other individuals. Will some larger force that we cannot see locally cause this surprise? What kind of help can be expected from higher levels? What are other groups doing?

---

[6] See, e.g., Claire B. Rubin and Martin D. Saperstein, *Community Recovery From Major Natural Disaster* (Boulder, Colo.: Program on Environment and Behavior, Institute of Behavioral Science, University of Colorado, 1985). One of the most fully developed programs for communicating risk has been developed in the UK. It is available on-line at http://www.ukresilience.info/risk (Accessed on November 8, 2005.)

6.4 Communication About Communication

When a surprise is known but its location, timing, and severity cannot be predicted, advance communication can help build resilience if it informs people about specific resilience strategies for specific surprises (for example, go to interior hallways in case of high winds), particularly if it shows how the strategy has worked for people in the past. This type of information is probably less effective for what many will perceive as Black Swans. Understandably, officials would want to send as much information as they can in advance to help people prepare, but information that is not immediately useful will be ineffective unless there is an easy way for people to store it for future use. Pamphlets are not very useful if we cannot find them when you need them, and only a very small minority of Americans will probably take the time learn specific responses to the many potential types of terrorist attacks.[7]

Therefore, any communication strategy about possible surprises should always include instructions on how to get more information, e.g., what channel on the radio to turn to, or which local schools or other institutions will act as points of information collection and dissemination. No matter how many times people have experienced a hurricane, they will always need to know what is happening now because each one will be different. People experiencing their first hurricane will not remember what they heard on a newscast or read in a government pamphlet several years ago. The most useful information will include where to find out what is happening, if they are in immediate danger, and if the electrical system is likely to fail. Radios powered by electricity are not helpful during a power outage, and even those with batteries will be useless when the batteries wear down. Pre-surprise information should thus place special emphasis on how people could prepare to communicate (both as senders and receivers of information) in case of extended telephone and/or power outages. This is likely to be far more useful than specific suggestions such as recommending that people keep a spare toothbrush and toothpaste at work.[8]

6.5 Communication After a Surprise

After a surprise has occurred or is clearly imminent (for example, when the hurricane is about to make landfall) the appropriate communication strategy differs from the one that was effective when the surprise was only possible. In many ways communicating after a surprise is easier than communicating about potential surprises, because there is no longer any doubt about when and if the event will occur. Thus, it is not necessary to convince people they need to pay attention; people will be actively seeking certain kinds of information. How big is the affected area or population? How bad are conditions in individual areas or populations? What are

---

[7] But if they choose to become modestly informed, they can get small cards with instructions in case of chemical, radiological, nuclear, and biological attack on-line at http://www.rand.org (Accessed on November 8, 2005.)

[8] This is one of the suggestions made by the *Wall Street Journal* in 2004 after an alert for potential attacks on financial institutions. The newspaper also mentioned that the government urges a communications plan that includes out-of-state contact with family. “Preparing for the Terror Alert,” *Wall Street Journal*, August 3, 2004, D1.

individuals or groups doing to cope? The first two questions must be answered by people whose field of vision is larger than local; the third question can only be answered by people who can observe what is happening locally.

As noted previously, resilience requires that individuals and groups have information from all appropriate scales, but in times of imminent physical danger the emphasis necessarily shifts powerfully to the local. People need to know how they can stay alive or keep from being hurt. The best mechanism is a trusted information source that can tell individuals what is proving effective for others in a similar situation. Top-down communication systems do not meet this need. Too often the flow of information to and about other individuals and groups is lost or delayed in the trip up the chain of command. Timing is often critical and information must be passed on to the level where people have been hurt or are in danger and must go into resistance or resilience mode.

For example, if it becomes clear that a ship will sink the captain will turn over resilience to individuals and order the abandonment of the ship. This is most effective when all the people on board have some resilience tools, such as life jackets and rafts, that they have been trained to use. It may mean the difference between life and death if they can communicate with their shipmates in the water to learn what sorts of dangers they face, such as sharks, and which strategies are helping to keep them alive. They also want to communicate their position to summon help. In this case they want to know if all ships in their area were sunk or damaged, which would make it more likely that they would have to wait for help from farther away.

In the case of a local surprise, such as a terrorist attack, individuals and households must be able to scan their local environment as soon as possible. If people are injured they need to know how to reach help; if they are unhurt, they need to know if they are in immediate danger and should move away or take cover. The most important information they need concerns what is working for other local people, not just what they are doing. Where are they getting help? Are they moving to a safe place?

A “follow your neighbors” strategy is not always best, particularly if the neighbors have panicked. The best way to avoid panic is to demonstrate that other people have not panicked and that they are pursing effective strategies. This was certainly true on September 11 and has also been seen in cases of major failures in electrical service. Assurances from government that everything is under control are not likely to be widely credited unless they are supported by evidence from local people. In fact, a recent study of public attitudes toward government instructions for responding to a smallpox outbreak or a “dirty bomb” indicated that only two-fifths of the American public would go to a vaccination site and only three-fifths would go to a shelter. Many people, particularly minority groups and recent immigrants, would not trust

government information, but would be more likely to be vaccinated or go to a shelter if they could communicate with their families and their own health care providers.[9]

One of the most famous surprises of the twentieth century was the discharge of radioactive material from the Three Mile Island nuclear power plant in Pennsylvania. This incident demonstrated that information about what is happening is needed on all scales (federal, state, local), but most critically at the local scale, where the information is most relevant and where there is more likely to be a trusted source of information. Richard Thornburgh, governor of Pennsylvania at the time of the incident, has described how, even from the governor's office, he could not get information he could trust from the electric utility that ran the plant, the federal inspectors, or the "experts" in the field. The people living near the plant had virtually no information they could trust. The results were an ill-advised evacuation and near panic. According to Thornburgh, the biggest lesson from Three Mile Island was "expect the unexpected." He also stated that in such situations a "trusted adhocracy" is often more valuable than an entrenched bureaucracy.[10]

6.6 Trusted Communication: the Critical Resource

A trusted source of information is the most important resilience asset that any individual or group can have in times of surprise. Trusted information is critical for rational risk assessment and the evaluation of options. These trusted sources must be maintained even during stable periods because in times of surprise you do not have time to check out new sources.

These sources are often likely to be local sources that can deal with local variability, because what is trustworthy for one person or community may not be for another. These sources must also be people and institutions who have reliable scanning capabilities to determine what is really happening and who have no interest in misleading anyone. In many cases the only sources—which are not always trusted—are local media and/or government speaking through local media. For the big picture, we often rely on organizations with national (and multinational) scanning capabilities: national media and national government. If we are to trust them in times of surprise, it is essential that we trust them at all other times.

Unfortunately, large organizations—or whole countries—facing a surprise sometimes look exclusively at the big picture. This leads them to resist giving individuals the freedom to choose their own resilience strategies. They assume there is always safety in numbers and everyone will

---

[9] Roz D. Lasker, *Redefining Readiness: Terrorism Planning Through the Eyes of the Public* (New York: Center for the Advancement of Collaborative Strategies in Health and The New York Academy of Medicine, September 2004).

[10] Richard L. Thornburgh, "Three Mile Island: A Case Study in C3I for Crisis Management," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1988*, I-89-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=300 (Accessed on November 7, 2005.)

be safer if a strategy is devised by somebody who sees the whole picture. They also assume that individuals will be safer if they are led from above.

Two authors have examined at these assumptions about top-down communication in times of surprise. Both indicate that top-down communication can sometimes reduce resilience, despite the very best of intentions. *The Wisdom of Crowds*, by James Surowiecki,[11] and *The Great Influenza: The Epic Story of the Deadliest Plague in History*, by John M. Barry,[12] both build a strong case against a resistance or resilience communication strategy that functions primarily from the top down. They believe that both global and local knowledge in the system must be distributed at all levels and that one informs the other. The highest levels of a communication system thus perform a coordination function and, while this level may turn data into knowledge and distribute it back down, knowledge can also be developed by using data from other levels and other groups and then moving the data up and out.

Otherwise, the two authors paint a very different picture. Surowiecki describes the research on decision making under uncertainty and points out that collective decisions that emerge from groups are often better than those dictated from above, even when all the members of the group have imperfect information. Interestingly, Surowiecki finds that crowds can be "wise" if they have diversity (many different individuals working on the same thing in their own way), independence (freedom to work on the problem in their own way), and a particular kind of decentralization that allows private decisions to be turned into collective ones. This describes two of the criteria considered key to resilience (see Chapter Four). Surowiecki does not deny that crowds may engage in herd behavior or may panic, but argues that this occurs only when the crowd—whether football fans or stock market investors—does not perceive that it has independence, in the form of options to move away from danger.

Barry's history of the horrific worldwide influenza epidemic of 1918 is a cautionary tale with direct relevance to the possible surprises of the twenty-first century. The tragedy was compounded by a failure to understand what was necessary for resilience. Governments lied to the public and the press about the extent of the epidemic in order not to undermine wartime morale and prevent "panic." Many in positions of leadership assumed that the virus and its transmission were predictable and would not change, but the virus mutated, which made very specific and top-down strategies useless. These leaders also failed to collect and disseminate the knowledge generated at the local level; nurses and local doctors could see what treatments were effective but could not communicate their observations. All of this meant that people got their information via rumors and, if they believed the government, did not take steps that would have made them more resilient and, perhaps, more resistant. It is clear that people needed to know

---

[11] James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (New York: Doubleday, 2004).

[12] John M. Barry, *The Great Influenza: The Epic Story of the Deadliest Plague in History* (New York: Penguin, 2004).

what was happening. They needed the freedom to ask specific questions without fear of being labeled unpatriotic, because generalized information was not always appropriate for their specific situation. This information would have allowed them to decide if they should move from danger or shift resources to build resistance and/or resilience strategies. What they did *not* need was isolation, because this led to fear.

> In virtually every home, someone was ill. People were already avoiding each other, turning their heads away if they had to talk, isolating themselves. The telephone company increased the isolation: with eighteen hundred telephone company employees out, the phone company allowed only emergency calls; operators listened to calls randomly and cut off service to those who made routine calls. And the isolation increased the fear. Clifford Adams recalled, "They stopped people from communicating, from going to churches, closed schools, ….closed all saloons….Everything was quiet."[13]

Barry points out that people who found themselves "in charge" in a time of surprise have "often sought security in imposing order, which gave them some feeling of control, some feeling that the world still made sense."[14] But individuals confronted with surprise do not need a false sense of order. In the short term, bringing everything into tight coupling and rigid control may make someone feel more in control, but, as noted above, this can actually make the system more brittle and likely to shatter.[15] Scapegoats are also tempting (one local official blamed the influenza on "foreign settlements" in his city—mostly Italians) because they divert attention and emotional energy from actual events to avoid blame. Succumbing to either of these temptations destroys the best resilience asset a government can give its people: a trusted source of information about what is actually occurring so that citizens can make decisions about their own strategies.

Governments have long tended to take control of communication in times of surprise. In the United States this has taken the form of seizing physical possession of the telecommunications networks in wartime and leaning heavily on media to send only approved messages.[16] This has the effect of reducing trust in both the media and the government, and it is certainly inimical to the resilience of local populations, who then have no trusted source of information about events outside their local range of vision. Sometimes, of course, government officials must give out some information before all the facts are in. This may be particularly true in cases of bioterrorism where, for example, the number of people infected and the infectious agent are not immediately

---

[13] Ibid., 328.

[14] Ibid., 395.

[15] This is consistent with Snook's findings about military organizations. See Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton, N.J.: Princeton University Press, 2000).

[16] See Paul Starr, *The Creation of the Media: Political Origins of Modern Communications* (New York: Basic Books, 2004), 395–402.

knowable. This may require a balancing of the twin goals of fast information and accurate information.[17] A recent report on communication and bioterrorism concludes:

> Resourceful, adaptive behavior is the rule rather than the exception in communities beset by technological and natural disasters as well as epidemics….
>
> In short, evidence that the public cannot be trusted with full, accurate disclosure of what is known about a bioterrorist attack is lacking. The events of 11 September 2001 and after further undermine the view that the public is prone to panic, incapable of effective participation and inclined to respond irrationally.[18]

This report goes on to recommend that plans for trusted communication in times of surprise should probably include all of the following:

- Treat the public as a capable ally in the response to the surprise
- Enlist civic organizations in activities
- Invest in public outreach
- Make sure that activities and plans reflect the values and priorities of local populations.[19]

This is not to say that there is no information that should be kept from all citizens. The balancing that must take place has sometimes been almost unimaginably hard. Who would want to decide if the residents of a city should be told in advance about an impending attack that will kill many of them if that information would reveal intelligence sources that may save millions? Careful balancing, as opposed to information stoppage as the standard operating procedure (SOP), may be the only way to retain the long-term trust of local individuals and groups.

Since the middle of the twentieth century the mass media in the United States have endeavored to serve as an alternative source of trusted information. This has not always been pleasant for government, and the media have not lacked their own biases, but media reports that are independently developed allow citizens to obtain information when the government cannot give it to them.

---

[17] The Working Group on Governance Dilemmas in Bioterrorism Response, "Leading During Bioattacks and Epidemics With the Public's Trust and Help," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* **2**, 1 (2004), 35.

[18] Thomas A. Glass and Monica Schoch-Spana, "Bioterrorism and the People: How to Vaccinate a City Against Panic," *Clinical Infectious Diseases* **34** (2002), 222.

[19] Working Group on Governance Dilemmas in Bioterrorism Response, 217.

6.7 Communicating About the Past—When Experience Counts

Both global and local strategies need memory across temporal scales. When trying to find what resilience strategy will work best, it is often helpful to know what has worked before. This may not be the best answer for today because critical variables may have changed, but lessons ignored are lessons that must be repeated. Unfortunately, there may be little time to find somebody who was alive the last time this type of surprise happened. Most readers of *The Great Influenza* do not remember that tragic time and do not know the hard lessons learned then. This seems to indicate that, when planning a resistance or resilience communications strategy, some sort of connection to the "slow" scale (where lessons are remembered) should be available at a moment's notice. Both governments and media may want to consult historical resources, both human and archival, that go back further than the memories of the current staff.

6.8 The Communications Media as a Resilience Tool

The media—print, broadcast, telephone, cable, satellite—play a critical role in times of surprise and in communication about potential surprises. In times of surprise, all people and all groups have a critical need for information that will help them reduce uncertainty and implement appropriate resistance or resilience strategies. They need trusted information for risk assessment, damage assessment, and options. They may also need new heuristics or schemata about effective approaches that will help them convert any residual uncertainty into risks they can manage.

Critics of the media seldom acknowledge the enormous task the media face in times of uncertainty and surprise. Because "the media" are often perceived as a monolithic institution, and because they are often very visible, they become additional victims of the Blame Game after a surprise.

People have always placed great confidence in the power of mass media (one message sent to many people) to influence the opinions and actions of those who use them.[20] Some evidence indicates that this confidence is shared by modern terrorists, who use the media as an ancillary weapon.[21] Other evidence indicates that this confidence is misplaced. Paul Starr has examined the evidence for media influence on public opinion and found it mixed:

> More than 2,000 years ago, Archimedes is supposed to have said, "Give me a lever long enough and a place to stand, and I will move the world." Many people hoping to move the world have thought that the media offered them a lever long enough and a place to stand – the place being in front of a microphone, camera, or computer screen. Mostly this is a

[20] For a collection of research on media effects, see, e.g., *Media Effects: Advances in Theory and Research,* 2nd ed., Jennings Bryant and Dolf Zillmann, eds. (Mahwah, N.J.: Lawrence Erlbaum Associates, 2002).

[21] See, e.g., Joan Deppa, Maria Russell, Dona Hayes, and Elizabeth Lynne Flocke, *The Media and Disasters: Pan Am 103* (New York: New York University Press, 1994), 323.

> delusion, as so many people are pushing in different directions. But the media certainly are mighty levers, and where our world moves in the future will depend on critical choices about them we have yet to make.[22]

Those choices about the missions of the media should take into account their critical role as communication coordinators and facilitators in times of surprise. Because information is such a major part of what individuals need before, during, and after a surprise, all of a country's communication assets are often necessary to get the job done. While many media outlets at the national level see their most important job in times of surprise as providing "oversight" of the actions of governments and corporations—clearly an important role—they sometimes forget about their ability to help individuals and groups by telling them what they need to know for resilience.

At a May 2002 meeting cosponsored by the Brookings Institution and the Shorenstein Center at Harvard University, journalists and government officials were asked about the media's role in the war on terrorism. Lee Hamilton, former chair of the House of Representatives Committee on Foreign Affairs, had this advice:

> What I detect among people is [that] they want to know what they should do in their personal lives….So one of the things the media has to do, and one of the things the government has do, is to try to help people, ordinary people, living ordinary lives, get through this crisis and tell them what they do with their lives. That's what's meaningful to them. And I don't think either government or the media is going a good job of that, although I think generally the media has done pretty good job of explaining the war on terrorism.[23]

Many small communities and many ethnic communities within larger ones have no broadcast or other communication service to which they can turn for local news in times of surprise. It is simply not economically feasible to maintain them. Even in communities that do have local media, competitive pressures to reduce costs may lead to efficiencies that reduce capacity to maintain redundant energy sources or information-gathering personnel who can be mobilized in short order. Government initiatives to increase competition have often failed to take this predictable side-effect of increased competition into account. As local outlets become more efficient to meet competitive pressures, they also become less resilient as businesses and as community resources in times of surprise. To the extent that increased competition results in fewer local media firms (local concentration is also predictable but seldom acknowledged[24]), it

---

[22] Starr, 402.

[23] Stephen Hess and Marvin Kalb, eds., *The Media and the War on Terrorism* (Washington, D.C.: Brookings Institution Press, 2003), 268.

[24] See P.H. Longstaff, *Competition and Cooperation: From Biology to Business,* P-98-4 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL:

reduces diversity in local messages. As noted previously, a lack of diversity can lower the resilience of local individuals and groups, because they may have fewer opportunities to review strategy options and see what is working for others. Any adaptations made by communications companies, including telephone companies, to respond to competitive pressures by reducing this local capability for providing information or communication services in times of surprise must be addressed, probably as a market failure that requires government intervention.

If there are no local media or not many of them, local communities need to build a resilience strategy that draws on other institutions that can assume roles in gathering and delivering trusted information about what is happening and can serve as a clearinghouse for information about what people are doing to be resilient. These resources might be schools or local service organizations. Government could take a leading role in helping to facilitate this local resilience planning, but the plan should come from the individual community where local needs and resources can be taken into account.

Local communication systems need to be both point-to-multipoint (one message to many: for example, radio or a bulletin board in a school) and point-to-point (one message from one person to another). This second type of communication allows people to talk to their families or other trusted people who are not available in their neighborhood. This type of "networked" communication has proven very effective in moving information, particularly if local "hub" individuals are part of the network and play the role of a clearinghouse for information.[25] It has been shown conclusively that people trust messages from other people more than they trust information from institutions. One of the most important studies in communications and public opinion concludes that, "In the last analysis, more than anything else people can move other people."[26] This means that propaganda will have only a limited effect if it is not consistent with what is happening locally or if local people can obtain information from other places.

The local and national communications media can also serve as an information source for national defense and intelligence agencies. They are part of what is known in intelligence circles as open source intelligence (OSINT), and their information-gathering activities are often used to validate other intelligence sources and to detect emerging trends.[27] Their value for defense and for tasks such as consumer and political analysis depends on their ability to collect data at the local level, that is, the level where the actions of individuals acting alone or in small groups can be detected. The failure to perform this function has implications not only for local individual

---

http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=374 (Accessed on November 7, 2005.)

[25] See, e.g., Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (New York and London: W.W. Norton & Co., 2003).

[26] Paul F. Lazarsfeld, Bernard Berelson, and Hazel Gaudet, *The People's Choice: How the Voter Makes Up His Mind in a Presidential Campaign* (New York: Duell, Sloan and Pearce, 1944), 158.

[27] See, e.g., Elizabeth Goldschmidt, "Open Source Intelligence: Sources, Methods, and Questions," presentation at Harvard University, May 7, 2004.

resilience but also for resilience planning at higher levels. Sometimes media coverage of an event is the only information available to policy makers. In one case, CNN was the only immediate source for information about a hijacking in Pakistan.[28]

Western media have become one of the trusted sources of information, not because they are smarter or better detectors of information but because there are many of them. If many people look at the same situation they will generate many views, and in that diversity people are more likely to find the information they need. If they compete on the basis of accuracy and fairness, then these traits are more likely to be selected as each firm and each medium evolves. Their diversity also gives them resilience in the face of surprise. If one company's equipment fails, the presence of other organizations builds in redundancy. Monopoly communications enterprises controlled by their governments may offer those governments better control of the "news" in the short term, but those monopoly enterprises are less likely to evolve into reliable information sources.

One of the greatest problems for competitive media is motivating readers and viewers to pay attention to what is happening at slower time scales. This includes news about potential surprises that evolve on a slower time scale than a twenty-four-hour news cycle. Bob Schieffer of CBS News has noted that before September 11 it was difficult to attract anyone's attention with news about possible terrorism in the United States, and when he built a whole *Face the Nation* show around the topic the program got the lowest ratings in its history. "[T]errorism until September 11 was so beyond all of our imaginations that you had a really hard time getting people interested in it."[29]

While there is always room for improvement, the U.S. news media and those of most developed countries succeed in bringing people and their governments important information for resilience. They often perform heroic work in detecting damage that affects or may affect their readers, listeners, and viewers. They save many lives every year by providing accurate information about the options that people have for evacuation and local resources for shelter, food, et cetera. But if the media are to play a more important role in resilience planning and implementation, they, like government, should consider some improvements.

1. Media organizations are often incapable of scanning for changes and detecting dangerous trends, but try to perform this function by interviewing "experts." Unfortunately, many potential or current surprises are very complex and require a variety of experts in order to explain them. It is tempting to spend more time with someone who has an easy answer that can be conveyed in a ten-second sound bite. Many news people believe that this is what their viewers or readers want. Perhaps it is, but this may be a chicken-and-egg problem. If we expect people to want simple answers, then that is what they seem to want,

[28] Michael Bohn, *Nerve Center: Inside the White House Situation Room* (Washington, D.C.: Brassey's Inc., 2003), 58.

[29] Hess and Kalb, 117.

but if we expect them to be able to handle more complex ideas, they may do what is expected and take the time to try to understand. If we cannot find a way to convey complex ideas and the inherent unpredictability of our complex systems, the future of democracy is in doubt and a new age of demagogues with simple (but wrong) answers is more than merely possible.

2. All media can take much more seriously their role in helping citizens interpret and criticize the security planning exercises that Lee Clark calls "Fantasy Documents."[30] These are supposed to assure us that every possible contingency has been anticipated and that we are capable of resisting danger or making everything go back to normal. They should be debated much more seriously and their limitations made explicit. The media should never give the public a false sense of security, because this will undermine their role as a trusted source of information.

3. The media can help people stay in touch with the slow scale. This includes bringing the public information about evolving situations that may present surprises. After a surprise has happened, it is important to provide information about similar surprises from history to give individuals and groups some ideas about their options for responding. This may not fit the standard definition of "news," but it will speed up the development of resilience.

4. In all reporting on surprises, the media must stop participating in the Blame Game until the crisis is over. Ill-timed debates about who is at fault divert critical time and energy from finding the information that individuals need to become resilient. The Blame Game may also make it less likely that the people involved will actually save and share important information about what actually happened. A national debate on the nature of responsibility (including response ability) in times of surprise is absolutely critical to prevent internal self-destruction. The media can be crucial in realigning expectations about managing complex, uncertain systems.

5. All media outlets at all levels, national to neighborhood, must improve their ability to explain risk assessment. They must rethink how they present complex technical information such as medical research, not only to improve clarity but also to eliminate any distorting "framing" of the information. This should include limitations in the research: any potential bias, assumptions that may not apply in all cases, and, perhaps most important, the context of any statistical analysis. Headlines should never say "Doing X will increase your chances of dying by Y percent."[31] The media should instead explore questions such as: What do probability statistics actually mean for individuals and groups?[32] What are the chances of an individual's being involved in any sort of terrorist attack in the United States? How should individuals look at this risk assessment?

6. Like other communicators who must send messages in times of uncertainty or surprise, the media must take into account the limitations on people's understanding of risks. They

---

[30] Lee Clark, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago and London: University of Chicago Press, 1999).

[31] Your chances of dying are 100 percent and nothing you do will change that.

[32] For a start, see the checklists offered by Paul Slovic, *The Perception of Risk* (London and Sterling, Va.: Earthscan Publications, 2000), 193–194.

should never reinforce people's perception that they are at greater risk of something bad happening just because it happened recently or got a large amount of media coverage.[33] They should be especially careful with the first reports of a surprise, because those reports tend to set initial perceptions. These will be difficult to modify because individuals will dismiss contrary reports as unreliable, erroneous, or unrepresentative.[34]

7. While media organizations generally do a good job of showing how individuals and groups are coping with a surprise, they sometimes neglect to show what is not working. This is just as important as showing success, and should never be perceived as placing blame on those who have tried and failed.

8. Media often play a critical role in helping people identify new sources of trusted information in situations such as Black Swans and New Surprises. Media organizations must have some way to identify and evaluate these new sources, even if it means sending viewers to another channel or another medium.

9. Communication about surprises should never assume that people are incapable of understanding the situation. When possible, the information should always include the options available to individuals and groups. The communicator should never assume that people will become mobs. If the media receive information from government agencies that makes these assumptions about mobs or herd behavior, they should make sure that they do not repeat the error in their own communication, and they should demand information about options.

10. Because they are a critical resource, media organizations must evaluate their own systems to make sure they are resilient. Can they bounce back if they lose electric power or the ability to transmit their messages? Do they need redundancy? Does the community need a diversity of trusted sources? If individual media organizations cannot afford to build a communication system that will build local resilience in times of surprise, then the best answer may be for them to cooperate. This will be difficult in very competitive situations, but we have often seen media outlets come together and put aside competition in times of natural disaster or national emergencies. It may be better for each community to examine some of these topics in advance.

[33] Ibid., 184–191.

[34] Ibid., 185.

Chapter Seven

Intelligence and Defense Agencies as Resilience (and Resilient) Assets

[T]he fog that surrounds the outcomes of war has always tempted people to spin theories about what lies on the other side. Yet the reality is always a surprise.

War: Ends and Means[1]

Almost every military strategist encounters the fog of war. There are dangerous things that we cannot see and cannot predict. Detailed battle planning has usually meant constructing a set of possible scenarios, collecting more data, and refining analysis, but the military increasingly accepts the role of uncertainty and how it can become a strategic weapon.[2] A paper submitted for the U.S. Navy's 2002 Colbert Prize suggests a transformation in the military paradigm that accepts uncertainty and takes advantage of resilience planning:

> The existence of frictional, intrinsic, and dynamic uncertainties suggests that the old paradigm is incomplete. First, coping with uncertainty requires *the deliberate creation of resilience* to manage the effects of inputs and interaction on the system. Chaos, adaptive complexity, and nonlinearity suggest that instability and fragility in the system can lead to unpredictable, disproportionate, and dysfunctional outcomes. Coping in advance with uncertainty requires creating conditions necessary for *resilience* in the system. Second, it demands the need for versatility and flexibility to respond to crisis and opportunities in a manner that derives maximum advantage from the situation. Last, it argues for the development of an approach to war that focuses on the creation and exploitation of uncertainty in the enemy.[3] (Emphasis added)

The very idea of accepting uncertainty conflicts with accepted assumptions such as the utility of the precision application force that is part of Air Force basic doctrine. These assumptions "suffer from important conceptual weaknesses that are amplified when examined from the perspective of nonlinear and complex systems."[4] Extensive planning in a resistance

---

[1] Paul Seabury and Angelo Codevilla, *War: Ends and Means* (New York: Basic Books, 1990), 76.

[2] See, e.g., David Alberts and Thomas Czerwinski, eds., *Complexity, Global Politics, and National Security* (Washington D.C.: Department of Defense, CCRP Publication Series, 1997). This book also has an excellent bibliography on complexity and chaos.

[3] Christopher D. Kolenda, "Transforming How We Fight: A Conceptual Approach," submitted for the Admiral Richard G. Colbert Memorial Prize, U.S. Naval War College, Newport, R.I., (May 16, 2002), 11.

[4] Timothy J. Sakulich, *Precision Engagement at the Strategic level of War: Guiding Promise or Wishful Thinking*, Occasional Paper No. 25 (Maxwell AFB, Ala.: USAF Center for Strategy and Technology, Air University, 2001).

mode (stopping all possible bad things) can lead to rigid and inflexible operations with less than optimum outcomes.

> Intellectual flexibility is needed in order to avoid a dogged, single-minded pursuit of an effect that is no longer important or even obtainable in an evolutionary system of strategic interactions…..Flexibility requires error tolerance and avoidance of over-control.[5]

Changing beliefs about the predictability of outcomes may be the military's greatest organizational and political challenge. It is not a matter of exchanging one paradigm for another; it is a matter of acknowledging the limitations of our ability to resist certain types of surprises and of building additional competence for bouncing back. The stereotype of the Western military organization that is tightly coupled and inflexible has never reflected the real situation. Armies of the West have been called the deadliest in the world because they generally have better technology, better organization, higher morale, and better discipline while at the same time encouraging initiative and flexibility. This is said to stem from the Western traditions of freedom, civic militarism, civilian audit, and dissent, which started with the Greeks.[6] These traditions of oversight and dissent do not always make warfare easy, but they do force commanders and politicians to acknowledge and learn from surprises. This, in turn, makes everyone better able to bounce back from similar surprises unless they get caught up in the Blame Game.

The mission of resisting surprise by predicting it before it happens will always be an important part of what governments ask their intelligence agencies and the military to do. It is always better to prevent an attack than to bounce back from it. New technical and human systems for resistance activities, such as data gathering and surveillance, can help lift the fog of war to some extent. Improved information for resistance strategies can, and will, save lives. As unpopular as it might be politically, perhaps it is time to admit that we cannot stop every conceivable attack in an era of asymmetric and/or network-centric warfare.[7] Many Black Swans and New Surprises may occur, and no conceivable amount of data and no higher level of analysis will make them predictable.

The concepts developed in this report can be useful in refining both offensive and defensive strategies for fighting in unpredictable environments. Indeed, any strategy has elements of both

---

[5] Ibid., 38.

[6] Victor Davis Hanson, *Carnage and Culture: Landmark Battles in the Rise of Western Power* (New York: Anchor Books, 2001).

[7] See, e.g., David Alberts, John Garstka, and Frederick Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: Department of Defense CCRP Publication Series, 1998), and Stuart Johnson, Martin Libicki, and Gregory Treverton, *New Challenges, New Tools for Defense Decisionmaking* (Santa Monica, Calif.: The RAND Corporation, 2003.

offense and defense. Anyone who has played or watched sports will recognize the truth of the following section from the U.S. Marine manual *Warfighting*

> While opposing forms, the offense and the defense are not mutually exclusive. In fact, they cannot exist separately. For example, the defense cannot be purely passive resistance. An effective defense must assume an offensive character, striking at the enemy at the moment of his greatest vulnerability.… The truly decisive element of the defense is the counterattack…. Similarly, the defense is an essential component of the offense. [8]

That Marine Corps manual goes on to acknowledge the offensive importance of *surprise*, because it reduces the enemy's ability to *resist*.[9] What if the adversaries do not try to resist, but instead adopt a resilience strategy? Believing that resistance is futile, they concentrate their efforts on the ability to bounce back and wait until they can go on the offensive again. Offensive weapons against a resilience strategy may differ from those employed where the enemy can be expected to resist. A resilience strategy is the more likely choice for the weaker combatant in asymmetric wars, and has certainly been adopted by modern terrorist organizations.

7.1 Resilience as an Offensive and Defensive Strategy

"Terrorist" enemies are not new to warfighters or intelligence agencies, but the scale of their attacks and their focus on civilian targets has caused some to rethink the options for response. Resilience must be part of this new thinking because it is clearly a part of the enemy's strategy. While the 9/11 Commission did not consider al Qaeda invincible, it noted that this "group" is widely described as adaptable, resilient, needing little higher-level organization, and capable of anything."[10] This is consistent with the military traditions of the horse warriors of the Arab and Mongol peoples, whose preferred style of fighting was evasion, delay, and indirectness.

> The horse warrior chose to fight at a distance, to use missiles rather than edged weapons, to withdraw when confronted with determination and to

---

[8] John Schmitt, *FMFM-1:Warfighting*, Foreword by Gen. A. M. Gray, Commandant, U.S. Marine Corps, Department of the Navy, 1995-401-461/40383 (Washington D.C.: U.S. Government Printing Office, 1989), 25, [On-line]. URL: http://www.clausewitz.com/CWZHOME/Warfit1.htm (Accessed on Sept. 27, 2005.) Carl von Clausewitz, one of the most famous military strategists, argued that offense is an integral part of defense, while defense is often a necessary evil in an offensive strategy. See Carl von Clausewitz, *On War*, M. Howard and P. Paret, trans. and ed. (Princeton, N.J.: Princeton University Press, 1984), 524.

[9] Ibid., 33.

[10] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary* (Washington D.C.: U.S. Government Printing Office, 2004), 17.

> count upon wearing down an enemy to defeat rather than by overwhelming him in a single test of arms.[11]

Against this style of warfare, the European Crusaders found that "face to face style often foundered; charging home could not be made to work against an enemy who saw no dishonor in avoiding contact."[12] Since the Arab armies could not resist the military power arrayed against them, they acted rationally and adopted a resilience strategy for their own defense while systematically breaking down the resilience of their enemies.

Al Qaeda does not have a single command structure that can be identified and attacked. It is a loosely coupled coalition without a unified command structure. This is said to be one of its chief strengths and gives it resilience against attack. In this regard, it follows the playbook developed for "resistance" fighters in occupied Europe during the Second World War.[13]

A resilience strategy can be broken by making the enemy system lose its capacity to absorb disturbance and its ability to undergo change while still retaining essentially the same functions, structures, identity, and feedbacks. A broad look at how similar distributed networks can lose their resilience reveals some new avenues to explore for counter-resilience strategies. It may be worth some effort to examine the long time scale for some clues. This could include looking again at other "hit-and-run" offensive strategists, such as the Vikings and the Mongols, and what ultimately defeated those strategies. In neither case was the answer a resistance defense.

Previous chapters noted several attributes of successfully resilient systems and the weaknesses of these systems. For example, distributed command and information networks respond well to known dangers but are vulnerable to new surprises. A system will become less resilient if it is forced to spend a lot of its resources on resistance strategies. Tightly coupled resistance strategies will make the system even more fragile. A system will also lose resilience when the dangers it must deal with are "too novel, too fast, or too abundant."[14]; that is, the system does not have response capabilities that are robust enough. It cannot marshal these responses quickly enough, or the various dangers are so powerful that they overwhelm all responses. The dangers may become too great if the system has been weakened by previous dangers and has not had time to recover. All of these weaknesses in resilience strategies suggest specific tactics that can be employed in a counter-resilience plan.

---

[11] John Keegan, *A History of Warfare* (New York: Vintage Books (1994), 388.

[12] Ibid., 390.

[13] John Keegan, *Intelligence in War: The Value and Limitations of What the Military Can Learn About the Enemy* (New York; Vintage Books, 2002), 315–319.

[14] C.R. Allen, "Ecosystems and Immune Systems: Hierarchical Response Provides Resilience Against Invasions," *Conservation Ecology* **5**, 1 (2001), 15, [On-line]. URL: http://www.consecol.org/vol5/iss1/art15 (Accessed on November 8, 2005.)

One possibility for both offensive and defensive resilience when dealing with terrorist attacks resembles the human immune system. It would have a diffuse (or distributed) informational and command network with no central control function. It would simultaneously pursue overlapping and even contradictory goals. It would do so, in part, by layering new systems onto old ones (giving the new ones “scaffolding”), parallel processing by several systems, dynamic engagement (an organization attacking for a short time and then being replaced by other organizations), and giving all the agents in the defensive system variable network connectivity. Laying out specific tactics would not be appropriate here, but they are not difficult to imagine.

Strategic options such as these are not unlike those currently included in any military operations plan. They are different in approach because they concentrate not only on destruction of the enemy but also on denying the ability to bounce back from the attack. Anti-resilience strategies/tactics would be multifaceted, simultaneous, and continuous. Chapter Five, which described what individuals, groups and coalitions need for resilience, indicates what kinds of things might be denied to an enemy who is seeking resilience. Some of the possibilities are obvious and well known, but others may indicate options not tried before:

- Reduce options for critical resources (e.g., fuel, people willing to commit suicide) to reduce broad tolerance to surprise such as attack
- Reduce/disrupt options to flee from danger, particularly the ability to melt into the population or flee to friendly states (deny sanctuary)
- Reduce/disrupt information about combatants’ options for safety
- Reduce/disrupt information about what is working for other combatants/units
- Reduce/disrupt access to trusted information about the surprise and what is happening at local and larger scales, e.g., How bad is it? How long will it last? How are others adapting? What do “experts” say?
- Encourage tight coupling to make organizations brittle
- Deny access to facilities needed for cooperation, e.g., communication, resource movement
- Deny coalitions any boundary-spanning personnel through disruption of transport or communication lines.

In a war of resilience the last surviving combatant wins. That side will have planned (and made some critical tradeoffs) for resilience as a weapon. Of critical importance will be the ability to spot emergent phenomena, even when those phenomena are not consistent with expectations or current understanding of how things work. We can be blind to small changes when nothing looks familiar. So, for example, we may only notice changes that indicate a population is shifting from resistance to resilience mode if we know how a particular culture implements those two modes. This may require realignment of intelligence-gathering priorities.

7.2 Resilient Military Organizations and Personnel

Uncertainty presents both a danger and an opportunity for military organizations, and can be offensive or defensive. The military can use it to disrupt the enemy and protect its own assets. Often it is not a weapon at all, but an unfortunate fact of life in complex environments. Scott Snook (U.S. Army, ret.) of the Harvard Business School has taken an in-depth look at a tragic accident in the immediate aftermath of the Persian Gulf War in which two U.S. fighter planes shot down a U.S. helicopter. He asks why nobody predicted the problems that led to this accident, and concludes:

> Part of the answer lies in our inherent limitations as information processors. Part of the answer lies in our linear deterministic approach to causality. Part of the answer lies in the inherent unpredictability of events in complex organizations.[15]

Surprises happen. To the extent that surprises will affect military operations or personnel, planning for the resilience of those assets becomes a logical focus of modern military strategy. As demonstrated in the preceding sections, this means building flexibility and diversity into the options available for critical resources (including physical safety). Snook points out that diverse adaptations to military procedures that make life easier locally can have tragic results when those local adaptations are unknown to outsiders who expect the SOP response. Snook calls local adaptation “practical drift” and suggests that it cannot be eliminated, but it can be acknowledged as a potential problem. It should never be a Black Swan or a New Surprise. Diversity of responses to local situations is both a potential strength and a known danger in distributed systems. We can be surprised by both good and bad things when they happen, but not surprised that they happen. Snook’s analysis presents an excellent example of how building (or encouraging the emergence of) resilience at the appropriate scale—individual, group or coalition—and how recognizing the tradeoffs that have been made can reduce, but not eliminate, tragedies such as friendly fire accidents.

7.3 Complex Military Technology and Resilience

It is tempting to believe that technology can solve the problems involved in building resilience as it has solved so many problems in warfare. While complex technology often increases efficiency for well-defined missions, efficient, complex technology can become the enemy of resilience. Communication systems that take advantage of informal networks and local knowledge, including practical drift, can help to compensate for the looser coupling that is often necessary to enable resilience. This was described in a *Wall Street Journal* article about a U.S. Army captain who used his informal network and knowledge of Iraqi village life to recover stolen

---

[15] Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton N.J.: Princeton University Press, 2000), 204.

equipment by going to the house of the local sheik and negotiating for its return.[16] This type of local communication would actually suffer if it required complex technology. Technology designed to protect combatants can also make them less resilient if it reduces their ability to flee from danger because it is too heavy, equips them only for very specific situations and thus denies them the ability to adapt to surprises, or is so complex that it is unreliable, perhaps due to unpredictable interactions among the components.

At least one military analyst has suggested that resilience will not come from technology in the wars that are likely to be fought in this century, especially if the technological fixes increase both the system's complexity and its inherent uncertainty. Instead of using our clearly superior air power for "discriminate strategic effects" it may be better to use that capability to foreclose options that may be open to adversaries, because denying them options will reduce their ability to prevail in the longer term.[17] Communication technologies may be helpful if they give combatants access to information that will allow them to be resilient. This is one of the goals of network-centric warfare planning: to give many people access to a network of information about what is happening at many scales (local/global and fast/slow) in an effort to help them adapt to unexpected conditions. Even if they have access to all available data, this will not allow them to predict the next moves of the enemy in a rapidly evolving situation.

> [T]he important underlying system interactions and linkages will remain latent and inherently unknowable until the system is stimulated….Even though data management systems like the Joint Targeting Toolbox have the potential to increase transparency in the targeting process, they do not provide "knowledge" any more than they substitute for the insight, judgment, subtlety, balance and finesse captured in the Clausewitzian concepts of coup d'oeil and commander genius.[18]

Troops on the ground must have as much "knowledge" as possible about what is happening and their options for resilience if a surprise occurs.[19]

---

[16] Unfortunately he did not understand the consequences of his action for the sheik, who was killed, apparently for collaborating with the captain. Greg Jaffe, "Trial by Fire: On the Ground in Iraq, Captain Ayers Writes His Own Playbook," *Wall Street Journal* (September 22, 2004), 1A.

[17] Kolenda.

[18] Ibid., 37.

[19] For the difference between knowledge and data (or Bull and Cow), see Anthony G. Oettinger, "A Bull's Eye View of Management and Engineering Information Systems," in *Proceedings of the Association for Computing Machinery*, (Philadelphia, Pa.: Association for Computing Machinery, 1964); and "Knowledge Innovations: The Endless Adventure," *Bulletin of the American Society for Information Science and Technology* **27**, 2 (December/January 2001), 10–15.

7.4 Resilience for Local Civilian Populations After the Battle

In many modern military actions the battle does not end with the conclusion of open hostilities. Military personnel are then asked to engage with local populations who are in either resistance or resilience mode. Local people may be seeking to bounce back from a local surprise (in which they may or may not have taken part) and has deprived them of critical resources, or they may be actively resisting the presence of foreign troops. In these cases military personnel are often asked to shift from seeing local populations as resisters to seeing them as resilience seekers. Sometimes there will be both types in the same population and it is difficult to tell them apart. Since failure to spot a resister can be fatal, it is understandable that it is often assumed that all locals are resisters unless proven otherwise, but this can stiffen resistance if it is perceived as being unresponsive to resilience needs. A potential aid in this dilemma may be gathering intelligence that focuses on and differentiates between resistance and resilience activity. This should be done at all appropriate scales: individual, group, and coalition. It would not enable prediction of what will happen with any particular individual(s), but this type of analysis might allow the deployment of resilience-type resources to areas where they will be used best, while resistance resources can go to where they are more likely to be needed.

The important role of communication, particularly trusted communication, is obvious when dealing with local populations. This is an important weakness of many of the states that are potential enemies of the United States and the European Union. They have often disrupted their own local communication channels in favor of state-controlled entities that are not trusted even by their own citizens. Gaining the trust of a local population is not easy, even if the population welcomes a foreign military presence. The list of recommendations from the Working Group on Bioterrorism Response is worth applying in this instance, since its purpose is to make local populations resilient.[20] A communication strategy that encourages local resilience after a military intervention would include the following tactics:

- Treat the public as a capable ally in promoting resilience to the surprise they have faced. Note: This is different from trying to enlist them as allies (or collaborators) of the new military presence.
- Enlist civic organizations in resilience activities, particularly those that have successful experience in dealing with surprise in this culture.
- Invest in public outreach using trusted sources of information, even if that must be dealt with on a very small scale such as extended families or neighborhoods.
- Restore the ability to communicate with family members as soon as possible and let people know they have options.

[20] The Working Group on Governance Dilemmas in Bioterrorism Response, “Leading During Bioattacks and Epidemics with the Public’s Trust and Help,” *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* **2**, 1 (2004), 217.

- Make sure that activities and plans reflect the values and priorities of local populations. The most efficient way to restore a public service may not be the culturally acceptable one.

7.5 Intelligence and Information for Homeland Resilience

One of the key problems in fighting an enemy like al Qaeda is identifying the enemy combatants. If an enemy does not use a strategy that seeks success with decisive battles, but hits and runs back into large populations, we need to sort that population into at least three groups: good people, dangerous people, and people who will supply the dangerous people. We can do this by relying on trusted locals who are willing to identify the potential adversaries (human source intelligence) or by using other information sources and trying to identify relevant and trustworthy data. These sources would include signals intelligence, such as telephone and Internet traffic; imagery, such as satellite photos; measurements and signatures; and open source information such as news media reports (OSINT). As intelligence agencies develop increasingly sophisticated ways to capture any signals generated within a mixed population, the sorting and interpretation of those signals becomes an ever more critical part of the process.

Both sorting and interpretation are massively more difficult when the enemy has no concrete form, but has "…aggressive belief systems not subject to central authority, shifting alliances of dangerous malcontents, stateless migrants disloyal to any country of settlement."[21] In a way, such an enemy is like a virus or bacterium that can cause infectious epidemics: it has no central control, but is opportunistic and constantly evolving. The only way to deal with it is to identify its location, characteristics, and strategies here and now. Timely intelligence thus takes on new importance for both offensive and defensive measures, which should also be opportunistic and constantly evolving. Specific long-term plans will be almost useless and, in an open society, subject to capture by enemy intelligence measures.

For homeland security, intelligence activities that sort and interpret for resilience and resistance activities could be used to detect changes in the status of potential internal enemies. For example, the top levels of groups may switch to resistance mode or engage resilience defenses at the beginning of an attack. Thus, unlike traditional armies that tend to become more tightly coupled before a battle, these groups might become more loosely coupled to be resilient to the inevitable counterattack. At the same time they prepare to strike a target they would also prepare to activate redundant communication systems or supplies that may be destroyed by retaliation.

Evolving social networks exhibit changing interactions between the human participants. Like all biological systems, human interactions take place at the individual and group levels. Thus, spotting the changes in these interactions is key to understanding the evolution of strategies

[21] Keegan, 318.

at the global and local levels. These interactions may be evidence of a switch from resistance to resilience. They include:

- Competition: An individual (or species) consumes a resource that otherwise would be available to another individual or species (zero-sum game);
- Predation: An individual (or species) kills and eats another individual or species;
- Parasitism: An individual (or species) takes resources from a host and damages the host;
- Commensalism: An individual (or species) takes resources from a host but does not cause any tangible effects;
- Detritivory: An individual (or species) consumes another that is already dead;
- Mutualism: Both individuals and species experience a net benefit;
- Protocooperation: Interaction is favorable to both but is not obligatory to the survival of either; and
- True Cooperation: Interaction is important to the safety or survival of participants and results in all parties getting more of a resource than they would have by acting alone.[22]

In terms of interpreting data anomalies that might indicate terrorist activity, any change in communication that indicates a movement toward mutualism, protocooperation, or cooperation would constitute critical information and indicate a change in a resistance or resilience strategy, or a new phase of an operation.

The interpretation of intelligence data should specifically include analysis of the various scales of the situation, especially local/global and fast/slow. As noted in previous chapters, any interactions between scales is likely to seem chaotic. This is an important insight for those who must analyze causes and develop strategic options. It may, in fact, help describe the allegiance of many different individuals and groups to al Qaeda's cause. Consider, for example, the new interaction of global forces with those that have been exclusively local in some countries. These global forces enter local communities with new communication and trading networks that enable the invasion of people and ideas from outside the locality. These networks also increase the speed of change and the "fast" scale starts to interact in new ways with the slow one. This chaos can be unsettling and is often perceived as a dangerous surprise. Individuals may feel that the only way to reduce the chaos is to choose between local and global and/ or fast and slow. Help in building other options will give them real resilience to these surprises.

---

[22] For more on the relationship between human and biological systems in regard to competition and cooperation see P.H. Longstaff, *Competition and Cooperation: From Biology to Business*, P-98-4 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=374 (Accessed on November 7, 2005.)

Other critical information functions can have an impact on the security of dispersed and loosely coupled organizations such as al Qaeda. These are most effective when implemented by (and shared with) people at all appropriate scales and can give clues about where to look for communication that can be intercepted and interpreted. In loosely coupled organizations these information functions are often not implemented in the same way that they would be in tightly coupled organizations.

- Scanning. Individual groups scan the local and global environments for information about changes in the local environment, resources available, and the detection of dangerous trends. They find this information by observing their immediate surroundings and using higher scale information sources such as the news media. They may or may not share the information they develop with higher levels or other groups, but they will share it with family and close neighbors.
- Damage detection. This is often critical in tightly coupled organizations, since what hurts one part hurts all the other parts as well. In loose coalitions that act independently, this damage detection function would be strictly local and would be used only to detect damage to critical functions or resources.
- Intruder detection. This function becomes especially critical to small dispersed groups, because identification of their members is the greatest danger they face. They may have elaborate schemes to protect against intrusion, and these schemes may be detectable in their communications. It is also possible that they may trigger resilience plans if they believe the group has been detected, thereby enabling an informant to gather more information about those plans.
- Change in trustworthy individuals. For the same reasons, the local group may take special precautions to detect any change in those who have been found to be trustworthy. This may be an important vulnerability in any group where deception is not considered a moral infraction.
- Information about successful strategy/tactics. Even groups that do not depend on each other would like to know what is effective for groups with similar aims, what makes other groups offensively successful, and what makes them resistant or resilient to attack. They can send this information in code to each other through conventional communications networks, although they risk the code's being broken. More often, they use the international news media to communicate this information, as these media are sometimes a more trusted information source than media in their home countries.

Surveillance of local (non-media) communication channels can also identify objects that are out of place or people who are acting abnormally. There is a very real danger that this could reduce local resilience of local populations by reducing local trust in their local communication channels. Any attempt to use local populations as information gatherers to report on other people can also reduce resilience if it makes the population fear the people they have always trusted. If they do not perceive that they have resilience they will be forced to look for resistance. This danger can be reduced, if not entirely avoided, by not requiring tight coupling of local behavior

(reporting of any deviance) but, instead, asking local individuals and groups to report effective resilience strategies.

There has been a great deal of debate in the United States about the need for coordination among the various agencies charged with defending the security of the homeland and of citizens abroad through both resistance and resilience strategies. There are, predictably, forces pushing these agencies together while others pull them apart. Some have argued that a single system would be more efficient and information would flow more easily. Others argue that a single agency would be more dangerous, because it would be tightly coupled and redundancy would be taken out of the system. Both sides have merit, and the policy debate must balance the efficient against the resilient. This probably means at least some redundancy. Anyone seeking resilience or resistance through redundancy should take note of the evidence that redundant functions are more likely to increase resilience if they do not exactly duplicate each other. The most resilient systems have overlapping functions and/or technologies that give the system several ways to accomplish something. For example, a study of large transportation systems concluded that redundancy is more stable if the overlapping agencies did not have to deal with the same superior agency on a daily basis.[23]

Using the concepts developed here to collect and interpret intelligence data should not replace time-tested techniques. We must build on the foundation of current practice, with the linked concepts of resistance and resilience as one of many screens through which data are sifted.

[23] J. Bendor, *Parallel Systems: Redundancy in Government* (Berkeley, Calif.: University of California Press, 1985).

Chapter Eight

First Steps for Security Planning in Unpredictable Environments

Accepting uncertainty is not easy. It is much easier to believe that if we just had the right information and used the right economic or political formula we could predict surprises and build a foolproof resistance strategy for them. As soon as we give up this belief in predictability, we can supplement resistance strategies with strategies to build a resilient system that gives us more of what we want more often:

- More freedom of movement for individuals and groups that allows them to take advantage of opportunities and take risks;
- A system that will bounce back, even in the face of Black Swans or New Surprises; and
- Reduced effectiveness of any deliberate attack. Such an attack would become successful only in the short term and in limited geographical areas with the affected populations receiving immediate and appropriate help to return them to the place they were before the attack, reducing the case for restrictive resistance strategies.

Certainly, resistance is the preferred strategy when trying to deal with a danger. It is better to not be in danger at all, but there are times when that is not possible. At other times resistance will place too many constraints on the system. It may be possible to strengthen cell walls in humans so that viruses cannot enter, but this would also keep out the oxygen and nutrients that the cell needs to live. Resistance can also become like friction or wind drag in physical systems: sometimes it can slow the system down so much that it cannot operate at acceptable levels. Too much passenger screening would slow down the passenger boarding process to the point where flights could not take off. A world where all systems were designed to resist any possible surprise would not move at all.

Military analyst and historian Paul K. Davis examined the ways people plan under conditions of uncertainty and listed what he considered the most important generic mechanisms for dealing with uncertainty:

- Ignore it, because the “cost of recourse” later is small, one can do nothing about the uncertainties, or one does not know better.
- Reduce it by eliminating particular sources of risk or improving the quality of prediction.
- Insure against it (i.e., share the risk by buying an insurance policy or joining groups that pool resources).
- Diversify, and thereby reduce vulnerability to specific risks, through a portfolio approach such as that used in financial investment.

- Hedge against problems by developing capabilities to cope with plausible events.
- Plan for sequential, adaptive, decision making over time.[1]

This report has discussed all of these options, which can be viewed as resilience strategies. It suggests that in environments with massive uncertainty, the best plan may be to not have one. The best strategy may be to build an ability to incorporate new information and change tactics as the situation unfolds. You might also prefer easily convertible resources.

8.1 First Steps Toward Managing Security in Unpredictable Systems

8.1.1 Realign Expectations About Certainty

This task may be the most important and the most difficult. Surprise is normal. The most successful people are not those who resist surprise, but those who make themselves or their organizations resilient. Resilience should be prized. In an evolving environment we can waste a large amount of resources trying to resist change. Probability calculations do not allow us to resist dangers; they only allow us to manage risks. Moreover, they are less than useless when the environment is unstable or when the calculations do not measure real variables or use real information.

8.1.2 Give up the "Blame Game"

While the Blame Game may be helpful for immediate emotional or political purposes, it seldom solves the real problem. Most experienced leaders already know the unpredictability of the system(s) in which they operate, but they cannot bring their suspicions into the open, because they fear this will be seen as a less than honest "excuse" for the unintended consequences of their actions. Alternatively, when bad things happen, leaders often fear that they have just misjudged the situation or done something wrong, which would mean they could be blamed. In fact, they may have made all the right choices but have been unable to predict (because prediction was impossible) how their actions would affect the system.[2] The 9/11 Commission took an important step in this direction when it decided that apportioning blame would be counterproductive.

---

[1] Paul K. Davis, *Strategic Planning Amidst Massive Uncertainty in Complex Adaptive Systems: The Case of Defense Planning* (Santa Monica, Calif.: The RAND Corporation).

[2] For more on managing complex organizations, see P.H. Longstaff, Raja Velu, and Jonathan Obar, *Resilience for Industries in Unpredictable Environments: You Ought To Be Like Movies*, P-04-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=595 (Accessed on November 7, 2005.)

8.1.3 Never Overdrive the Headlights

If a system has several subsystems that operate at different scales we will encounter unavoidable surprises. We will fail to manage the system if we try to make the system move faster than it can respond to surprises.

> The deer frozen in the headlights. The driver frozen at the wheel with no time to brake or swerve—both are doomed by speed and bad luck. Bad luck you cannot do much about; speed you can. Overdriving the headlights—that is, counting on no surprises out there in the darkness—is folly on any road. Braking time must match awareness time.[3]

8.1.4 Trade Some Efficiency for Some Resilience

We must consider where to use some of our resources to build resilience through strategies such as redundancy for critical functions and a broad tolerance that will allow us to function even in the face of surprises. This is especially important if we are competing with an organization that uses a resilience strategy: the last one standing will be the winner. If a supplier is critical to survival, we should demand that it have a resilience plan, which may mean higher prices if the supplier must trade efficiency for resilience. This trade may not be easy, but it should be made deliberately.

8.1.5 It Is Not Just a Government Problem

The private sector has important roles to play, because it must be able to bounce back from surprises to keep the economy operational. The energy and creativity exhibited by publicly traded businesses that the Securities and Exchange Commission forced to disclose their preparations for potential computer problems in the year 2000 gives hope that they could perform equally well if they accepted the challenge of developing resilience plans. Specific government mandates could be counterproductive, because if each organization has its own plans there is less danger of a brittle, tightly coupled system that can be brought down by finding a common weakness.

8.1.6 Do Not Design Security, Discover It

We must iterate our way to success. Small steps that allow us to change course often will be more effective than big steps in a time of great uncertainty. We must resist the demands for big solutions that impose the same answer on many individuals or many situations, because this reduces diversity. We must try many things, sow many seeds, and encourage experiments. We must concentrate on finding approaches that are effective here, today, and reward them with more

---

[3] Stewart Brand, *The Clock of the Long Now* (New York: Basic Books, 1999), 9.

resources. We must pay equally close attention to failed approaches and reduce the resources allocated to them, but without playing the Blame Game.

8.1.7 Develop More Trusted Sources of Information

We cannot manage risks without good information about surprises. Organizations that suppress information about “failures,” or that fail to reward candor, reduce their ability to improve their performance next time. We must build a loose network of people who have access to information in many domains, and we must not forget to remember.

Research on security in unpredictable systems is just beginning, and continues to evolve as this report goes to press. The future of these ideas is uncertain. Any “knowledge” that may be developed will come from diverse trusted sources, but errors will always occur. In the end, the best way to build security in an unpredictable system may be counterintuitive. The most secure systems may be those that can find their own answers at the right scale and the right time, and the definitions of “risk management” and “leadership” may have to change.

Acronyms

NYFD	New York Fire Department
OSINT	open source intelligence
SOP	standard operating procedure
UNK	unknown

Appendix A

Overview of Complex Systems

Three types of unpredictable systems are considered here: chaotic, complex, and complex adaptive. Most human systems fit in the last category, but it is important to review briefly how all these systems work before we address security considerations. We begin by defining what complex systems are not.

A. 1 Simple Systems

Simple systems are ones where 2 plus 2 always equals 4. They are systems where, if we do A under condition B, it will result in C. Simple systems exist in many places in nature. Under most conditions, if we add two molecules of hydrogen to one molecule of oxygen, we will get water. If we cool the water to 32 degrees it will freeze. These types of systems are responsible for most of the technology we use. They are useful precisely because they are predictable. Discovering them is the enduring achievement of science. Simple systems also have few interactions and feedback/feed-forward loops, centralized decision making, and decomposability, so that taking away parts does not destroy the whole.[1]

A.2 Chaotic Systems

In the last century science began to investigate systems about which reliable predictions could not be made, because, for example, the system included so many variables that the mathematics become impossible. Yet these are important systems: they include natural ecological systems and human organizations, and the interest in them has been intense.

A *chaotic* system is almost the exact opposite of a simple one. A system is said to be chaotic if its operations at certain scales show no patterns and the predictability of variables decreases quickly over time. Some systems may become chaotic in the short term and then settle back into some kind of “bounded” equilibrium where behavior deviates (often unpredictably) within a given range. Chaotic systems can also become unstable or turbulent due to the buildup of small perturbations in the forces working on them. For example, water running in a pipe will become turbulent or chaotic at certain velocities.[2] Often, turbulence is caused when things interact at different speeds, densities, etc. Human systems are seldom truly chaotic, even if they seem unpredictable in the short term, because they generally operate within some rational bounds. However, they are often complex.

---

[1] See, e.g., John Casti, *Complexification: Explaining a Paradoxical World Through the Science of Surprise* (New York: Harper Collins, 1994), 271–272.

[2] See **Appendix B** for additional information.

A.3 Complex Systems

Complex systems have at least two defining properties: intricate interdependencies and many variables operating at the same time. Systems are said to become complex when they are made up of several parts that depend on each other to function. A depends on B and C, while C depends on A and D, and E depends on A, B, C, and D working together. Examples of complex systems include the weather, which depends on an astonishing array of interactions among many forces around the globe, and the spread of disease in a population, which depends on such factors as contact rates, transmissibility rates, susceptibility of the population to intervention strategies, et cetera.

A.3.1 Self-Organization

Perhaps the most important property for the study of security in these systems is their ability to self-organize or reorganize at critical points of instability. This is possible because there are feedback loops that reinforce things that work well and remove things that do not. Factors such as the system's history will affect the direction in which it moves when it becomes unstable. Movement toward a new equilibrium does not start with a blank slate and is said to be "path dependent," but the path taken under the old equilibrium does not "predict" the new path: it merely restricts the options.

A.3.2 Nonlinearity

The effect of an input to the system, such as an infected person or the air disturbed by a butterfly flapping its wings, may diffuse unevenly throughout the system because the other components of the system are not evenly distributed or the force causing the distribution is not equally strong throughout the system. Adding an element to the system that can be further duplicated within it may cause a shift in the total system that is much greater than the amount added. For example, sending a rumor about a company via email to a friend in that company only adds one piece of information to that company's information system. Because many agents (employees) in the company are connected via email, the piece of information can multiply in the system as each employee sends it to many others. The information multiplies in the system because the agents are interconnected in a network.[3] Because the trajectories (e.g., rates of increase or decline) of complex systems are nonlinear it is easy to be deceived about what they will do next. Just because they increase today does not necessarily mean they will do so tomorrow.

[3] There is a growing body of scholarship on the nature of networks and how they increase complexity; see **Appendix B**.

A.3.3 Emergent Properties

Complex systems have a tendency to do things that would not be anticipated by looking at a diagram, no matter how detailed, of the system's operation. Human consciousness is thought to be an emergent property of our enormously complex brains. In complex technical systems, "bugs" are sometimes an emergent property.

> A bug is a particular kind of failure. It's an emergent property of a system, one that is not desirable. It's different from a malfunction. When something malfunctions, it no longer works properly. When something has a bug, it misbehaves in a particular way, possibly unrepeatable, and possibly unexplainable. Bugs are unique to systems. Machines can break, or fail, or not work, but only a system can have a bug.[4]

A.4 Complex Adaptive Systems

Some complex systems are *adaptive* or are said to *evolve* when individual agents operate independently in response to forces in their environments via feedback. In some systems the agents can "learn" from each other when some agents obtain more resources and their actions are copied by other agents. In systems where other agents in the current generation cannot learn about or absorb the change—for example, when the change is a mutation in an organism's genetic structure—that change can, nevertheless, become prevalent in succeeding generations because agents that have changed will leave more offspring. This is evolution by natural selection. For example, a mouse with better hearing is more likely to survive the presence of foxes in her environment and to leave more offspring than other mice. Over many generations these offspring will also leave more offspring and gradually the number of mice without acute hearing will decline.[5] Yet even the mouse species that is best adapted to the current environment will become extinct if it does not adapt along with its environment. It needs to alter its resistance or resilience strategies as the dangers it faces change, and any changes it makes will force changes in species it interacts with. Stability is thus very rare in these systems.

---

[4] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: John Wiley & Sons, Inc., 2000), 7.

[5] German scientist Dietrich Dorner has given us another way to visualize how complex adaptive systems work in human undertakings:

> [W]e could liken a decision maker in a complex situation to a chess player whose set has many more than the normal number of pieces, several dozen, say. Furthermore, these chessmen are all linked to each other by rubber bands, so that the player cannot move just one figure alone. Also, his men and his opponent's men can move on their own and in accordance with rules the player does not fully understand or about which he has mistaken assumptions. And, to top things off, some of his and his opponent's men are surrounded by a fog that obscures their identity.

Dietrich Dorner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations* (New York: Metropolitan Books, 1996).

Appendix B

Further Reading

B.1 Anthropology and History

John M. Barry, *The Great Influenza: The Epic Story of the Deadliest Plague in History* (New York: Penguin, 2004).

Stewart Brand, *The Clock of the Long Now* (New York: Basic Books, 1999).

P.F. Brown, *Venice and Antiquity: The Venetian Sense of Past* (New Haven, Conn.: Yale University Press, 1997).

John Lewis Gaddis, *Surprise, Security, and the American Experience* (Cambridge, Mass.: Harvard University Press, 2004).

James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (New York: Doubleday, 2004).

A.P. Vayda and B.J. McCay, "New Directions in Ecology and Ecological Anthropology," *Annual Review of Anthropology* **4** (1975), 293–306 .

B.2 Biology and Ecology

Michael Begon, John L. Harper, and Colin R. Townsend, *Ecology: Individuals, Populations, and Communities*, 3rd ed. (Oxford and Cambridge, Mass.: Blackwell Science, 1996).

Daniel R. Brooks and Deborah A. McLennan, *The Nature of Diversity: An Evolutionary Voyage of Discovery* (Chicago and London: University of Chicago Press, 2002).

Harvey Brooks, "The Typology of Surprises in Technology, Institutions, and Development," in *Sustainable Development of the Biosphere*, W.C. Clark and R.E. Munn, eds. (Laxenburg, Austria: International Institute for Applied Systems Analysis, 1986).

Robert B. Glassman, “Persistence and Loose Coupling in Living Systems,” *Behavioral Science* **18** (1973), 83–98.

Lance H. Gunderson and C.S. Holling, eds., *Panarchy: Understanding Transformations in Human and Natural Systems* (Washington, D.C., and London: Island Press, 2002).

Lance H. Gunderson and Lowell Pritchard, eds., *Resilience and Behavior of Large Scale Systems* (Washington, D.C., and London: Island Press, 2002).

Shahid Naeem, “Biodiversity Equals Instability?” *Nature*. **416** (2002), 23–24.

Charles G. Orosz, “An Introduction to Immuno-ecology and Immuno-informatics, in *Design Principles of the Immune System and Other Distributed Autonomous Systems*, Lee A. Segel and Irun R. Cohen, eds. (Oxford and New York: Oxford University Press, 2001), 125–149.

Charles L. Redman and Ann P. Kinzig, “Resilience of Past Landscapes: Resilience Theory, Society, and the *Longue Durée,” Conservation Ecology* **7**, 1 (2003), [On-line]. URL: http://www.consecol.org/vol7/iss1/art14

Robert E. Ricklefs and Gary L. Miller, *Ecology*, 4th ed. (New York: W. H. Freeman and Co., 1999).

Lee A. Segel, “Diffuse Feedback From a Diffuse Information Network: The immune System and Other Distributed Autonomous Systems,” in *Design Principles of the Immune System and Other Distributed Autonomous Systems*, Lee A. Segel and Irun R. Cohen, eds. (Oxford and New York: Oxford University Press, 2001), 203–226.

B.3 Business and Economics

Gary Ahlquist, Gil Irwin, David Knott, and Kimberly Allen, “Enterprise Resilience,” *Best’s Review*, July 2003.

Robert Jackall, *Moral Mazes: The World of Corporate Managers* (New York: Oxford University Press, 1988).

Daniel Kahneman and Dan Lovallo, “Timid Choices and Bold Forecasts: A Cognitive Perspective on Risk Taking,” *Management Science* **39**, 1 (1993), 17–31.

M.L. Katz and C. Shapiro, “Systems Competition and Network Effects,” *The Journal of Economic Perspectives* 8, 2 (Spring 1994), 93–115.

Benoit Mandelbrot and Richard L. Hudson, *The (Mis)behavior of Markets: A Fractal View of Risk, Ruin, and Reward* (New York: Basic Books, 2004).

Dennis S. Mileti and John H. Sorenson, “Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events,” *Columbia Journal of World Business*, (Spring 1987), 14.

Paul Ormerod, *Butterfly Economics: A New General Theory of Social and Economic Behavior* (New York: Basic Books, 1998).

Yossi Sheffi, *The Resilient Enterprise: Overcoming Vulnerability for a Competitive Age* (Cambridge, Mass.: MIT Press, 2005).

F.M. Sherer and Dietmar Harhoff, “Technology Policy in a World of Skew-Distributed Outcomes,” *Research Policy* 29, 4–5 (April 2000), 559–566.

B.4 Communications Media/Services

BITS Guide to Business-Critical Telecommunication Services (Washington, D.C.: BITS, 2004).

Jennings Bryant and Dolf Zillmann, eds., Media Effects: Advances in Theory and Research, 2nd ed. (Mahwah, N.J.: Lawrence Erlbaum Associates, 2002).

Joan Deppa, Maria Russell, Dona Hayes, and Elizabeth Lynne Flocke, *The Media and Disasters: Pan Am 103* (New York: New York University Press, 1994).

Steven Hess and Marvin Kalb, eds., *The Media and the War on Terrorism* (Washington, D.C.: Brookings Institution Press, 2003).

Norris R. Johnson, “Panic and the Breakdown of Social Order: Popular Myth, Social Theory, and Empirical Evidence,” *Sociological Focus* **20**, 3 (1987), 171–183.

Brigitte Nacos, *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism* (New York: Rowman and Littlefield, 2002.

Nancy Palmer, ed., *Terrorism, War and the Press* (Cambridge Mass.: Joan Shorenstein Center, Harvard University, 2003).

Paul Starr, *The Creation of the Media: Political Origins of Modern Communications* (New York: Basic Books, 2004).

B.5 Complexity, Chaos, General Systems Theories

Yaneer Bar-Yam, ed., *Unifying Themes in Complex Systems: Proceedings of the International Conference on Complex Systems* (Cambridge, Mass.: Perseus Books, 2000).

Ludwig von Bertalanffy, *General System Theory: Foundations, Development, Applications* (New York: George Braziller, Inc., 1969).

Mark Buchanan, *Ubiquity: The Science of History…or Why the World Is Simpler Than We Think* (New York: Crown Publishers, 2000).

Murray Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex* (New York: W.H. Freeman, 1994).

James Gleick, *Chaos: The Making of a New Science* (New York: Penguin Books, 1988).

Stephen Hawking, *The Universe in a Nutshell* (New York: Bantam, 2001).

John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (Reading, Mass.: Addison-Wesley, 1995).

Steven Johnson, *Emergence: The Connected Lives of Ants, Brains, Cities, and Software* (New York: Scribner, 2001).

Stuart Kauffman, *At Home in the Universe: The Search for the Laws of Organization and Complexity* (New York: Oxford University Press, 1995).

F. David Peat, *From Certainty to Uncertainty: The Story of Science and the Ideas of the Twentieth Century* (Washington, D.C.: John Henry Press, 2002).

M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos* (New York: Simon & Schuster, 1992).

Phillip R. Wallace, *Paradox Lost: Images of the Quantum* (New York: Springer, 1996).

Stephen Wolfram, *A New Kind of Science* (Champaign, Ill.: Wolfram Media, 2002).

B.6 Computer/Digital Security

Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (New York: Wiley, 2001).

Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: John Wiley & Sons, Inc., 2000).

B.7 Engineering and Physical Science

Steven D. Gribble, "Robustness in Complex Systems," in *Proceedings of the 8th Workshop on Hot Topics in Operating Systems* (New York: IEEE, May 2001), 21–26.

Max Henrion and Baruch Fischoff, "Assessing Uncertainty in Physical Constants," *American Journal of Physics* **54**, 9 (1986), 791–798.

B. 8 Interdisciplinary Studies

Philip Ball, *Critical Mass: How One Thing Leads to Another* (New York: Farrar, Straus and Giroux, 2004).

John Seely Brown and Paul Duguid, *The Social Life of Information* (Cambridge, Mass.: Harvard University Press, 2000.

D. Batten, J. Casti, and R. Thord, eds., *Networks in Action: Communication, Economics and Human Knowledge* (Berlin, New York, and London: Springer-Verlag, 1995).

Fikret Berkes, Johan Colding, and Carl Folke, eds., *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change* (London and New York Cambridge University Press, 2003).

Harvey D. Brooks, “The Typology of Surprises in Technology, Institutions, and Development,” in *Sustainable Development and the Biosphere*, W.C. Clark and R.E. Munn, eds. (Laxenburg, Austria: International Institute for Applied Systems Analysis, 1986), 325–347.

John L. Casti, *Complexification: Explaining a Paradoxical World Through the Science of Surprise* (New York: Harper Collins, 1994).

John L. Casti and Anders Karlqvist, eds., *Cooperation and Conflict in General Evolutionary Processes* (New York: John Wiley & Sons, 1995).

Dietrich Dorner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations* (New York: Metropolitan Books, 1996).

Carl Folke, Fikret Berkes, and Johan Colding, “Ecological Practices and Social Mechanisms for Building Resilience and Sustainability,” in *Linking Social and Ecological Systems: Management Practices and Social Mechanisms for Building Resilience*, Fikret Berkes and Carl Folke, eds. (Cambridge, UK: Cambridge University Press, 1998), 414–436.

Lance H. Gunderson and C.S. Holling, eds., *Panarchy: Understanding Transformations in Systems of Humans and Nature* (Washington, D.C.: Island Press, 2002).

C.S. Holling, “Understanding the Complexity of Economic, Ecological, and Social Systems,” *Ecosystems* **4** (2001), 390–405.

Granger Morgan and Max Henrion, *Uncertainty: A Guide to Dealing With Uncertainty in Quantitative Risk and Policy Analysis* (Cambridge, UK: Cambridge University Press, 1992, reprinted 1998).

F. David Peat, *From Certainty to Uncertainty: The Story of Science and the Ideas of the Twentieth Century* (Washington, D.C.: John Henry Press, 2002).

Lee A. Segel and Irun R. Cohen, eds., *Design Principles for the Immune System and Other Distributed Autonomous Systems* (Oxford and New York: Oxford University Press, 2001).

Nassim Nicholas Taleb, *Fooled by Randomness: The Hidden Role of Chance in Life and the Markets* (New York: TEXERE, 2004).

B.9 Management and Organizational Studies

Chris Frost, David Allen, James Porter, and Philip Bloodworth, *Operational Risk and Resilience* (Oxford and Boston: Butterworth Heinemann, 2001).

Dietrich Dorner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations* (New York: Metropolitan Books, 1996).

Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston: Little, Brown and Company, 2000).

Gary Hamel and Liisa Valikangas, "The Quest for Resilience," *Harvard Business Review* (September 2003), 52–63.

M.T. Hannan, "Uncertainty, Diversity, and Organizational Change," *Behavioral and Social Sciences: Fifty Years of Discovery*, N.J. Smelser and D.R. Gerstein, eds. (Washington, D.C.: National Academy Press, 1986).

P.H. Longstaff, *Competition and Cooperation: From Biology to Business*, P-98-4 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=374

P.H. Longstaff, Raja Velu, and Jonathan Obar, *Resilience for Industries in Unpredictable Environments: You Ought to Be Like Movies*, P-04-1, (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=595

Ian McCarthy and Jane Gillies, "Organizational Diversity, Configurations and Evolution," in *Complex Systems and Evolutionary Perspectives on Organizations: The Application of Complexity Theory to Organizations* (Oxford UK: Elsevier Science, 2003), 71–97.

John W. Meyer and W. Richard Scott, *Organizational Environments: Ritual and Rationality* (Beverly Hills, Calif.: Sage, 1983).

Dennis S. Mileti and John H. Sorenson, "Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events," *Columbia Journal of World Business* (Spring 1987), 13–18.

Eve Mitleton-Kelly, ed., *Complex Systems and Evolutionary Perspectives on Organizations: The Application of Complexity Theory to Organizations* (Oxford, UK: Elsevier Science, 2003).

Anthony G. Oettinger, "A Bull's Eye View of Management and Engineering Information Systems," in *Proceedings of the Association for Computing Machinery* (Philadelphia, Pa.: Association for Computing Machinery, 1964).

Anthony G. Oettinger, "Knowledge Innovations: The Endless Adventure," *Bulletin of the American Society for Information Science and Technology* **27**, 2 (December/January 2001), 10–15.

J. Douglas Orton and Karl E. Weick, "Loosely Coupled Systems: A Reconceptualization," *Academy of Management Review* **15**, 2 (1990), 203–223.

Uriel Rosenthal, Michael T. Charles, and Paul T. Hart, eds., *Coping With Crisis: The Management of Disasters, Riots and Terrorism* (Springfield, Ill.: Charles C. Thomas Publishers, 1989).

Peter Schwartz, *The Art of the Long View* (New York: Currency, 1996).

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

R. Stacey, *Complex Responsive Processes in Organizations: Learning and Knowledge Creation* (London and New York: Routledge, 2001).

R. Stacey, *Complexity and Group Processes: A Radically Social Understanding of Individuals* (London: Brunner-Routledge, 2003).

R. Stacey, *Strategic Management and Organizational Dynamics: The Challenge of Complexity*, 4th ed. (London: Pearson Education, 2003).

R. Stacey, D. Griffin, and P. Shaw, *Complexity and Management: Fad or Radical Challenge to Systems Thinking* (London and New York: Routledge, 2000).

David Stark, "Heterarchy: Distributing Authority and Organizational Diversity," in *The Biology of Business: Decoding the Natural Laws of Enterprise*, John Henry Clippinger III, ed. (San Franciso: Jossey-Bass, 1999), 153–179.

Arthur L. Stinchcombe, *Information and Organizations* (Berkeley, Calif.: University of California Press, 1990).

James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (New York: Doubleday, 2004).

Peter Wayner, "Predict the Future? You Can Bet on It," *The New York Times*, October 2, 2003.

B.10 Military and National Security

David Alberts and Thomas Czerwinski, eds., *Complexity, Global Politics, and National Security* (Washington, D.C.: Department of Defense, CCRP Publication Series, 1997).

David Alberts, John Garstka, and Frederick Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: Department of Defense, CCRP Publication Series, 1998).

Alan D. Beyerchen, "Clausewitz, Nonlinearity and the Unpredictability of War," *International Security* **17**, 3 (Winter 1992), 59–90.

Paul K. Davis, "Strategic Planning Amidst Massive Uncertainty in Complex Adaptive Systems: The Case of Defense Planning," [On-line]. URL: http://www.rand.org/contacts/personal/pdavis/davisICCS.html

John Lewis Gaddis, *Surprise, Security, and the American Experience* (Cambridge, Mass.: Harvard University Press, 2004).

Elizabeth Goldschmidt, "Open Source Intelligence: Sources Methods, and Questions," presentation at Harvard University (May 7, 2004).

Victor Davis Hanson, *Carnage and Culture: Landmark Battles in the Rise of Western Power* (New York: Anchor Books, 2001).

Andrew Ilachinski, *Land Warfare and Complexity* (Arlington, Va.: Center for Naval Analysis, 1996).

Stuart Johnson, Martin Libicki, and Gregory Treverton, *New Challenges, New Tools for Defense Decisionmaking* (Santa Monica, Calif.: The RAND Corporation, 2003).

John Keegan, *A History of Warfare* (New York: Vintage Books, 1994).

John Keegan, *Intelligence in War: The Value and Limitations of What the Military Can Learn About the Enemy* (New York: Vintage Books, 2002).

Christopher D. Kolenda, Major, U.S. Army, *Transforming How We Fight: A Conceptual Approach*, submitted for the Admiral Richard G. Colbert Memorial Prize, U.S. Naval War College, Newport, R.I., (May 16, 2002).

Anthony G. Oettinger, *Whence and Whither Intelligence, Command and Control? The Certainty of Uncertainty*, P-90-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=339

Timothy J. Sakulich, *Precision Engagement at the Strategic level of War: Guiding Promise or Wishful Thinking*, Occasional Paper No. 25 (Maxwell AFB, Ala.: USAF Center for Strategy and Technology, Air University, 2001).

Paul Seabury and Angelo Codevilla, *War: Ends and Means* (New York: Basic Books, 1990).

Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton, N.J.: Princeton University Press, 2000).

Carl von Clausewitz, *On War*, M Howard and P. Paret, trans. and ed. (Princeton N.J.: Princeton University Press, 1984).

John Schmitt, *FMFM-1: Warfighting*, Foreword by Gen. A. M. Gray, Commandant, U.S. Marine Corps, Department of the Navy, 1995-401-461/40383 (Washington, D.C.: U.S. Government Printing Office, 1989).

B.11 Networks and Network Science

Albert-Laszlo Barabasi, *Linked: The New Science of Networks* (Cambridge, Mass.: Perseus Press, 2002).

Mark Buchanan, *Nexus: Small Worlds and the Groundbreaking Science of Networks* (New York and London: W.W. Norton & Co., 2002).

Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (New York and London: W.W. Norton & Co., 2003).

Duncan J. Watts, *Small Worlds: The Dynamics of Networks Between Order and Randomness* (Princeton, N.J.: Princeton University Press, 1999).

B.12 Psychology and Education

Uri Merry, *Coping with Uncertainty: Insights from the New Sciences of Chaos, Self-Organization and Complexity* (Westport, Conn., and London: Praeger, 1995).

B.13 Public Policy and Government

Johannes M. Bauer, "Harnessing the Swarm: Communications Policy in an Era of Ubiquitous Networks and Disruptive Technologies, *Communications & Strategies* **54** (2nd quarter 2004), 19–43.

J. Bendor, *Parallel Systems: Redundancy in Government* (Berkeley, Calif.: University of California Press, 1985).

Michael Bohn, *Nerve Center: Inside the White House Situation Room* (Washington, D.C.: Brassey's Inc., 2003).

Russell R. Dynes, "Community Emergency Planning: False Assumptions and Inappropriate Analogies," *International Journal of Mass Emergencies and Disasters* **12**, 2, 141–158.

Thomas A. Glass and Monica Schoch-Spana, "Bioterrorism and the People: How to Vaccinate a City Against Panic," *Clinical Infectious Diseases* **34** (2004), 217–223.

Roz D. Lasker, *Redefining Readiness: Terrorism Planning Through the Eyes of the Public* (New York: Center for the Advancement of Collaborative Strategies in Health and The New York Academy of Medicine, September 2004).

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary (Washington, D.C.: U.S. Government Printing Office, 2004).

Peter J. May, *Recovering From Catastrophes: Federal Disaster Relief Policy and Politics* (Westport, Conn., and London: Greenwood Press, 1985).

Claire B. Rubin and Martin D. Saperstein, *Community Recovery From Major Natural Disaster* (Boulder, Colo.: Program on Environment and Behavior, Institute of Behavioral Science, University of Colorado, 1985).

James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven and London: Yale University Press, 1998).

Richard L. Thornburgh, "Three Mile Island: A Case Study in C3I for Crisis Management," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1988*, I-89-1 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=300

Robert P. Wolensky and Kenneth C. Wolensky, "Local Government's Problem With Disaster Management: A Literature Review and Structural Analysis," *Policy Studies Review* **9**, 4 (Summer 1990), 703-725.

The Working Group on Governance Dilemmas in Bioterrorism Response, "Leading During Bioattacks and Epidemics with the Public's Trust and Help," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* **2**, 1 (2004), 25–39.

B. 14 Risk Management

Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley & Sons, 1996).

James R. Chiles, *Inviting Disaster: Lessons From the Edge of Technology* (New York: Harper Business, 2001).

Lee Clark, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago and London: University of Chicago Press, 1999).

Andrew Kirby, ed., *Nothing To Fear: Risks and Hazards in American Society* (Tucson, Ariz.: University of Arizona Press, 1990).

Alexander Kouzmin and Alan Jarman, "Crisis Decision Making: Towards a Contingent Decisions Path Perspective," in Uriel Rosenthal, Michael T.Charles, and Paul T. Hart, eds., *Coping With Crisis: The Management of Disasters, Riots and Terrorism* (Springfield, Ill.: Charles C. Thomas Publishers, 1989), 397–435.

Darius Lakdawalla and George Zanjani, "*Insurance, Self Protection, and the Economics of Terrorism*, Working Paper of the RAND Institute for Civil Justice, WR-123-ICJ (Santa Monica, Calif.: The RAND Corporation, December 2003).

Uri Merry, *Coping With Uncertainty* (Westport, Conn., and London: Praeger, 1995).

Douglas Paton, Leigh Smith, and John Violanti, "Disaster Response: Risk, Vulnerability and Resilience," *Disaster Prevention and Management* **9**, 3 (2000), 173–179.

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

James Reason, *Managing Risks of Organizational Accidents* (Aldershot, UK, and Brookfield, Vt.: Ashgate, 1997).

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

Barry Strauch, *Investigating Human Error: Incidents, Accidents, and Complex Systems* (Aldershot, UK, and Burlington, Vt.: Ashgate Publishing, 2002).

Zur Shapira, *Risk Taking* (New York: Russell Sage Foundation, 1995).

Paul Slovic, *The Perception of Risk* (London and Sterling, Va.: Earthscan Publications, 2000).

PPLONGSTAFF

ISBN 1-879716-95-X