Risk Analysis, Vol. 29, No. 4, 2009 DOI: 10.1111/j.1539-6924.2009.01216.x

Perspective

On the Definition of Resilience in Systems

Yacov Y. Haimes*

1. INTRODUCTION

In the current era of world-wide terrorism, the terms "vulnerability" and "resilience" have become common in the parlance of risk analysis, and various attempts have been made to define and to quantify them. In an article published in *Risk Analysis*, "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures,"[1] I offered the following definitions: *Vulnerability* refers to the inherent states of a given system (e.g., physical, technical, organizational, and cultural) that can be exploited by an adversary to adversely affect (cause harm or damage to) that system. *Intent* is the desire or motivation of an adversary to attack a target and to cause adverse effects. *Capability* is the ability and capacity to attack a target and to cause adverse effects. *Threat* denotes the *intent* and *capability* to adversely affect (cause harm or damage to) the system by adversely changing its states. A threat with adverse effects to a vulnerable system may lead to risk. (Throughout the rest of this article, the term *threat* will connote a threat with adverse effects.) *Resilience*, however, has been defined in the literature in many different ways. Consider, for example, the following definitions. (1) Resilience is the ability of a system to absorb external stresses.[2] (2) Resilience is a system capability to create foresight, to recognize, to anticipate, and to defend against the changing shape of risk before adverse consequences occur.[3,4] (3) Resilience refers to the inherent ability and adaptive responses of systems that enable them to avoid potential losses.[5] (4) Resilience is the result of a system (i) preventing adverse consequences, (ii) minimizing adverse consequences, and (iii) recovering quickly from adverse consequences.[6] (5) Resilience engineering is a paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success.[7]

The resilience of a system is a manifestation of the states of the system. Perhaps most critically, it is a vector that is time dependent. Resilience in this article is defined as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks.[8] Moreover, resilience is similar to vulnerability in that it cannot simply be measured in a single unit metric; its importance lies in the ultimate multidimensional outputs (the consequences) of the system for any specific inputs (threats). (Note that the consequence that is considered as part of the risk metric is in fact the output of the system model, and that the input of the system's model is parallel to the concept of threat.) Indeed, the risk associated with a cyber attack on a cyberinfrastructure system will depend not only on the resilience of the system but also on the type and sophistication of the cyber attack. This is because the resilience of a system can be measured only in terms of the specific threat (input) and the system's recovery time and the associated composite costs and risks. Thus, different attacks would generate different consequence (output) trajectories for the same resilient system.

Consider the immunization of a population against a major strain of a flu virus termed Type B. Assume that the population develops resilience for multiple strains of viruses of Type B, except for an evolving strain of Type A. In this case, even though the population might have resilience (immunity) for Type B, the appearance of strain A into this population will likely be infectious. Here, again, the risk to

* Address correspondence to Yacov Y. Haimes, Engineering Area Editor, L. R. Quarles Professor of Systems and Information Engineering, and Founding Director (1987) of the Center for Risk Management of Engineering Systems, University of Virginia, Fairfax, VA 22030, USA; tel: 434-924-3803; fax: 434-924-0865; haimes@virginia.edu.

the population from a threat is dependent on the type of threat, the resilience of the system, and the ability of the system to withstand that specific threat.

Similarly, consider any large-scale physical infrastructure such as electric power, transportation, or telecommunication. In any such complex system, the question "What is the resilience of infrastructure x?" is unanswerable because the question implicitly depends upon knowing whether infrastructure x would recover following any attack y within an acceptable time and composite costs and risks. Thus, the only way such a question can be answerable is when the threat (or a set of threats) is specifically identified. Indeed, the system's resilience is not merely an abstract attribute of the system; rather, it is a state of the system (composed of a vector of substates) for which any specific substate may respond differently to different inputs (threats). For example, a water distribution system may have redundancy in its electric power subsystem, and thus it may be resilient to a major storm that would shut down one of the power lines to the water distribution system, leaving the other redundant line intact. On the other hand, suppose the water distribution system depends on only one main pipe to supply water to its customers but is located in a region susceptible to earthquakes. The system is resilient only to the extent that the main pipe is functioning and can withstand an earthquake up to level 4 on the Richter Scale. However, the system would likely fail during an earthquake of level 5 or 6. Here, again, measuring the resilience of the water system is actually measuring the responses of the system to the specific threat, in this case the scale of the earthquake.

Furthermore, one may associate a vector of resilience with each subsystem. Thus, there can be a hierarchy of resilience attributes for any large-scale natural or constructed environment. For example, the human body as a system is made up of many subsystems (e.g., the digestive, pulmonary, auditory systems, etc.), each with a set of resilient organs and suborgans, where the level of such resilience depends on the input (physical or biological threats) and the output (a temporary or long-term loss of functionality of specific organs or suborgans). This example reinforces the thesis that system resilience can be measured in terms of the outputs for given inputs to the system. (Note that the inputs to the system, the states of the system, and the outputs are commonly time variant and probabilistic, as will be discussed subsequently.) To further appreciate the centrality of the system's input-output relationship to its resilience (states of the system), consider the fact that despite the resilience of the human body to various physical and biological attacks on it, its ultimate resilience depends upon the states of the body at the time as well as the type and strength of such attacks.

A system may also be characterized by its specific redundancy and robustness—both of which lead to a specific vector of resilience.[9,10] *Redundancy* refers to the ability of certain components of a system to assume the functions of failed components without adversely affecting the performance of the system itself. Of course, redundancies constitute an integral part of all safety-critical systems. *Robustness* refers to the degree of insensitivity of a system to perturbations or to errors in the estimates of those parameters affecting the design choice.

2. ON THE RELATIONSHIPS AMONG PREPAREDNESS, VULNERABILITY, AND RESILIENCE

Both vulnerability and resilience are manifestations of the states of the system. In principle, they are two sides of the same coin; vulnerability addresses only a system's protection, whereas resilience focuses also on a system's recovery following an adverse event. As states of the same system, both represent the capability of the system to withstand threats. On the one hand, vulnerability represents those states of the system that can be adversely affected by specific types and levels of magnitude of threats. On the other hand, resilience *also* represents the ability of the system to recover within an acceptable time and composite costs and risks, having been presented with a threat. That is, the vulnerability of a system does not provide information about the ability of the system to recover from a particular threat. What, then, is the relationship between preparedness and vulnerability, and what is the relationship between preparedness and resilience? If the primary objective of preparedness is reducing the vulnerability of a system to specific threats, it may (although not necessarily) also improve the resilience of the system to the same threats. For example, hardening a system against specific threat scenarios (e.g., adding more security by building fences or formulating policies and procedures that would limit access to infrastructures) but without addressing the recovery needs following a successful attack would reduce the vulnerability to such threat scenarios; it might not, however, necessarily improve the resilience of the system in terms

of its recovery time and composite costs and risks. For example, an electric power generation unit might be hardened against terrorist attacks or major natural hazards, thus reducing its vulnerability to such events, but such hardening would not necessarily improve its resilience to an acceptable level of recovery. By the same token, improving the resilience of the electric power supply system by adding redundant power lines crossing different geographical sites could ensure an acceptable level of resilience to the same threat, but it would not lessen the vulnerability of the electric power generation unit to a physical threat.

3. ON THE RELATIONSHIP BETWEEN RESILIENCE AND RISK

Improving a system's resilience offers significant advantages in managing risk; improving the resilience of a system constitutes an integral part of the risk management process. A fundamental benefit is that an acceptable level of residual risk to the system (i.e., an acceptable level of affordable safety) can be determined for each class of threat scenario. More specifically, because of the probabilistic nature of threats, given the occurrence of a class of threat scenarios, the outputs (consequences) are best represented with probability distribution functions. The resulting risks in terms of recovery time and composite costs can be calculated in a variety of ways, including the expected value of risks or the conditional expected value of risk of the extremes.[11] And ultimately, the tradeoffs among the various levels of risks and costs associated with each investment (e.g., through preparedness) in the system's resilience can be evaluated. The fact that the severity levels of the consequences resulting from a threat to a system are used as the metric with which the system's vector of resilience is evaluated—and given that the inputs and thus the outputs to the system are probabilistic in nature—necessarily leads to the following three basic questions in risk management: *What can be done and what options are available? What are the associated tradeoffs in terms of all relevant costs, benefits, and risks? What are the impacts of current decisions on future options?*[11,12] The answers to these questions, because they are so specific to each system and to each scenario, defy the ability to assign general and absolute scores to a system's resilience, as is discussed in the following section.

4. ON SCORING A SYSTEM'S RESILIENCE

The importance of resilience as a state of a system's capability to withstand forced changes to its organizational structure, functionality, and operational continuity has led to the development of capability metrics as surrogates for resilience. Indeed, several scoring systems for measuring the resilience of cyber systems are emerging. For example, Carnegie Mellon's Software Engineering Institute is developing a *Resiliency Engineering Framework* (REF),[13] which posits a vector of 21 capability areas that can be measured on a maturity scale that will demonstrate which cyber security and resilience practices can most effectively be integrated into common and frequent management decisions. The underlying notion is that if mature business processes are in place and if they appropriately integrate common decisions with security decisions, then the organization is more likely to see, understand, and respond to a cyber threat in a way that would reduce the consequences and minimize recovery time and costs.

On the other hand, attempts to characterize the resilience of a system with a specific numerical descriptor (as a metric) and to use this metric to compare the resilience of different systems could be misleading unless we pretend to assume that these different systems will be subjected to the same exact threats and the same exact levels of such threats with the same exact probabilities. Given the diversity of the functionality and the configurations of contemporary infrastructure systems (and in particular of cyber systems), and given the immense uncertainties associated with these differences and the threats to which any such system might be subjected, it is unreasonable to assign a numerical scale or number of resilience to any of these systems.

An important conclusion that can be drawn from the above discussion is that the resilience of a system might be measured in terms of the myriad sub-states that characterize that system for a specific time period and threats. It is an entirely different question, however, to project in the abstract the recovery time and composite costs and risks associated with any unspecified phantom set of threat scenarios. Here, again, the risk, as a measure of the probability and severity of adverse affects,[14] can be assessed only for a specific threat scenario at any given time.

Measuring the efficacy of a system's resilience might be achieved, for example, through the unique functionality of that particular system and its responses (outputs) to specific inputs. And given that

such inputs are probabilistic, so are the outputs, meaning that the system's resilience—because it is measured in terms of responses to the inputs—can be measured (quantified) only in probabilistic terms and for specific inputs. We can thus adduce the following premises for scoring resiliency:

1. The probabilistic nature of threats and thus of their associated outputs necessitates a holistic, multidimensional probabilistic scoring system of resilience. Furthermore, the myriad plausible threat scenarios, each with associated magnitude and duration, necessarily limit any such scoring system of resilience to specific classes of input threats.
2. Resilience, as a vector of the states of all physical and natural systems, is time variant; given the inherent characteristics of such systems, their resilience will deteriorate over time. Thus, even an input-limited scope of any scoring will be further constrained by the inherent time variant resilience of the system.

5. EPILOGUE

Resilience—complex and composite attributes of the states of a system—which commonly constitutes a vector of substates, cannot be characterized with a single numerical descriptor. Resilience must be understood and evaluated in the context of a probabilistic and dynamic set of input threat scenarios to the system and in terms of the complex set of associated consequences attached to any such threat.

ACKNOWLEDGMENTS

This article was inspired by my work on a cyber security project funded by the Institute for Information Infrastructure Protection (I3P) and the U.S. Department of Homeland Security.

REFERENCES

1. Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis, 2006; 26(2):293–296.
2. Holling CS. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 1973; 4(1):1–23.
3. Woods DD. Creating foresight: Lessons for resilience from Columbia. Pp. 289–308 in Farjoun M, Starbuck WH (eds). Organization at the Limit: NASA and the Columbia Disaster. Malden, MA: Wiley-Blackwell, 2005.
4. Woods DD. Essential characteristics of resilience. Pp. 21–34 in Hollnagel E, Woods DD, Leveson N (eds). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press, 2006.
5. Rose A, Liao S. Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. Journal of Regional Science, 2005; 45(1):75–112.
6. Westrum R. A typology of resilience situations. Pp. 49–60 in Hollnagel E, Woods DD, Leveson N (eds). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press, 2006.
7. Hollnagel E, Woods DD, Leveson N (eds). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press, 2006.
8. Haimes YY, Crowther KG, Horowitz BM. Homeland security preparedness: Balancing protection with resilience in emergent systems. Systems Engineering, 2006; 11(4):287–308.
9. Matalas NC, Fiering MB. Climate, Climatic Change, and Water Supply, Chapter III Panel on Water and Climate, Geophysics Study Committee, Geophysics Research Board, National Research Council Water-Resource Systems Planning. Washington, DC: National Academy of Sciences, National Research Council, 1977.
10. Haimes YY, Matalas NC, Lambert JH, Jackson BA, Fellows JFR. Reducing the vulnerability of water supply systems to attack. Journal of Infrastructure Systems, 1998; 4(4):164–177.
11. Haimes YY. Risk Modeling, Assessment, and Management, 3rd ed. New York: Wiley, 2009.
12. Haimes YY. Total risk management. Risk Analysis, 1991; 11(2):169–171.
13. Software Engineering Institute (SEI). CERT Resiliency Engineering Framework, Preview version, v0.95R, 2008. Available at: http://www.cert.org/resiliency_engineering/. Accessed on January 5, 2009.
14. Lowrance WW. Of Acceptable Risk. Los Altos, CA: William Kaufmann, 1976.