

Roadmap for Modeling Risks of Terrorism to the Homeland

Yacov Y. Haimes

Lawrence R. Quarles Professor of Systems and Information Engineering, Director, Center for Risk Management of Engineering Systems, Univ. of Virginia, Charlottesville, VA 22903.

Summary

The terrorist acts of September 11, 2001, were a wake-up call for changing our past practices in ensuring homeland security. The positive results of these changes, however, are accompanied by myriad visible and invisible risks. Accepting change implies assessing and managing these risks in a comprehensive and systemic fashion, avoiding an ad hoc approach. This paper offers a holistic risk assessment and management framework for modeling the risks of terrorism to the homeland. Two major interconnected systems are addressed: the homeland system and the terrorist networks system. In modeling the two systems, the centrality of state variables is highlighted. It is worth noting that the community of risk analysts has been developing and applying systems-based methodologies and tools for many years. The roadmap presented in this paper builds on the findings of many prior analyses.

Introduction

Numerous studies, including the report by the US National Intelligence Council, *Global Trends 2015* (NIC 2000), warn us of:

- the increased activities of terrorist networks and their quests to cause major casualties and disrupt our social fabric;
- the asymmetric wars that we may increasingly confront;
- “[t]he declining sovereignty and legitimacy of the nation-state as it struggles to respond to economic, social, and political challenges brought on by the information revolution” (Cope-land 2000);
- conflicts as seen in the past 5 years of peacekeeping and peace-making missions, where precision munitions, accurate intelligence; and reliable command and control play critical roles; and
- information technology attacks (e.g., viruses, hackers, and infrastructure attacks).

U.S. military and civilian security agencies cannot meet these present and future challenges, nor can they assess and manage the risks of terrorism to the homeland on an ad hoc basis. The risks to our national security and well-being are too dangerous. Quantitative risk assessment and management is vital, and it must rely on sound systems engineering and systems analysis principles and models. These must be capable of representing the essences of the *homeland*, the *terrorist networks*, and the *global geo-political environment*, each as a separate system, and of developing the causal relationships among them. Developing and deploying such a systemic modeling effort can forestall surprises to the designers and implementers of homeland security and help to evaluate the efficacy of risk management policy options in a dynamic, widely distributed, and uncertain environment.

Systems engineering is distinguished by its practical philosophy that advocates holism in cognition and in decision-making

(Haimes 1998). This philosophy is grounded on the arts, natural and behavioral sciences, and engineering and is supported by a complement of modeling methodologies, optimization and simulation techniques, data-management procedures, and decision-making approaches. Its ultimate purpose is: (1) building an understanding of the system’s nature, functional behavior, and interaction with its environment; (2) improving the decision-making process (e.g., in conception, planning, design, development, operation, and management); and (3) identifying, quantifying, and evaluating risks, uncertainties, and variability within the decision-making process. If the *system* is the homeland and one major *objective* is its protection, then we must seek to know and understand everything about the *state* of the system (leading to our understanding of its vulnerabilities) and about the *inputs* (threats from terrorism) to the homeland. To comprehensively assess the threats, and thus the corresponding risks, we must know the history, culture, mores, organization, decision-making processes, leadership, and other forces that characterize and motivate enemy and terrorist networks (Y. Haimes, paper presented at U.S. Military Academy Workshop, January 16, 2002).

The *gestalt* psychology/holistic philosophy common to two seemingly separate cross-disciplinary fields—risk and systems analysis—serves as a dominant common denominator that imbues synergy to both. The two disciplines span the arts, the humanities, the natural, social, behavioral, and organizational sciences, law, medicine, and engineering.

Centrality of State Variables in Modeling Risks to Homeland

Why do farmers irrigate crops during nonrainy seasons, and why do they add fertilizer? The fundamental answers are that a farmer irrigates crops to maintain an appropriate level of *soil moisture* and fertilizes the soil to maintain an appropriate level of *soil nutrients*. Soil moisture and soil nutrients are two important state variables (among others) that characterize the state of the farmer’s soil at any instant, determine the ultimate crop yield, and are affected and continuously modified by a plethora of factors (which are not necessarily mutually exclusive). These include decision variables (e.g., irrigation and fertilization), random variables (e.g., precipitation and other climate conditions), input (e.g., drainage and the quality of water flowing from upstream), output (e.g., crop yield), and exogenous variables (e.g., the price of water and fertilizer). Thus, to model the growth of the farmer’s crops, one ought to understand the causal relationships among all critical factors (variables) affecting the (state variables of the) farm and its output. Indeed, the state variables serve as the critical “bridge” between all the systems’ inputs and outputs and enable the systems analyst to model these interdependencies and interconnectedness. As an example, Fig. 1 shows the interdependencies between civilian and military infrastructures. In the same way, when modeling terrorist networks and homeland systems, knowledge of their representative state variables is essential. A sample of state variables that represent the essence of the homeland and terrorist networks is presented in Fig. 2 and will be discussed subsequently. For example, vulnerabilities are tightly related to the

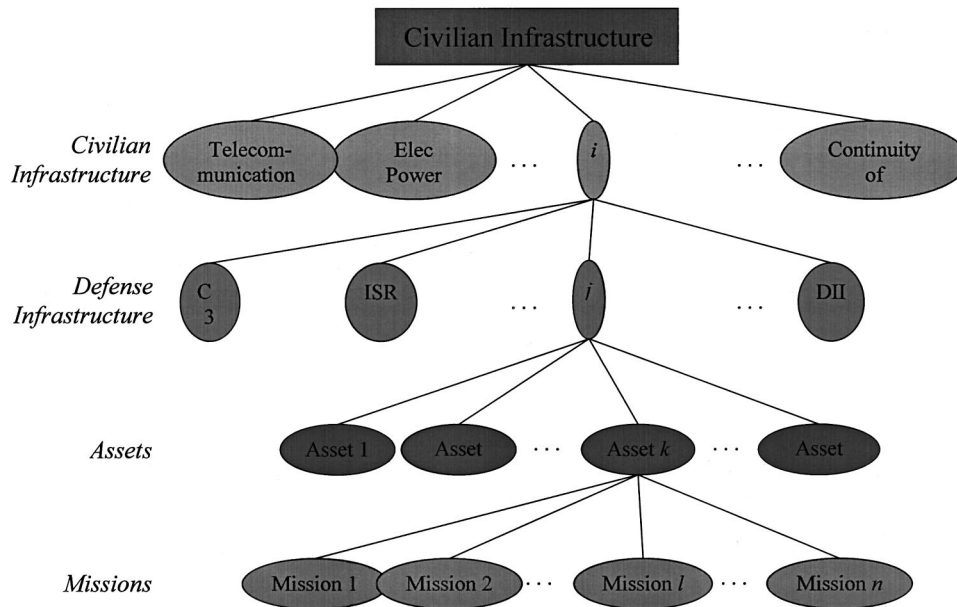


Fig. 1. Interdependencies among civilian and military infrastructures

state of the homeland—its open society and long borders—thus rendering the homeland at risk when it is threatened by terrorist networks. Similarly, the threats from terrorist networks constitute an input to the homeland. These can be understood and modeled only when we can identify and understand the societal environment as well as the geo-political dynamics within which terrorist networks are energized and operate (i.e., identifying and understanding the state variables of terrorist networks). Thus, the causal relationships between the inputs and outputs of the homeland and terrorist systems must be well understood in order to build models capable of predicting the efficacy of risk management policy options. Such options might include reengineering and realigning the design and implementation of both civilian and military institutional and organizational infrastructures to meet present and future risks and challenges.

Risk Modeling Process

If the adage “to manage risk, one must measure it,” constitutes the compass for risk management, then modeling constitutes the roadmap that guides the analyst throughout the journey of risk assessment. The process of risk assessment and management may be viewed through many spectacles, depending on one’s perspectives, vision, and circumstances. The first step in the risk assessment and management process is trying to identify all conceivable sources of risk. Four major categories of risk to the homeland can be identified (Fig. 2):

- Risk to human lives and to individual property, liberty, and freedom;
- Risk to organizational-societal infrastructures, and to the continuity of government operations, including the military and intelligence-gathering infrastructure;
- Risk to critical cyber-physical infrastructures; and
- Risk to economic sectors.

The *sine qua non* for a sound decision-making process is identifying these and other sources of risk to the homeland. This will enable the development of effective strategic and tactical planning to assess and manage (i.e., respond to) these risks. Hierarchical

holographic modeling (HHM), which has been effectively used on such problems as multidimensional modeling and risk identification, can be most useful here (Haimes 1981, 1998).

HHM is suggested by holography—the technique of lens-less photography. In the abstract, a mathematical model may be viewed as a one-sided image of the real system that it portrays. With single-model analysis and interpretation, it is quite impossible to clarify and document the sources of risk associated with the multiple components, objectives, and constraints of a complex system of systems, and also with its diverse societal aspects.

It follows that no single model can adequately represent the essence and perspectives of the homeland system of systems. Central to the HHM philosophy is the notion that understanding the interconnectedness and interdependencies within a large-scale system of systems can be achieved through multiple decompositions. Figs. 3 and 4 represent an example of an HHM that identifies a plethora of sources of risk associated with the military Joint Vision 2020 (Haimes et al., submitted for publication, 2002).

An extensive HHM-based decision support-system methodology was developed and tested with the National Ground Intelligence Center (NGIC) for Operations Other Than War (OOTW) (Dombroski 2001; Dombroski et al. 2002). This created a comprehensive risk-identification base that can be adapted, modified, extended, and deployed for homeland protection and security. Other applications of HHM for identifying risks of terrorism to the homeland include Lamm (2001), Mahoney (2001), Ezell (1998), and Watson (1998). Fitting hierarchical holographic modeling into the theory of scenario structuring can be found in Kaplan et al. (2001).

Modeling Terrorism Network System

Understanding terrorist networks as a system is essential, because its outputs *are* the same as the four sources of risk that constitute the input to the homeland system (Fig. 2). (Again, these are: risks to human lives and to individual property, liberty, and freedom; to organizational-societal infrastructures, and to the continuity of government operations, including the military and intelligence-

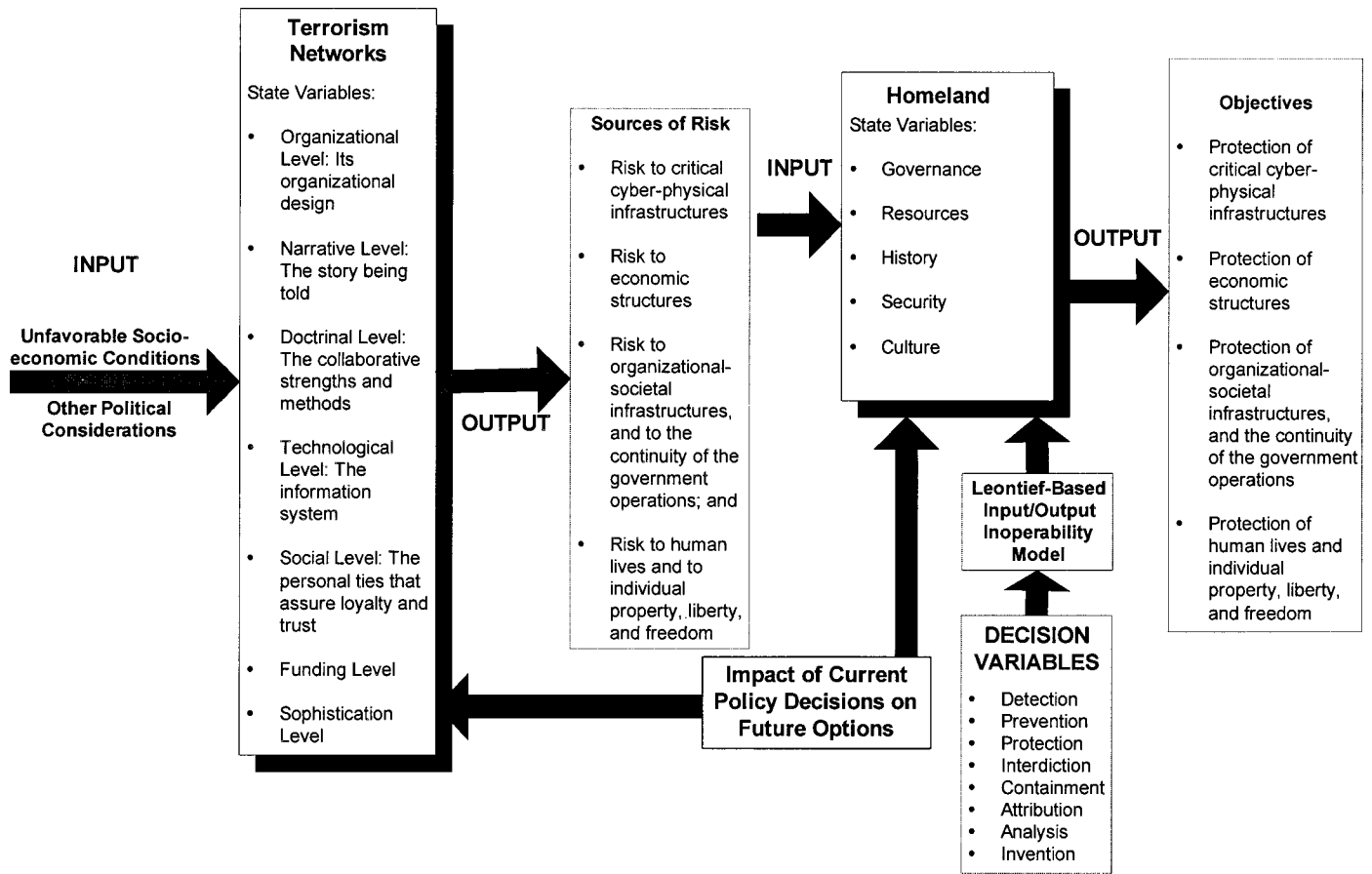


Fig. 2. Model of homeland and terrorist networks systems of systems

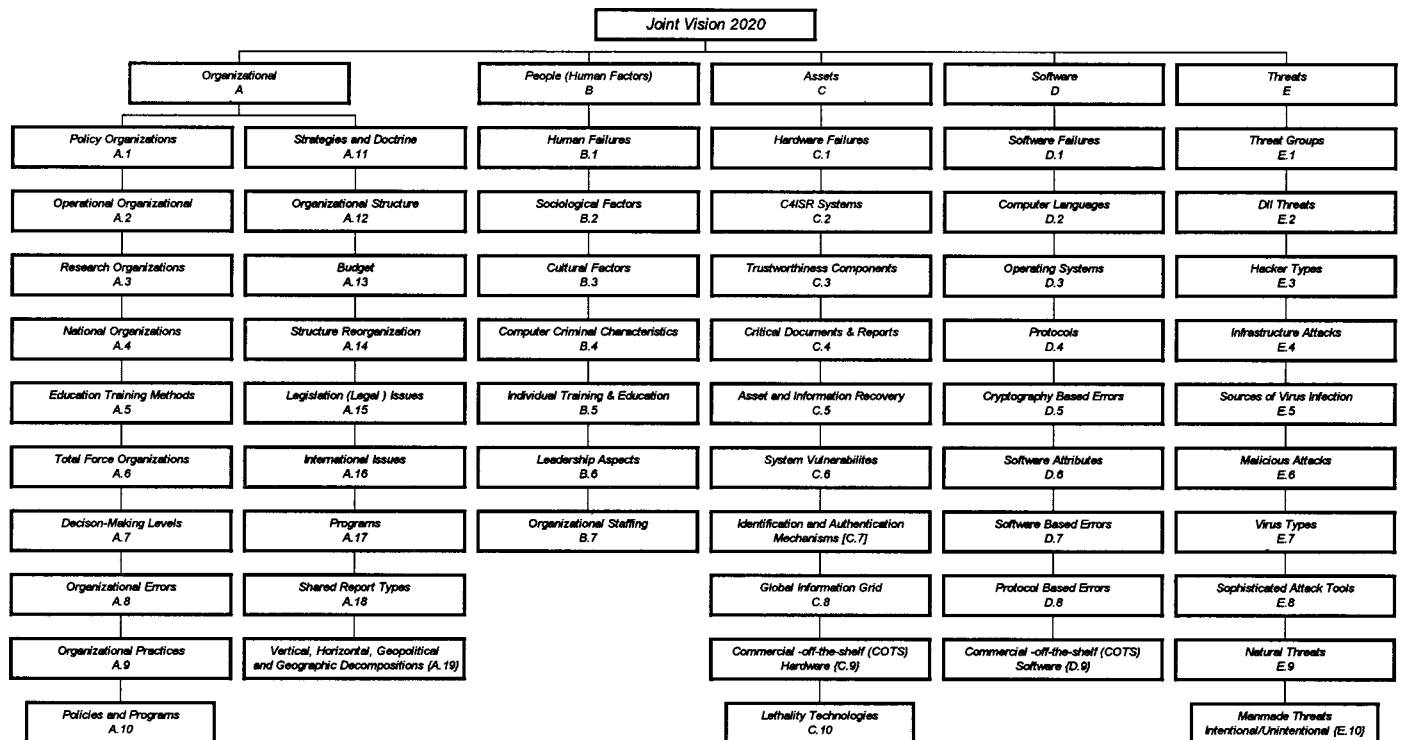


Fig. 3. JV 2020 hierarchical holographic modeling: Decomposition and identification of risks

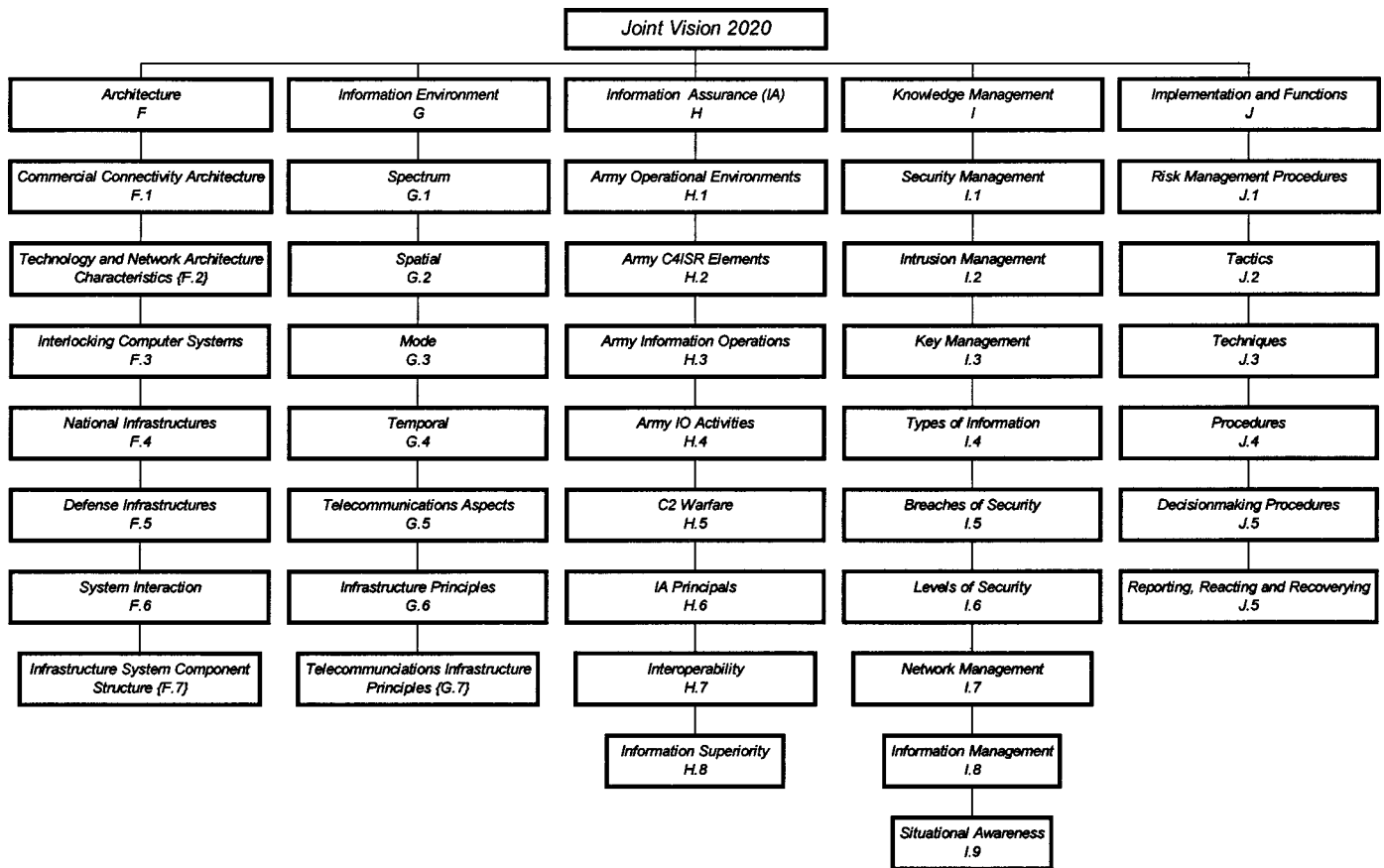


Fig. 4. Continuation of hierarchical holographic modeling for JV2020

gathering infrastructure; to critical cyber-physical infrastructures; and risk to the economic sectors.)

In their quest to better understand and appreciate the culture, motives, mode of operations, and bonding among terrorist networks, Arquilla and Ronfeldt (2001) identified the following “five levels of analysis,” which represents a sample of state variables for terrorist networks system (Fig. 2):

1. *Organizational level*—its managerial design. To what extent is a terrorist, or group of terrorists, organized into a network? And what does that network look like?
2. *Narrative level*—the story being told. Why have the members assumed a particular network form? Why do they remain in that form?
3. *Doctrinal level*—the collaborative strengths and methods. What doctrines exist for making best use of the network form of organization?
4. *Technological level*—the information system. What is the pattern of, and capacity for, information and communications flow within an organizational network? What technologies support them?
5. *Social level*—the personal ties that assure loyalty and trust. The full functioning of a network also depends on how well, and in what ways, the members are personally known and connected to each other.

These samples of state variables of the terrorist networks system model contribute to the comprehensive, holistic, and encompassing HHM effort to identify conceivable sources of risk to the homeland. They need to be complemented with additional state variables such as the funding level supporting the terrorist groups and the level of sophistication these groups can apply to develop-

ing specific actions. At the same time, it is imperative to identify the driving forces (input) that nourish and sustain these attributes of terrorist networks, such as unfavorable socioeconomic conditions or political considerations (Fig. 2).

By identifying and understanding the state variables that characterize the terrorist networks system, and the input to it, decision-makers can deploy effective preventive measures to manage and reduce the risks to the homeland. (One example would be investing funds and resources to mitigate the dire poverty and lack of educational opportunities in countries that spawn terrorists.)

Modeling Homeland System

Similar to those of the terrorist networks system model, the following is a sample set of five homeland state variables (Fig. 2):

- *Governance*—a free democratic society with a balanced three branches of government;
- *Resources*—strong economic, military, and organizational infrastructures with high scientific and technological advances, and appreciation of the arts and individual creativity;
- *History*—cyber, physical, organizational, societal, and domestic security infrastructures are *not* designed with terrorism in mind, allowing would-be terrorists an easy legal entrance to the homeland and access to its myriad infrastructures;
- *Security*—long borders that are easy to penetrate, a very large volume of imported goods stored in millions of containers, thousands of trucks transporting goods daily; and
- *Culture*—apopulation characterized by trust, acceptance of

foreigners, immigrants, diversity, support of the needy, and a devotion to public service, where everyone is innocent until proven guilty.

The above sample of state variables, which characterize the state of the homeland, can be instrumental in identifying critical sources of risk and generating risk management policy options that build on the output from the risk assessment process. Carter (2001) identifies the following eight risk management phases (decision variables) for homeland security and protection (Fig. 2):

- Detection,
- Prevention,
- Protection,
- Interdiction,
- Containment,
- Attribution,
- Analysis, and
- Invention.

Along with reengineering and realigning our civilian and military institutional and organizational infrastructures and investing funds and other resources abroad to alter the unfavorable conditions that spawn and nourish terrorist networks, implementing these phases can be instrumental in managing the risks of terrorism to the homeland cited earlier. Indeed, the output resulting from these phases are (Fig. 2):

- Protection of human lives and of individual property, liberty, and freedom.
- Protection of organizational-societal infrastructures, and the continuity of government operations, including the military and intelligence-gathering infrastructure;
- Protection of critical cyber-physical infrastructures;
- Protection of economic sectors; and
- Recovery contingency for unanticipated failures.

Global Geo-Political Dimension

To assess the risks to the homeland (as a system) and thus develop policy options to manage them, the analyst must address not only the terrorist networks as a system that affects the homeland, but also the global geo-political environment within which both systems operate. To do so, the assumptions made, the constraints, and other considerations (Slay, personal communication, 2001) must be articulated and made explicit. This would include the *assumptions* made on emerging technology and global socio-economic and political conditions, national goals and objectives, and the myriad military, financial, domestic, and political *constraints* and *other considerations* within which the homeland system operates. As an example, consider information technology and its ever-increasing impact on communications and reliability in the civilian and military sectors. Information assurance (IA), which is much more than information technology, *represents the trust that information presented by the system is accurate and properly represented; its measure of level of acceptable risk depends on the system's mission criticality* (Longstaff and Haimes 2002). In the military sector, Joint Vision 2020 (JV2020) commits the U.S. military to rely heavily on information technology and on information superiority in *command, control, communications, computers, intelligence, reconnaissance and surveillance* (C4ISR). However, this reliance on IT may provide the terrorist networks with opportunities to create a disproportionate amount of trouble (Haimes et al., unpublished, 2002; Lamm 2001).

Furthermore, global interconnectedness through the Internet and the ever-increasing use of supervisory control and data acqui-

sition (SCADA) systems to remotely operate our critical infrastructures through telecommunications networks, have rendered our information systems more vulnerable to intrusion and to the transmission of malicious misinformation and signals. Fortunately, the widely distributed nature of our systems makes it difficult for terrorist networks to disrupt all of them. By the same token, we might not be able to ascertain exactly which systems were attacked. Of particular concern are extreme events that can cause catastrophic results—rare, unanticipated, high-damage events—such as the use of weapons of mass destruction. It is essential to identify and manage all such critical sources of extreme and catastrophic risk (Haimes 1998).

Holistic Risk Assessment and Management Process

The entire process of risk assessment and management is essentially a synthesis and amalgamation of the empirical and the normative, the quantitative and the qualitative, and of objective and subjective evidence. It has built on contributions of individuals from diverse disciplines. For example, many of the theories, quantitative tools, and methods employed by risk analysts today have been developed primarily by mathematicians, statisticians, biostatisticians, health scientists, systems analysts, and systems engineers. At the same time, social, behavioral, and organizational scientists have markedly contributed to our understanding and appreciation of the human dimension of risk analysis, e.g., human perception, organizational and institutional barriers, communication, trust, and conflict resolution (Haimes 1998, 2001).

In risk assessment, the analyst often attempts to answer the following set of triplet questions:

1. What can go wrong?
2. What is the likelihood that it would go wrong?
3. What are the consequences? (Kaplan and Garrick 1981).

Answers to these questions help risk analysts to identify, measure, quantify, and evaluate risks and their consequences and impacts. Risk management builds on the risk-assessment process by seeking answers to a second set of three questions (Haimes 1991):

1. What can be done and what options are available?
2. What are the trade-offs in terms of all costs, benefits, and risks?
3. What are the impacts of current management decisions on future options?

Note that the last question is a critical one for managing the risks of terrorism to the homeland, as it is for any managerial decision-making. Policy decisions cannot be deemed “optimal” in any sense of the word unless the negative and positive impacts of current decisions on future options are assessed and evaluated (to the extent possible). Holistic risk management can be realized only when the above questions are addressed in the broader context of management and decision-making. *This means that costs, benefits, risks, and impacts of all viable options and their associated trade-offs are addressed within a hierarchical-multiobjective framework.* The feedback loop in Fig. 2 highlights the importance of assessing the impact of current policy decisions on future options and of their impacts on the state variables of terrorist networks and the homeland systems. A holistic risk management approach that harmonizes overall system management must also address the following four sources of failure: (1) organizational; (2) human; (3) hardware; and (4) software (Haimes 1991, 1998). This set of failure sources is intended to be internally comprehensive, i.e., comprehensive within the system's own internal environment. (External sources of failure are not discussed here be-

cause they are commonly system-dependent.) These four elements are not necessarily independent of each other, however. The distinction between software and hardware is not always straightforward, and separating human and organizational failures is often a difficult task.

Modeling Infrastructure Interdependencies

Historically, many critical national infrastructures were physically and logically separate systems. Today, the United States economy and civilian and military infrastructures are increasingly interdependent (Fig. 1). For example, transportation, banking and finance, telecommunications, and electric power are highly interdependent. Current critical infrastructures are marked by immense complexity characterized by interconnectedness, strong intra- and interdependencies, and multiple hierarchies. These characteristics have been intensified by the increasing use of advanced information technology spearheaded by the Internet. It has changed the landscape of our society just as the steam engine and telephone did long ago. Modeling interdependencies improves our ability to assess and manage the risks of terrorism to these infrastructures, and this has already become high on the national agenda.

The following is a brief summary of an inoperability model that builds on the economic input/output model developed by the Nobel Laureate, Wassily Leontief (Leontief 1951a,b, 1966). Although the inoperability model takes the same form of $\mathbf{x} = \mathbf{Ax} + \mathbf{c}$ as the Leontief model, the inputs and outputs in the two models are reversed and assume entirely different interpretations. The following elements of the Leontief-based input-output inoperability model are defined in Haimes and Jiang (2001):

- \mathbf{x} is an output vector of inoperability of the infrastructures of interest (i.e., its components are the inoperabilities of each infrastructure in the system);
- \mathbf{A} is the interdependency matrix (i.e., its elements express the degree to which the inoperability in one infrastructure depends upon the inoperability of other infrastructures); and
- \mathbf{c} is an input vector of perturbation (i.e., its components represent the inputs that cause an inoperability in those infrastructures that are directly attacked (e.g., by terrorist networks), and which can subsequently cause inoperabilities in other interdependent infrastructures through the interdependency matrix \mathbf{A}).

The linear system of equations $\mathbf{x} = \mathbf{Ax} + \mathbf{c}$ can be solved for the \mathbf{x} , given \mathbf{A} and \mathbf{c} , provided that \mathbf{A} is a stable matrix. Inoperability is defined as a level of dysfunctionality of an infrastructure that may be measured as a percentage of its operating capacity. Thus, inoperability is represented by the \mathbf{x} variables whose values fall between 0 and 1. An inoperability of 0 of the i th infrastructure means it operates flawlessly, while an inoperability of 1 means a complete failure. Perturbations in the form of terrorist attacks, accidental events, or natural causes contribute to inoperability. This model captures not only the resulting inoperability of the attacked infrastructures, but also the propagated inoperability caused by the coupling of the infrastructures. For example, a coal plant that experiences an attack will cause other infrastructures, such as power generation units, to become inoperable because of the degradation of the required supply of coal. The inoperability vector \mathbf{x} can be defined and measured not only in terms of the production of physical outputs (e.g., commodities), but also in infrastructure performance, such as quality of service.

One of the central challenges in inoperability modeling is determining the interdependency matrix \mathbf{A} , whose elements express

the interdependencies between pairs of infrastructures. Determining the interdependency from first principles is not a trivial problem. Work is underway exploring the possibility of generating this matrix from available economic data collected and analyzed by the Bureau of Economic Analysis (BEA) of the U.S. Department of Commerce. This requires understanding the correspondence between the original Leontief model and the corresponding economic parameters, namely the elements of the inoperability \mathbf{A} matrix.

Beyond Quantitative Risk Assessment and Management

State variables and modeling efforts guide quantitative analyses and add to them substance, reality, and effectiveness, but quantitative analyses must be supplemented and complemented by normative-qualitative analyses as well. Quantitative risk assessment and management is only a necessary condition for effective management and decision-making. (The term quantitative connotes here a mathematical process and not necessarily an analytical one.) Because some of the state variables of terrorist networks and the homeland are qualitative in nature, they cannot be addressed through mathematical-empirical tools alone. This is harmonious with the premise that systems engineering and systems analysis (and thus risk analysis) are based on a holistic philosophy that is grounded on the arts, natural and behavioral sciences, and engineering, that is, on empirical-quantitative and normative-qualitative analyses.

The emerging critical importance of knowledge management is another example of added complexities and interdependencies that are introduced by our ever-increasing use of information technology (Davenport and Prusak 1998). However, the challenges, and thus the emerging risks, are based only partially on technology. Many other factors significantly impede communications and knowledge management (Haimes et al., unpublished, 2002). These include: turf protection, the lack of cooperative trust, and severe competition over scarce resources among the various civilian and government agencies and military branches. Such obstacles have become the enemy from within.

Epilogue

The homeland and its myriad economic, organizational, institutional, and other sectors constitutes a complex large-scale system of systems. The same applies to terrorist networks and to the global socio-economic and political environment. Each is composed of numerous interconnected and interdependent cyber, physical, and organizational infrastructures (subsystems). The relationships among these subsystems are dynamic (i.e., ever-changing with time), nonlinear (defeating a simplistic modeling schema), and spatially distributed (agents and infrastructures that may have some overlapping characteristics are spread all over the world). All of these factors make their management difficult, at best. These systems are managed or coordinated by multiple government agencies, corporate divisions, and decision-makers, with different missions, resources, timetables, and agendas that are often in competition and conflict. Because of the above characteristics, human and organizational errors and failures are common. Risks of extreme and catastrophic events facing this complex and large-scale system of systems, are of critical importance. Clearly, any attempt to assess and manage these myriad risks on an ad hoc basis is unlikely to succeed. Thus, systems modeling is imperative.

The modeling roadmap presented in this paper provides principles and guidelines for the challenging journey of modeling the risks of terrorism to the homeland. It is based on many years of model development and application by a community of analysts focused on how best to approach real-world problems of risk assessment and management. By their nature, principles and guidelines are not a substitute for “the real thing.” Models are built to address and provide answers to specific questions, but no single model can ever capture and represent all the essence of large-scale systems. Nor can a single model answer all the needs of analysts and decision makers. As discussed earlier, hierarchical holographic modeling is one attempt to capture the multifarious dimensions and perspectives of a system through a holistic model.

The state variables presented for the homeland and terrorist networks systems, as well as the other inputs and variables, should not be considered inclusive. Rather, they serve as guidelines for those who will take up the challenge of modeling this complex system of systems and then use that model to develop effective responses to terrorism.

Acknowledgments

This editorial draws on an unpublished keynote presentation titled *Guidelines for a Holistic Risk Assessment and Management Framework for Future Combat System*, at the US Military Academy’s Workshop “Building Achilles: Assessing the Vulnerabilities of the Future Combat System,” West Point, New York, January 16, 2002. Thanks to my colleagues Barry Horowitz and Jim Lambert for carefully reading a draft of this paper and for their valuable comments and suggestions. Thanks also to Grace Zisk for her technical editorial assistance and to Della Dirickson for her administrative assistance.

References

- Arquilla, J. and Ronfeldt, D. (2001). *Networks and netwars*, National Defense Research Institute, Rand, Pittsburgh.
- Carter, A. B. (2001). “The architecture of government in the face of terrorism.” *Int. Security*, 23(3), 5–23.
- Copeland, T. E. (2000). “The information revolution and national security.” Strategic Studies Institute, U.S. Army War College, Washington, D.C.
- Davenport, T. H., and Prusak, L. (1998). *Working knowledge: How organizations manage what they know*, Harvard Business School Press, Boston.
- Dombroski, M. (2001). “A risk-based decision support methodology for operations other than war (OOTW).” MS thesis, Systems Engineering Dept., Univ. of Virginia, Charlottesville, Va.
- Dombroski, M. J., Haimes, Y. Y., Lambert, J. H., Schluskel, K., and Sulcoski, M. (2002). “Risk-based methodology for support of operations other than war.” *Military Oper. Res. J.*, 7(1), 19–38.
- Ezell, B. C. (1998). “Risks of cyber attack to supervisory control and data acquisition for water supply.” MS thesis, Systems Engineering Dept., Univ. of Virginia, Charlottesville, Va.
- Haimes, Y. Y. (1981). “Hierarchical holographic modeling.” *IEEE Trans. Syst. Man Cybern.*, 11(9), 606–617.
- Haimes, Y. Y. (1991). “Total risk management.” *Risk Anal.*, 11(2), 169–171.
- Haimes, Y. Y. (1998). *Risk modeling, assessment, and management*, Wiley, New York.
- Haimes, Y. Y. (2001). “Risk analysis, systems analysis, and Covey’s seven habits.” *Risk Anal.*, 2(2), 217–224.
- Haimes, Y. Y., and Jiang, P. (2001). “Leontief-based model of risk in Complex interconnected infrastructures.” *J. Infrastruc. Syst.*, 7(1), 1–12.
- Kaplan, S., and Garrick, B. J. (1981). “On the quantitative definition of risk.” *Risk Anal.*, 1(1), 11–27.
- Kaplan, S., Haimes, Y. Y., and Garrick, B. J. (2001). “Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk.” *Risk Anal.*, 21(5), 807–819.
- Lamm, G. A. (2001). “Assessing and managing risks to information assurance: A methodological approach.” MS thesis, Systems Engineering Dept., Univ. of Virginia, Charlottesville, Va.
- Leontief, W. W. (1951a). “Input/output economics.” *Sci. Am.*, 185(4).
- Leontief, W. W. (1951b). *The structure of the American economy, 1939*, 2nd Ed., Oxford University Press, New York.
- Leontief, W. W. (1966). *Input output economics*, Oxford University Press, New York.
- Longstaff, T. A., and Haimes, Y. Y. (2002). “A holistic roadmap for survivable infrastructure systems.” *IEEE Trans. Syst., Man Cybern.*, in press.
- Mahoney, B. (2001). “Quantitative risk analysis of GPS as a critical infrastructure for civilian transportation applications.” MS thesis, Systems Engineering Dept., Univ. of Virginia, Charlottesville, Va.
- NIC. (2000). *Global Trends 2015*, National Intelligence Council Access available via PURL (<http://www.cia.gov/cia/publications/globaltrends2015/index.html>).
- Watson, R. L. (1998). “Risk analysis of the physical vulnerabilities of hydroelectric power plants.” MS thesis, Systems Engineering Dept., Univ. of Virginia, Charlottesville, Va.