SANDIA REPORT
SAND2008-5381
Unlimited Release
Printed August 2008

Metaphors for Cyber Security

Thomas H. Karas, Judy H. Moore, and Lori K. Parrott

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2008-5381
Unlimited Release
Printed August 2008

Metaphors for Cyber Security

Thomas H. Karas and Lori K. Parrott
Strategic Studies Group
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0839

Judy H. Moore
Contractor to Strategic Studies Group

Abstract

This report is based upon a workshop, called "CyberFest," held at Sandia National Laboratories on May 27-30, 2008. Participants in the workshop came from organizations both outside and inside Sandia. The premise of the workshop was that thinking about cyber security from a metaphorical perspective could lead to a deeper understanding of current approaches to cyber defense and perhaps to some creative new approaches. A wide range of metaphors was considered, including those relating to: military and other types of conflict, biological, health care, markets, three-dimensional space, and physical asset protection. These in turn led to consideration of a variety of possible approaches for improving cyber security in the future. From the proposed approaches, three were formulated for further discussion. These approaches were labeled "Heterogeneity" (drawing primarily on the metaphor of biological diversity), "Motivating Secure Behavior" (taking a market perspective on the adoption of cyber security measures) and "Cyber Wellness" (exploring analogies with efforts to improve individual and public health).

Acknowledgements

The workshop organizers wish to thank, first, the participants who shared their time and ideas with each other and with us, providing the substance for this report. In addition, Steve Burbeck, Neil Rowe, Anil Somayaji, and Fred Yen kindly reviewed and commented on the draft. Also essential contributors were those who shared in session facilitating duties: John Cummings, Wendell Jones, and Steve Rinaldi. Providing essential records of the discussions were note-takers Kathryn Hanselmann, Ed Talbot, Ricky Tam, and Drew Walter. (In late stages, Rinaldi and Talbot were also full participants.)The workshop would not have been possible without the dedicated administrative support provided by Shanann Candelaria, Alicia Cloer, June Smith, and Sharon Lemm. We are also grateful for the assistance of Audra Johnson and Nicole Herschler. Last but not least, our thanks to the official host and sponsor of the event, Rob Leland.

Contents

Preface

This report is based upon a workshop, called "CyberFest," held at Sandia National Laboratories on May 27-30, 2008. The event was organized by the Strategic Studies Department, Strategic Foundations Organization, Institutional Development Center of Sandia. It was formally hosted by Robert Leland, Director of Computing and Network Services, and held in support of a strategic planning effort he was leading. Participants in the workshop came from organizations both outside and inside Sandia; background information on the participants can be found in an appendix to the report.

Beginning on the evening of May 27, and continuing through May 28 and 29, participants joined a variety of activities—written, simultaneous "brainstorming," sub-divided working team deliberations, and full-group discussions—all designed to elicit creative thinking about the problems of cyber security. These activities were held on an unclassified basis, with a smaller, security-cleared subset of participants remaining on May 30 for further, classified discussions. (This report is based on the unclassified discussions; a separate, short classified annex will also be issued.) The working theme was the use of metaphors in thinking about cyber security; the rationale for this theme is explained in the body of the report.

The report is not a transcript of the workshop proceedings, but a paper derived from written materials produced and notes taken during the workshop, post-workshop comments on the draft from participant-reviewers, and some supplemental analysis and references. Workshop participants were promised individual non-attribution to encourage frankness, but whatever is useful in the report can be credited to their contributions.

Lori Parrott managed the workshop preparations, both substantively and administratively. Judy Moore led development of the workshop design and agenda and helped organize the output for use in the report. Tom Karas drafted the report.

Executive Summary

This report is based upon a workshop, called "CyberFest," held at Sandia National Laboratories on May 27-30, 2008. Participants in the workshop came from organizations both outside and inside Sandia. The premise of the workshop was that thinking about cyber security from a metaphorical perspective could lead to a deeper understanding of current approaches to cyber defense and perhaps to some creative new approaches.

As Lakoff and Johnson concluded in 1980, metaphorical thought is unavoidable, ubiquitous, and mostly unconscious. Exploration of the metaphors we use in the cyber security domain may help improve our thinking and discussion in four ways. First, we may gain a clearer understanding of the value and limitations of the concepts we have mapped from other domains into the cyber security domain. Second, trying out less common or new metaphors may feed the imagination of researchers and policy developers. Third, metaphors that work particularly well might be developed into a whole new models or sets of concepts for approaching cyber security problems. Fourth, a metaphor serves a heuristic purpose -- bringing clearer understanding of abstract concepts from the field of cyber security into domains with which the non-specialist may be more familiar.

Workshop participants considered four scenarios illustrating difficult threat-related problems of information confidentiality, integrity, and availability. These scenarios included exploitation of a software vulnerability leading to loss of information services in a large company, large-scale theft of proprietary information by a company employee, loss of a valuable oil exploration submersible traced to design and test errors traced to (intentionally?) flawed hardware and software, and an un-attributable network attack leading to disasters in an air traffic control system. These scenarios illustrated not only a set of security issues, but also the influence that implicit metaphors and issue framing can have on problem definitions and solutions.

Next, a wide range of metaphors was considered, including those relating to military and other types of conflict, biological, health care, markets, three-dimensional space, and physical asset protection. Metaphor examples that participants discussed include fortress, cops and robbers, warfare, complex adaptive systems, ecosystem biodiversity, immune systems, programmed cell death, disease prevention and health care, market incentives, risk management, outer space, the US western frontier, the global environment, banking, games, martial arts, and military deterrence.

Discussion of these in turn led to consideration of a variety of possible approaches for improving cyber security in the future. From the proposed approaches, three were formulated for further discussion.

An approach labeled "Heterogeneity" drew primarily from the metaphor of biological diversity. Computer systems may fail because of hardware software flaws that emerge only when particular, unforeseen system states are reached—in analogy to natural catastrophes in ecosystems—and homogeneous systems are more likely to fail completely. Similarly, computer networks in which all the components have the same vulnerabilities are easier for attackers to bring down, but more diverse systems would deprive attackers of sufficient target

knowledge to do as much damage. What is more, systems comprising diverse hardware and software components would make it easier to confuse and deceive attackers.

It can thus be argued that diversity is one of the ways of "baking" security into systems—designing them from the start to be more secure, as opposed to adding on security measures later. Moving toward more diverse systems would require both technical and policy advances. Technically, human designed systems tend to converge to uniformity. Therefore, there is a need for new ways of creating software (and perhaps hardware components) that automatically introduce diversity.

A second approach, "Motivating Secure Behavior," took a market perspective on the adoption of cyber security measures. The central concept is that many of the vulnerabilities in current systems can be traced to human behaviors shaped by the structure of incentives facing both suppliers and users of information technology. Therefore, the overall task is to make it easier for people to do the "right" thing and harder to do the "wrong" thing. Responsibilities (and therefore incentives) should be developed for and by different system levels and actors: Individuals (e.g., US consumers, managers); Institutions (e.g., Microsoft, Universities); Government agencies (e.g., DOE, Sandia); Public Policy (e.g., Congress, Executive Branch, Agencies, Courts, States); and Standards bodies/associations.

A disadvantage of this focus is that it is vague about exactly what technologies developers, vendors, buyers, and users should be "incentivized" to create, sell, buy, and use.

The third approach was called "Cyber Wellness," exploring analogies with efforts to improve individual and public health. Its objective is to keep the population (of users and networked systems) as healthy as possible: resistant to attacks, resilient under stresses, wary of dangerous environments, treatable if diseased, and able to limit contagions. Much responsibility for personal (local) wellness depends on individuals, but various levels of corporate and public health management, from the local to the international, are equally important. Numerous analogies emerged between human wellness mechanisms and institutions on the one hand and actual or potential cyber security arrangements on the other.

An advantage of this approach is that it encourages thinking about the interactions of all the components at all levels of the "health" maintenance system, ranging from the individual who practices risky or less risky behaviors to the institutions who analyze, model, financially underwrite, or incentivize behaviors. For these discussions, however, the group developing the approach chose to pursue a vision of the future of computing in which users are represented by "avatars," or mobile software agents whose "health" is monitored and maintained. In this way, each user has a direct incentive to keep his or her avatar in good health. Security is a distributed, rather than centralized, function. Although the "avatar" vision does imply a new approach to "baking" security into the computer networking systems of the future, it is also true that mobile software agents and the computers that host them face a number of security challenges of their own.

Some final observations of workshop participants were that those responsible for setting future directions for cyber security need to have a bold vision; develop a gradual adoption/implementation strategy; accept and sustain a strategy through the inevitably

gradual and evolutionary process that will ensue; and show benefits for users and operators, not just push solutions that aren't seen as beneficial outside the security world.

I. Why Metaphors?

Metaphor may commonly be dismissed as a subject relevant only for humanities scholars or literary critics, but not as one particularly relevant for specialists in cyber security. The premise of the workshop reported here, however, was that thinking about cyber security from a metaphorical perspective could lead to a deeper understanding of current approaches to cyber defense and perhaps to some creative new approaches.

Nearly 30 years ago, linguists George Lakoff and Mark Johnson began a book by arguing that:

> Metaphor is for most people a device of the poetic imagination and the rhetorical flourish—a matter of extraordinary rather than ordinary language...most people think they can get along perfectly well without metaphor. We have found, on the contrary, that metaphor is pervasive in everyday life, not just in language but in thought and action. Our ordinary conceptual system, in terms of which we both think and act, is fundamentally metaphorical in nature.[1]

Among their conclusions were:

- Conceptual metaphors are grounded in everyday experience.
- Abstract thought is largely metaphorical.
- Metaphorical thought is unavoidable, ubiquitous, and mostly unconscious.
- Our conceptual systems are not consistent overall, since the metaphors used to reason about concepts may be inconsistent.
- We live our lives on the basis of inferences we derive via metaphor.[2]

Much of the remainder of this report will illustrate these points.

Given that metaphor is our dominating theme, it may be useful to offer a definition of metaphor. One scholar proposes the following:

> In the cognitive linguistic view, metaphor is defined as understanding one conceptual domain in terms of another conceptual domain...Examples of this include when we talk and think about life in terms of journeys, about arguments in terms of war, about love also in terms of journeys, about theories in terms of buildings, about ideas in terms of food, about social organizations in terms of plants, and many others. A convenient shorthand way of capturing this view of metaphor is the following: CONCEPTUAL DOMAIN (A) IS CONCEPTUAL DOMAIN (B), which is what is called a conceptual metaphor. A conceptual metaphor consists of two conceptual domains, in which one domain is understood in terms of another. A conceptual domain is any coherent organization of experience. Thus, for example, we have coherently organized knowledge about journeys that we rely on for understanding life.[3]

---

[1] *Metaphors We Live By* (Chicago: University of Chicago Press, 2003), p. 3. Originally published in 1980.

[2] Op.cit., pp. 272-273.

[3] Zoltán Kövecses, *Metaphor: a Practical Introduction* (New York: Oxford University Press, 2002), pp. 4-6.

In fact, the very notion of "cyber space" is itself a metaphor, and most concepts relating to cyber security have been "mapped" into that realm from other domains.

Conscious awareness of the metaphors we use in the cyber security domain may help improve our thinking and discussion in four ways. First, we may gain a better understanding of the value and limitations of the concepts we have mapped from other domains into the cyber security domain. For example, Deborah Frincke and Matt Bishop have pointed out that in the computer security field,

> ...the original and most commonly used metaphor is the computer (or network) as a fortress, the walls of which must be guarded against potential breaches. This metaphor is useful, but like all metaphors, it is not precise. Understanding the differences between the metaphor of a fortress and the realities of securing a system is crucial to students understanding the subtleties of computer security.[4]

Second, trying out less commonly used metaphors may feed the imagination. Analogies from other domains that seem to apply to cyber security may lead to new ideas for solving problems. Even analogies that don't work well may suggest other ones that work better. For example, one workshop participant pointed out that a cyber "fortress" may have a moat and strong walls, but may also have wires running underneath the walls and carrying out the information that is supposed to be protected. Plus, additional, new kinds, of defensive measure may be necessary. This is what is considered an ampliative use of metaphor.

Third, metaphors that work particularly well might be developed into whole new models or sets of concepts for approaching cyber security problems. This possibility is illustrated in Section IV below. Fourth, a metaphor can work as a communication tool--bringing abstract concepts from the field of cyber security into domains with which the non-specialist may be more familiar. A metaphor may heuristically help computer users understand why they should follow certain protective procedures. Or, a particularly powerful metaphor might help public policy makers understand how a new cyber security program would work, and why it is important that they should support it.

Examples of all four of these potential benefits emerged during the workshop.

II. Observations on Threats to Cyber Security

The range of potential threats in the cyber world is as wide as our use of information technology. (See Box 1 for a broad survey of the dangers.) Generally speaking, the literature on cyber security usually refers to three characteristics of information systems that need protection:

---

[4] "Guarding the Castle Keep: Teaching with the Fortress Metaphor," IEE Security & Privacy, May/June 2004, p. 69, available at http://ieeexplore.ieee.org/iel5/8013/29015/01306975.pdf.

1. Confidentiality—privacy of information and communications. In government this might mean, for example, assuring access to classified information only by authorized individuals. In commerce, it might mean the protection of proprietary information.

2. Integrity—assurance that information or computing processes have not been tampered with or destroyed. In the case of critical infrastructures (say, for example, the power grid), loss of data integrity could take the form of destructive instructions to the system resulting in financial, material, or human losses.

3. Availability—assurance that information or services are there when needed. Denial of service attacks, which overload system servers and shut down websites, are examples of interfering with availability.

Box 1: Cyber Security Threats

WHAT IS AT STAKE

Information technology (IT) is essential to the day-to-day operations of companies, organizations, and government. People's personal lives also involve computing in areas ranging from communication with family and friends to online banking and other household and financial management activities. Companies large and small are ever more reliant on IT to support diverse business processes, ranging from payroll and accounting, to tracking of inventory, operation of sales, and support for research and development (R&D)-that is, IT systems are increasingly needed for companies to be able to operate at all. Critical national infrastructures -- such as those associated with energy, banking and finance, defense, law enforcement, transportation, water systems, and government and private emergency services -- also depend on IT-based systems and networks; of course, the telecommunications system itself is a critical infrastructure for the nation. Such dependence on IT will grow. But in the future, computing and communications technologies will also be embedded in applications in which they are essentially invisible to their users. A future of "pervasive computing" will see IT ubiquitously integrated into everyday objects in order to enhance their usefulness, and these objects will be interconnected in ways that further multiply their usefulness. In addition, a growing focus on innovation in the future will require the automation and integration of various services to provide rapid response tailored to the needs of users across the entire economy.

The ability to fully realize the benefits of IT depends on these systems being secure -- and yet nearly all indications of the size of the threat, whether associated with losses or damage, type of attack, or presence of vulnerability, indicate a continuously worsening problem. Moreover, it is almost certainly the case that reports understate the actual scope of the threat, since some successful attacks are not noticed and others noticed but not reported.

The gaps between commercial practice and vulnerabilities in critical infrastructure are still wide. Meanwhile, the ability of individuals, organizations, or even state actors to attack the nation's institutions, its people's identities, and their online lives in cyberspace has grown substantially. Industry trends toward commoditization have resulted in clear targets for focused attacks, making coordinated attacks by hundreds of thousands of co-opted cooperating agents practical for the first time in history.

Cont'd next page

The potential consequences of a lack of security in cyberspace fall into three broad categories. First is the threat of catastrophe -- a cyber attack, especially in conjunction with a physical attack, could result in thousands of deaths and many billions of dollars of damage in a very short time. Second is frictional drag on important economic and security-related processes. Today, insecurities in cyberspace systems and networks allow adversaries (in particular, criminals) to extract billions of dollars in fraud and extortion -- and force businesses to expend additional resources to defend themselves against these threats. If cyberspace does not become more secure, the citizens, businesses, and governments of tomorrow will continue to face similar pressures, and most likely on a greater scale. Third, concerns about insecurity may inhibit the use of IT in the future and thus lead to a self-denial of the benefits that IT brings, benefits that will be needed for the national competitiveness of the United States as well as for national and homeland security.

THE BROAD RANGE OF CAPABILITIES AND GOALS OF CYBERATTACKERS

A very broad spectrum of actors, ranging from lone hackers to major nation-states, poses security risks to the nation's IT infrastructure. Organized crime (e.g., drug cartels) and transnational terrorists (and terrorist organizations, perhaps state-sponsored) occupy a region in between these two extremes, but they are more similar to the nation-state than to the lone hacker.

High-end attackers are qualitatively different from others by virtue of their greater resources -- money, talent, time, organizational support and commitment, and goals. These adversaries can thus target vulnerabilities at any point in the IT supply chain from hardware fabrication to end uses. Furthermore, they are usually highly capable of exploiting human or organizational weaknesses over extended periods of time. The bottom line is that the threat is growing in sophistication as well as in magnitude, and against the high-end attacker, many current best practices and security technologies amount to little more than speed bumps -- thus requiring additional fundamental research and new approaches, such as a greater emphasis on mitigation and recovery.

Seymour E. Goodman and Herbert S. Lin, eds., Toward a Safer and More Secure Cyberspace (Committee on Improving Cybersecurity Research in the United States, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies (Washington: National Academies Press, 2007), pp. 2-3. Available at http://www.cyber.st.dhs.gov/docs/Toward_a_Safer_and_More_Secure_Cyberspace-Full_report.pdf

To encourage some concreteness in metaphorical discussions of cyber security, four scenarios of cyber security problems were presented to the workshop participants. Each of these scenarios essentially represented one or more of the above three cyber security risks, although they were not framed that way. What turned out to be interesting about the scenarios was that they not only illustrated the kinds of problems that cyber security personnel worry about, but they also illustrated two important characteristics of the much of the discourse on this subject (as well as most discourse on most subjects). That is, first, **metaphors are hard to avoid, even if we are not consciously using them**. Second, **how a problem is framed frequently implies certain kinds of solutions, while implicitly reducing the likelihood that others will be considered.**

Scenario I: “Zero-Day Attack”

Cyber Challenge–Detecting the Zero Day Attack

- *A Fortune 500 company has critical information needs – customer data, its R&D data, manufacturing information, human resources data, …*
- *Without 24/7 access to its information, the company would collapse – its survival depends upon instant access to its information*
- *The company takes all appropriate security measures and follows established and recommended best practices to secure its information:*
  - *Regular backups*
  - *Patches and software upgrades*
  - *Access controls*
  - *Updated and enforced information security policies*
  - *…*
- *In May 2009, the company’s access to its information is mysteriously and instantaneously cut, records are damaged and destroyed, its IT department is overloaded…and the company fights for its survival*
- *CNN reports a hitherto unknown and extremely subtle software flaw was exploited by unknown attackers in companies across the nation, with severe economic repercussions*

In this scenario, the victims lose *availability* of their information (and, if the record damage is permanent, loss of *integrity* as well). The idea of “zero day” is that attackers are able to discover and exploit the hidden vulnerability before the victims can learn about and fix it. The mystery of the origins of the attack leaves open a range of metaphors: are the attackers vandals, industrial saboteurs, thieves, terrorists, or a national military preparing for some broader conflict? Because known “best practices” cannot detect the vulnerability in advance, and because the attack comes without warning, the implied solutions would seem to fall into two categories:

a. build future information systems that are somehow inherently less prone to such vulnerabilities, or

b. build resiliency or redundancy into existing systems so that they might fail more gracefully and recover more easily.

During the workshop, category “a)” received more discussion.

Cyber Challenge Scenario–Insider Threat

Tightly controlled design criteria of a field programmable gate array (FPGA) used in various fly-by-wire systems have appeared inappropriately in various research papers and other documents. The Air Force is very concerned that defense contractor information and project security have serious gaps and may have contributed to this loss of information.

Conditions at this defense contractor set up tremendous pressures on employees.

- *People are constantly switching projects, there is no management continuity, and people are having to work overtime and weekends to meet deadlines.*
- *IT support is being curtailed and projects are being asked to deliver ahead of schedule and under cost.*

A recent newspaper article details a story that is troublesome in this environment:

- *An employee of a New York-based firm used a flash drive to steal hundreds of original designs.*
- *What tipped off the company to the culprit's identity was a computer trail indicating that the massive data download coincided with the moment an external drive was attached to the suspect's terminal.*
- *A couple of decades ago, you would have had to stand by a copying machine for hours to accomplish that. Now, it only takes a few minutes.*

The implied metaphor in the second scenario is that of the fortress holding valuable items that are stolen by a person inside the fortress. The loss in this scenario is that of *confidentiality* of information. A useful observation to be made about this scenario is that while it is possible to imagine technologies that make it more difficult to do the "wrong" thing (thus far, technologies appear to have made it *easier*), in the end human beings are crucial components in information systems. Some humans will make mistakes, while others will intentionally steal or inflict damage. But humans will have to be trusted as long as the technologies serve human purposes. Wider access to information systems may increase vulnerability to losses of *confidentiality* and *integrity*; narrower access to only the most trusted persons compromises *availability*.[5] The perfectly secure environment will be a work-free environment.

[5] In the workshop, some participants observed that in the cyber realm, the lines between "insiders" and "outsiders" is being blurred—actors in various roles may be one, both, or either depending on the circumstances.

Scenario III: “Unknown Pedigree”

Cyber Challenge Scenario–
Unknown Pedigree of Tools

- *Deep ocean petroleum production suffered an enormous setback when our flagship exploration and survey submersible lost hull integrity at 23,271 feet below the surface.*
- *Recovered wreckage reveals that the hull compromise was not caused by impact or material defects, but rather a discrepancy between the design specifications and the measured dimensions of the recovered components.*
- *Test and evaluation (T&E) experts found inaccuracies in the analytical equipment that prevented discovery of the non-compliant components during verification and validation (V&V).*
- *Errors were found in automated design tools built on commercial hardware and software.*
- *Errors were also found in automated test equipment falsely indicating test pressures.*

The concept of “pedigree” is itself a metaphor, applying the family tree concept usually used for humans, dogs, and horses. In this case, *integrity* is lost in both system hardware and software components—which in turn leads to physical losses. It is unclear from the scenario whether the faults were accidentally or intentionally built into the components. The scenario illustrates the fuzzy line between *reliability* as a problem and *security* as a problem. Of particular concern to cyber security specialists is the potential for intentional, undetected introduction of flaws at various links in the supply chain.

Workshop participants pointed out that even well-traced pedigrees may not ensure security. "Trusted" components may nevertheless interact in untrustworthy ways; patches to correct problems can introduce new problems; components may be surreptitiously changed in transit from one trusted party to another; or, pedigrees may be counterfeited. It is not clear what entity could be created that could reliably guarantee pedigrees.

One approach to the problem is to try to so control production processes that the opportunity to introduce flaws is greatly reduced. Another is to try to mitigate the potential impacts of poorly “pedigreed” components.

Scenario IV: "Attribution Problem"

Cyber Challenge Scenario– Attribution

- *On August 17, 2011, New York area air traffic control systems became nonresponsive, resulting in hundreds of fatalities and widespread, cascading service disruptions.*
- *As with all critical US systems, the air traffic control systems are built on commodity computing equipment and standard commercial operating systems.*
- *The cause was determined to be IT-based, resulting from network traffic.*
- *The event was malicious in nature, triggered by a network based attack.*
- *IP traces lead to computers in three countries with varying degrees of distrust towards the US.*
- *We have strong suspicion, but IP traces are insufficient to constitute proof.*

In this case, loss of system *availability* results in serious loss of human life and economic resources. If caused (or intentionally enabled) by a national government, the metaphor of "warfare" would come to mind. If a non-governmental group intended to cause something like the damage that occurred, the act would probably be called "terrorism." If the attacks were conducted by hackers intent on mischief, but not foreseeing the actual consequences, the perpetrators would at least be considered to be "cyber criminals." In workshop discussions, the prevailing metaphor was "cops and robbers."

Implicit in characterizing the scenario as a problem of attribution, as opposed to a problem of denial of service, is a focus on finding and punishing the perpetrators as a means of deterring them or others from committing such acts in the future. As desirable as that may be, some workshop participants questioned whether the best cyber security resource allocation would be toward solving the extremely difficult problem of ferreting out the attackers, or toward better securing critical information systems.

Some Issues Relating to Threats

Targets

As the National Academy report quoted in Box 1 points out, a broad spectrum of actors poses even a broader spectrum of threats to the information technology infrastructure. From a public policy point of view, the question arises as to whether there is a special class of "national security" targets that either pose special problems, or that can and should be protected in different ways than other, civilian and commercial, targets. Military operational command and control systems might constitute one such set of targets. Intelligence information systems might be another. Systems for managing the nuclear weapons stockpile might be a third. From a Federal Government perspective, it might make sense to treat these potential cyber security problems separately from others. They are at the center of the government's defense and war-making capabilities. To some extent, their information

systems maybe isolatable from the Internet or other broad networks. And, because the potential consequences of attacks are so high, it may be worth applying technology solutions that would be considered unaffordable in commerce or in other day-to-day governmental operations.

On the other hand, it can be argued that attacks on other critical infrastructure systems (e.g., the power grid, telecommunications, or financial operations) not directly connected to military functions could cause as much damage to the nation as attacks on military-related systems. In addition, , the national security arms of government cannot afford to concentrate solely on a narrow set of vulnerabilities, but have to protect the nation as a whole if they are to protect themselves:

> …[networked systems] have been incorporated into virtually every sector of the Nation's critical infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.
>
> Beyond economic repercussions, the risks to our Nation's security are clear. In addition to the potential for attacks on critical targets within our borders, our national defense systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid (GIG), which is projected to cost as much as $100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.[6]

Attackers

The spectrum of potential attackers may range from the teenaged vandal to the sophisticated nation-state. And the nation-state determined to carry out acts of "cyber warfare" might have simultaneous access to a range of attack modes not generally available to lesser adversaries: a substantial cyber warfare R and D base, large numbers of highly skilled cyber "warriors," embedded spies or saboteurs, kinetic energy attacks on hardware or personnel, and perhaps, latent hardware or software vulnerabilities introduced into government procurement supply chains. This class of attackers might also use particular techniques not usually seen in the realm of day to day cyber crime and mischief. (On the other hand, they might utilize frequently seen modes of attack (e.g., a botnet denial-of-service attack) to help evade attribution and retribution.)

III. Metaphors Old and New

Participants in the workshop were asked to "brainstorm" a list of potential metaphors applicable to cyber security. They were asked, in addition, to identifying the most common metaphors underlying current discussions of cyber security, to list as many others as they

---

[6] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Washington, DC: Executive Office of the President, February, 2005), pp. 1-2. At www.nitrd.gov/pitac/reports/20050301_**cybersecurity/cybersecurity**.pdf.

could think of. The newer or rarer metaphors were then grouped into several categories to facilitate further elaboration.

Predominant Metaphors

As mentioned above, a common metaphor in cyber security is that of the fortress.[7] A valued body of information is held within a walled enclosure, perhaps encircled by a moat, accessed by portals or gates, and guarded by watchmen assigned to keep out the unauthorized. A second common metaphor is that of cops and robbers: criminals (or maybe just vandals) break into the house and steal valuables. Forensic measures are taken to track them down, after which they are identified and legally prosecuted. A third common metaphor is that of warfare: enemies, using various weapons and tactics, attack and steal or destroy property (or perhaps just commit espionage) in order to achieve some strategic goal.

Newer metaphors

Biological

Some cyber security metaphors come from the field of biology. A broad approach is to think of cyber systems as instances of complex, adaptive systems—as our biological systems. One example of such systems is the ecosystem: a complex system of interdependent species in populations in a particular kind of environment. A concept drawn from ecosystem studies is that of biodiversity: the idea that systems with diverse components are likely to be more stable, resilient, and adaptable to change. This metaphor is utilized below (p.26) in the section on "Heterogeneity." Another example is that of biological immune systems, the subject of a growing body of computer science literature and attempts to show how the mechanisms of immune processes systems can be imitated in hardware and software systems. A related metaphor is that of programmed cell suicide—apoptosis—in multicellular organisms: computers might be programmed to recognize if they have become infected and detach themselves from their network.[8]

Medical/Health

Numerous analogies between personal and public health measures and cyber security measures can be imagined. These are not enumerated here because they will be explored more fully below in Section IV.

Market Systems

In many ways, of course, the Internet is a vast marketplace in which goods and services are being bought and sold continuously, even though it lacks the physical accoutrements of traditional marketplaces. Hardware and software systems themselves are bought and sold. But the direction of this metaphorical exploration was to consider how market and economic principles might be applied to cyber security problems. Given that the cyber "world" is

---

[7] See footnote 4.

[8] See Steve Burbeck's description at http://evolutionofcomputing.org/Multicellular/ApoptosisInComputing.html

subject to economic forces that have historically not led to highly secure systems, could one imagine changes in economic incentives that might change that trend?[9]

Thinking from an economic perspective, then, could incentives be created that would harness the self-interest of the participants in the market in ways that would lead to greater security? On the one hand, it would be desirable, if possible, to reduce the profits from the development and use of malware by cybercriminals. On the defensive side, as commercial interests encounter increasing losses from cyber crime, incentives to enhance security might emerge without much external prompting. As losses cut further into profits, purchasers of computers and software might demand that manufacturers guarantee some level of security in their products. They might also be willing to pay higher prices for greater levels of security. Insurers might offer indemnities for cyber related losses, provided that those insured adhered to higher security standards or purchased security measures recommended by the insurers.

Beyond the loss-induced changes in economic incentives, the Federal Government, taking cyber security as a public good, might exert its ability to affect economic incentives by using taxation, subsidies, regulations, legislation, and purchasing power to encourage higher standards of security in the market.

A related business concept is that of risk management, in which organizations (possibly corporations, possibly government agencies) attempt to assess the risks they face, prioritize them, and take management measures appropriate to those risks: avoidance, reduction, acceptance, or transfer. Each of these has a cost, which is weighed against the potential losses. Workshop participants pointed out that although estimating the uncertainties involved is difficult in any case, business have the advantage that the assets they hope to protect are usually fungible—can be translated into financial gain or loss. In the case of governmental organizations, on the other hand, losses and costs of protection may not be fungible. For example, a monetary insurance policy (transfer of risk) for the loss of a military or intelligence secret would not be feasible. Or, the political cost of an apparent breach of security may outweigh any clear direct damage from the loss of a secret.

Spatial Metaphors

The term “cyberspace” was invented in 1982 by science fiction writer William Gibson, and it became commonly applied to the Internet and the World Wide Web in the 1990’s. It is a good example of how a metaphor—mapping of one domain (three dimensional space as humans experience it) to another domain (computer networks)—has become so pervasive that we scarcely even think of it as a metaphor any more. The newly formed Air Force Cyber Command describes its mission in ways that imply that cyberspace is not a metaphorical concept, but just one more class of physical spaces that it calls “domains”:

---

[9] For a project on “An Economic Approach to Security,” see http://cs-www.cs.yale.edu/homes/jf/econsecurity.html#description . For an analysis of business incentives to invest in cyber security, see Lawrence A. Gordon,. *Testimony for the House Committee on Homeland Security’s Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology*. 31 October 2007. “Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective.” http://homeland.house.gov/SiteDocuments/20071031155020-22632.pdf

> Cyberspace is a domain like land, sea, air and space and it must be defended. Although we've been operating in cyberspace for a very long time—since the invention of telegraph, radio and radar—we now conduct the full range of military operations in this domain. Just as the sea domain is characterized by use of water to conduct operations, and the air domain characterized by operations in and through the atmosphere, the cyber domain is characterized by use of electronic systems and the electromagnetic spectrum.[10]

Several variations on the spatial metaphor emerged during the workshop "brainstorming." While the Air Force may perceive the sea domain as a place where military operations are conducted, there are other ocean metaphors that can be applied to cyberspace. It is a global domain across which many kinds of traffic (personal, commercial, civil, military) move. To varying degrees national users agree to "rules of the road," but there is no single sovereign to enforce a well-codified body of law. Military operations may be conducted there, as well as piracy.[11]

Another possible metaphor is that of outer space, through which many national (and some international) satellites move continuously across national boundaries, providing a variety of services. Satellites are vulnerable to various kinds of attack, the origins of some of which might be difficult to determine. Defensive measures can be taken, but the advantage seems to be with the offense. Some countries (e.g., the U.S.) are more dependent on satellite services than others, and therefore there are asymmetries in national vulnerabilities. This makes deterrence by threat of retaliation in kind problematic.

Some spatial metaphors may be more explicit about mapping the social, economic, and political characteristics of the "source domain" to the "target domain." An example is the Wild West or U.S. Western frontier metaphor:

> Like all metaphors, the Western Frontier metaphor provides a particular perspective on the object described. The metaphor constructs the Inter-net as a version of the Western Frontier, a historical phenomenon that glorifies individuality and the benefits of minimal government. Put slightly differently, the Western Frontier metaphor suggests that the Internet will permit everyone to live a modern, improved version of America's westward expansion. Like the American West, the unregulated Internet has inherent characteristics that support unlimited economic opportunity, equality, individual freedom, and even political liberty. [12]

Another suggested metaphor was that of the global environment, with emphasis on the "tragedy of the commons" (itself yet another metaphor). The emphasis here is on the

---

[10] See http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10784

[11] Cf. Aaron Turner & Michael Assante:

In modern times, the nearly ubiquitous availability of powerful computing systems, along with the proliferation of high-speed networks, have converged to create a new version of the high seas--the cyber seas. The Internet has the potential to significantly impact the United States' position as a world leader. Nevertheless, for the last decade, U.S. cybersecurity policy has been inconsistent and reactionary. The private sector has often been left to fend for itself, and sporadic policy statements have left U.S. government organizations, private enterprises and allies uncertain of which tack the nation will take to secure the cyber frontier.

"Freedom of the Cyber Seas," at http://www.csoonline.com/article/329164/Freedom_of_the_Cyber_Seas/1 s

[12] Alfred C. Yen, "Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace," *Berkeley Technology Law Journal*, Vol. 17, 2003 Available at SSRN: http://ssrn.com/abstract=322522 . Yen, however, argues that "Feudal Society" is a more appropriate metaphor for the Internet than "Western Frontier".

phenomenon that, while most of the actors in cyberspace have a common interest in the maintenance and improvement of security, the incentives facing them individually do not reward behavior that serves the common interest.

Physical Asset Protection

This group of metaphors also draws upon analogies to objects in the spatial (physical) world, but in narrower, more specific ways. The castle or fortress metaphor introduced above (p. 10) falls in this category. One observation about castles is that not only do they attempt to maintain layers of physical protection, but they may operate at varying levels of security (e.g. portcullis up or down) depending on the level of threat; accordingly, there will be times when normal levels of traffic in and out will be reduced. The same may apply to computer network protection—the highest level of protection entails shutting down the system. The castle metaphor can also make more apparent other weaknesses of current approaches to cyber security: castles are reactive, immovable, inflexible, unable to adapt to novel attacks (explosives made castles obsolete).

A bank might be seen as a version of the fortress—walls, vaults, guns, guards protecting valuable objects (gold, currency, safe-deposit items.) In a way, however, banks were like cyber-entities before there was cyberspace. Credit is a promise of cash, but banks loan out more than they hold in actual currency. Since departure from the gold standard, currency itself is a promise to pay something else. More and more finance is conducted electronically, and the objects to be protected are pieces of information, connecting buyers and sellers, owners and borrowers with numbers of "credits." Such security features as accurate identification of actors, non-repudiation of transactions, and integrity of data were important to banking before banking moved into cyberspace.

Numerous analogies between banking and cyber asset protection were suggested. Audits of records help track assets. Trusted employees (insiders) can steal or enable stealing. Protected assets have to flow in and out to maintain the business. Where cyber security relates to money, companies can write off or insure against financial losses. On the other hand, some losses of information are irreplaceable (e.g., high value intellectual property or very important government or military secrets).

The first session of the workshop was held in a hotel, and it occurred to some participants that a hotel might be considered as a metaphor for cyber security issues. The following features of security issues in the hotel business were cited as have possible analogies to cyber security:

- The asset being protected at the hotel is the ability to sell/utilize rooms to make a profit.
- Capacity planning takes place under dynamic situations (holiday travels, slow season, etc.).
- Hotels must innovate to survive, and meet the needs of customers; it is important to know your brand and your customers (user of the asset—e.g., some times of year your customers are parents of graduating students, other times vacationers, others.)

- Hotels supposedly know who checked-in, but can't know for sure who is using the room (fake ID, sell/give your room key away to another person, 10 people sleep in one room, etc.)
- Hotels have some control (staff go into the room to clean every day and can notice things amiss, cameras monitor hallways and elevators, some hotels require room keys to use the elevator).
- The lowest-paid and least-educated employee is given the master key to all the rooms of the hotel.
- Hotels have an implied sense of security that is not really all that valid.
- There is a cost of doing business that is acceptable to hotels (stealing towels, breaking into mini-bar, room damage), etc. But they can handle this by charging your credit card later for stolen items or damages.

Varieties of Conflict

Since cyber security is intrinsically a conflict issue, some participants asked whether "conflict" could really be considered a metaphor. Taken in its most abstract sense of opposition between two entities, perhaps it can't be considered a metaphor. Even so, as soon as the concept of conflict is further characterized, metaphors seem unavoidable. A predominant metaphor is that of warfare.[13] But our ideas about warfare come from the physical clash of military forces, involving soldiers (or sailors or airmen), kinetic weapons, delivery platforms and vehicles, or at least other tools for attacking or defending against the preceding. Ideas about strategy and tactics can be more abstract, but still derive from the history of physical battle.

Another type of conflict is the competitive game.[14] The question was raised in the workshop whether cyber conflict more closely resembled chess or poker. A chess game (rich in metaphors of combat, even in its playing pieces) involves strategies and tactics, attacks, defenses, counterattacks, captures, sacrifices. These have counterparts in cyber conflict. When the opponent is not a computer, attempts at psychological manipulation may be made. However, the board, pieces, and allowable moves are always known to both sides (though the calculations of the adversary can only be inferred). In poker, each side starts (and for some period of time remains) uncertain about the cards held by the adversary as well as the cards remaining to be dealt. Secrecy and deception are parts of the game. Many would argue that cyber conflict is more like poker than chess.

The Chinese game of Go was nominated as another metaphor for cyber conflict. Two scholars of "netcentric" warfare have argued that

---

[13] For an early discussion of the pros and cons of the warfare metaphor, see Martin Libicki, Defending Cyberspace and Other Metaphors (Washington: National Defense University Press, 1997), available at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA368431&Location=U2&doc=GetTRDoc.pdf

[14] The categories of games and warfare frequently overlap. Military institutions "play" war games (sometimes using low or high-fidelity simulations, sometimes using real military personnel and equipment on physical terrain) to test training and concepts. Many games, on the other hand, either attempt to simulate warfare or make heavy use of military metaphors. The two categories share terms e.g., strategy, tactics, winning or victory, losing or defeat, stalemate.

> The game of Go provides a better analogy for conflict in the information age, especially for irregular warfare and for networked types of conflict and crime at the low-intensity end of the spectrum... The goal is to control more of the battlespace than one's opponent does. Once emplaced, a piece exerts a presence in that part of the board, making it easier for the player to place additional pieces on nearby points in the process of surrounding territory. As a result, there is almost never a front line, and action may take place almost anywhere on the board at any time. The key battles are less for control of the center than of the corners and sides (since they are easier to box off)… Thus Go, in contrast to chess, is more about distributing one's pieces than about massing them. It is more about proactive insertion and presence than about maneuver. It is more about deciding where to stand than whether to advance or retreat. It is more about developing web-like links among nearby stationary pieces than about moving specialized pieces in combined operations. It is more about creating networks of pieces than about protecting hierarchies of pieces. It is more about fighting to create secure territories than about fighting to the death of one's pieces. Further, there is often a blurring of offense and defense—a single move may both attack and defend simultaneously. Finally, the use of massed concentrations is to be avoided, especially in the early phases of a game, as they may represent a misuse of time and later be susceptible to implosive attacks. This is quite different from chess, which is generally linear, and in which offense and defense are usually easily distinguished, and massing is a virtue. Future conflicts will likely resemble the game of Go more than the game of chess.[15]

Also suggested as a suitable metaphor was that of the martial arts. The primary concept here was the turning of the adversary's attacks and strengths against him.

Conflict metaphors can serve numerous useful purposes in thinking about cyber security. They stimulate thinking about longer-term strategic as well as immediate tactical defense. They invite exploration of the potential utility of deception in cyber defense as well as offense.[16] (Some recommend studying *The Art of War* by Sun Tzu, which asserts that "All war is based on deception.") Thinking about the interactions of offense and defense can lead to a complex adaptive systems perspective, which in turn may yield further insights about how to improve security. Some analysts have applied mathematical game theory to cyber security issues.[17]

The war metaphor also leads to discussions of deterrence. Deterrence may be viewed in a narrower sense of threatening potential attackers with some sort of retaliation, or in a broader sense of generally raising the prospective costs of an attack by improving defenses (whether passive or active) or having the resilience to withstand or quickly recover from whatever damage has been inflicted. As mentioned above, deterrence based on retaliatory threats implies an ability to perform the extremely challenging task of attribution of attack origins. Those favoring an emphasis on retaliatory deterrence point out that attackers always seem to have the advantage: they can keep trying until they succeed, and the success of only one

---

[15] John Arquilla and David Ronfeldt, "A New Epoch — and Spectrum — of Conflict ," Chapter One of *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: Rand Corporation, 1997), pp. 10-11. Available at http://www.rand.org/pubs/monograph_reports/MR880/ .

[16] See Neil C. Rowe, "A Model of Deception during Cyber-Attacks on Information Systems," in *IEEE First Symposium on Multi-Agent Security and Survivability*, 30-31 Aug. 2004, pp. 21- 30.

[17] See Samuel N. Hamilton, Wendy L. Miller, Allen Ott , and O. Sami Saydjari, "The Role of Game Theory in Information Warfare" available at http://www.cyberdefenseagency.com/publications/The_Role_of_Game_Theory_in_Information_Warfare.pdf, and, by the same authors, "Challenges in Applying Game Theory to the Domain of Information Warfare" at http://www.cyberdefenseagency.com/publications/Challenges_in_Applying_Game_Theory_to_the_Domain_of_Information_Warfare.pdf . See also Peng Liu, Wanyu Zang, and Meng Yu, Incentive-based modeling and inference of attacker intent, objectives, and strategies, ACM Transactions on Information and System Security (TISSEC), Volume 8 , Issue1 (February 2005), pages78-118.

attack out of many may provide satisfactory payoff. Others argue that, given the long-term, multi-sourced character of the threat, resources would be better invested in greatly improved protection than on retaliation in kind, or at the very least, a credible threat of retaliation that has the effect of deterring attack.

A related debate is whether cyber conflict should be approached as an ongoing game likely to continue indefinitely without permanent winners or losers, or whether game-ending victory is possible.[18]

IV. Some New Approaches to Cyber Security

After the general discussion of metaphors, the workshop participants were asked to propose lines of inquiry for three "breakout" groups that would explore broad system-level ideas for improving cyber security in the future. The concepts informing these inquiries might further develop a metaphor already introduced, utilize some combination of metaphors, or merely be inspired by the preceding discussion. Box 2 lists the ideas proposed, along with a few supporting points for each. Full group discussion of these ideas resulted in the combination of some, the exclusion of others, and the formulation of three topics for further exploration. The three topics were entitled "Heterogeneity," "Motivating Secure Behavior," and "Cyber Wellness." These are described in further detail in the remainder of this report.

Box 2: Ideas for New Models of Cyber Security

Cyber Richter Scale
Published index of cyber dangers; lets lay people grasp the relative impact of a threat.
Provides an anchor for wide public discussion and gross appreciation of the breadth of impact.
Web of Trust
Federated systems –we both assemble systems from diverse components and rely on ensemble services made up of sub-services run by diverse entities.
How do we begin to understand how to make these secure?

Sun Tzu Metaphor (All Warfare is Deception)
Intelligence collection is not the only motive for cyber attack. Think Sun Tzu—deception is another objective. Let us think of walking the cat back to see what they're doing.
Lying software: Have software lie in the presence of suspicious behavior just as people do.
Other metaphors may play in as well.

"Intrinsic" or "Baked in" Security
What does this really mean? Who does the baking?
How do we deal with conflicting security goals? Or changing roles?
Which problems will, or will not, be resolved this way?
How can we effect change in a free market (society) where we don't control the market ?

Cont'd next page

[18] For an argument that, at least, "cyberspace dominance" or "cyberspace superiority" is possible, see Rebecca Grant, *Victory in Cyberspace*: *An Air Force Association Special Report*, October 2007, available at http://www.afa.org/media/reports/victorycyberspace.pdf.

Human Error Assumed
Steady state is one in which humans fail. Is elimination of "stupid" errors really the easy part?
Put effort into designing a system where you assume human error.
Do any other human systems have this solved?

Information ByWay
The way it was built it is a shared responsibility–distributed responsibility.
Everyone has "car" insurance.
Secrets cost IT dollars.
Note: Misconfiguration–any intrusion up to one of criminal intent is usually system misconfiguration.
Nation state attacks exploit flaws.

Render Safe
Reduce the internet footprint of compute systems.
Recover from attacks to a state of inertness—i.e. when perturbed, return procedurally to a state of trust/safety.

Multicellular Life Metaphor
We have moved from simple computers to very complex systems; analogous to the transition from multicellular to complex systems.
What can we learn from evolution of single-cell life to multicellular? Do we have to learn how to get lots of computers to collaborate in a robust manner the hard way?

Wellness Metaphor
Analogies to diet/nutrition/prevention for maintaining system "wellness."
Disease/bio attack analogies to cyber attacks.
Proposed system discussion context: future national "intelligent" power grid.

Futures Market
Using a futures market to predict large-scale cyber attack: people's greed and self-interest utilized as indicators of impending cyber attack.
Those to invest the most will be the ones most confident in an analysis or the ones with some sort of insider/expert knowledge. Also a good way of synthesizing information is distribution throughout the population.

Futures and Trends
Trends say virtual 3D net with avatars for users are the future of the internet: as in "Second Life "game, users have a 3D identity.
Avatars holding personal info of each user.
How will this affect security?

Cyber Dosimeter
Computer systems given exposure indictors: take a threat that is invisible and make it visible.
Measure damage (e.g. risk exposure), measure anomalies, correlate and respond

FEAR:
Apply domain-specific risk models to computer systems
Degrade service for those with "risky" behavior
Better service with assurance
Model: skittish

Characteristics of a future state
In designing a new system, begin with a vision of the desired characteristics, in which security measures are:
Intrinsic–built into the overall design
Integrated– see bio metaphor and health of our system
Flexible—in fact of uncertainty, adapt before anything happens.
Cont'd next page

Guaranteed Software:
Require guarantees from software vendors on the absence of bugs.
Produce radically simplified software tools (including an operating system), which permit vendors to buy insurance..

Diversity
Push the biological metaphor of biodiversity (such as concepts of speciation, ecological niche, predators, parasites, survival of the fittest, competition).
Look for analogies in coping with unexpected threats: alien invasion, asteroid hit, flu pandemic etc. -- how could those informed security planning and response?
Break system into smallest parts and mix them up.
Consider computer systems in which the interfaces between hardware and software components remain static, but the implementations are unpredictable. As in biological systems, this means some of the population will be immune to any attack.
Further, for intelligent attacks that hide by working across components, makes the makeup of the various components unpredictable to attack planners.

3 Fold Construct:
(Approach security from three related, but distinct, perspectives)
Social Causes and Solutions
Insecurity results from self-interested individual and collective behavior, which must be understood and engaged through cooperation and confrontation
Technical causes and solutions
The creation, design, and operation of computers and networks creates and influences opportunities for cyber attack, as well as our ability to respond to attack.

Economic markets, tradeoffs and incentives
Security is something society can produce: we must give a broad, diverse, and decentralized collection of actors and institutions the incentive to produce system security and compare/trade its value against other social and human goods and values.

Heterogeneity

The "Heterogeneity" approach draws on the ecological concept of biodiversity in designing future computer network systems. In a very homogeneous ecological system, severe environmental changes can lead to mass extinctions, while greater diversity increases the chance that at least some species, or individuals within will survive. Computer systems may fail because of hardware software flaws that emerge only when particular, unforeseen system states are reached—in analogy to natural catastrophes in ecosystems—and homogeneous systems are more likely to fail completely.

Similarly, computer networks in which all the components have the same vulnerabilities are easier for attackers to bring down, while more diverse systems would deprive attackers of sufficient target knowledge to do as much damage. What is more, systems comprising diverse hardware and software components would make it easier to confuse and deceive attackers. It can thus be argued that diversity is one of the ways of "baking" security into systems—designing them from the start to be more secure, as opposed to adding on security measures later.

Operational unpredictability would increase their uncertainty about what might be an effective mode of attack.[19] Frequent automated network reconfigurations might be an operational way to introduce heterogeneity. Unpredictability might be increased by varying cryptographic algorithms and keys. It was suggested that "late binding" could also increase attacker uncertainty.[20] A related example offered was that of Google searches, in which there is no way of knowing in advance which of the company's thousands of servers will handle any given request.

User interfaces among the diverse components should be common (necessary for practical use), and could thereby cover underlying diversity in function and implementation. An analogy can be found in automobiles, where dashboard and other controls are fairly standard, while the engine and other subsystem designs may vary quite widely. In the same way, users need not be greatly inconvenienced by underlying variations in computer software and hardware operations. There are techniques (such as object-oriented programming) that make more heterogeneity feasible.

Moving toward more diverse systems would require both technical and policy advances. Technically, human designed systems tend to converge to uniformity. Therefore, there is a need for new ways of creating software (and perhaps hardware components) that automatically introduce diversity. The economics of the industry—imposing incentives for convenience, efficiency, speed, and low cost—have impelled management, developers, and service providers to press for uniformity. Uniformity provides economies of scale in both the production and maintenance of computer systems. Hence, there is a prevailing presumption that standardization, rather than diversity, should be the norm.

Because standardization was so successful in enabling mass production in the industrial revolution, heterogeneity may seem counterintuitive. What is required is for government and industry consumers to recognize the security value of diversity. They might then encourage it by the following:

- yielding to bottom-up desires for diverse hardware and software through more varied procurement and willingness fund non vendor-specific technical support;
- requiring multiple supply sources;
- in procurements, focusing on performance requirements, not technical specifications; and
- demanding that these multiple vendors adhere to common interface and interoperability standards.

---

[19] For discussion of some relevant papers, see CarolTaylor and Jim Alves-Foss. (Eds.). (2005). "Diversity As a Computer Defense Mechanism: A Panel," *Proceedings from New Security Paradigms Workshop 2005*, Lake Arrowhead, CA (New York: ACM, 2005).
[20] "Binding is a process of matching function calls written by the programmer to the actual code (internal or external) that implements the function. It is done when the application is compiled, and all functions called in code must be bound before the code can be executed." From http://support.microsoft.com/kb/245115, which also discusses the differences between early and late binding and why early binding is usually preferred.

Although most procurement of information technology is commercial, US Government procurement standards could help set market standards. In the commercial sector, the benefits of improved security might make buyers more willing to pay the costs of increased diversity, while vendors could advertise good security as a selling point.

An issue of concern in the heterogeneity model is how applicable it might be to high-value military, intelligence, law enforcement, or critical infrastructure systems. On the one hand, diversity could complicate the operation of these critical systems. On the other hand, the high value of the targets involved may very well justify the additional costs of adopting more heterogeneous systems. Moreover, increased heterogeneity in commercial systems may lead anyway to increased diversity in the government or critical infrastructure operations, since they frequent utilize commercially purchased systems.

There is also potential benefit to be gained in matching outputs from diverse computing processes: agreement among them would suggest a higher probability of valid results. "Voting" systems (such as used with the multiple computers on the Space Shuttle[21]) could increase confidence in system reliability.

A second question about this approach is whether it might hinder the detection of successful adversary attacks: system behavior might also be less predictable and understandable to owners as well as to attackers. An answer to the question is that heterogeneous systems would generate more data about adversary strategies and tactics, because the adversary would have to conduct more probing experiments to have much chance at successful attacks. A related question is that of reconciling the transparency needed for internal audits and evaluations with the opacity needed to keep adversaries uncertain. One answer would be to limit the auditing function to a very few auditors, but to give them very broad access.

Yet another question is whether prior system penetration would preclude the benefits of moving to greater heterogeneity. An answer is that replacing existing system components with newer, more varied, components could disrupt the existing penetration. And if the penetration were by an insider, the chances would be lessened that any one insider would have complete understanding of the whole system.

Given the change from current practices proposed here, it is clear that considerable analysis, research, testing, and continuous "red team" challenging would be necessary to ascertain exactly where and how the principles of heterogeneity could be most effectively and efficiently applied.

Motivating Secure Behavior

The second explored approach to the future of cyber security, "Motivating Secure Behavior," placed less emphasis than the first on underlying security technologies, and more

---

[21] Each Space Shuttle carries four computers: " The four general-purpose computers operate essentially in lockstep, checking each other. If one computer fails, the three functioning computers "vote" it out of the system. This isolates it from vehicle control. If a second computer of the three remaining fails, the two functioning computers vote it out. In the rare case of two out of four computers simultaneously failing (a two-two split), one group is picked at random." See http://en.wikipedia.org/wiki/Space_Shuttle.

on the human element. The theme is inspired by taking an economic or market perspective on the security problem. The central concept is that many of the vulnerabilities in current systems can be traced to human behaviors shaped by the structure of incentives facing both suppliers and users of information technology. Therefore, the overall task is to make it easier for people to do the "right" thing and harder to do the "wrong" thing.

The ideal would be to instill a sense of shared responsibility—as opposed to a mindset of forced compliance—among suppliers, system administrators, and users. Education, community mores, and government advocacy might help (though changes in law, regulation and market incentives may be more important). In particular, to encourage the reporting of problems so that the community can address them, users and administrators should not be punished for self-reporting errors in their own security behavior, or blamed for being the victims of cyber attacks.

Responsibilities (and therefore incentives) should be developed for and by different system levels and actors:

- individuals (e.g., US consumers, managers);
- institutions (e.g., Microsoft, universities);
- government agencies (e.g., DOE, Sandia);
- public policy makers(e.g., Congress, Executive Branch, agencies, courts, states), and
- standards bodies/associations (e.g., IETF,[22] ICANN,[23] BSA,[24] BITS-FSR[25]).

Individuals should be given user-friendly tools that make it easier for them to engage in safe computer behavior, such as maintaining protective measures or using safe e-mail practices. A technological challenge is to develop user interfaces that give legitimate users the functionality they need, while making it more difficult for malicious insiders to abuse their access. Institutions providing information technology services might be held to regulated standards of security and penalized by law or civil liability if the do no meet them. Working with industry, insurance companies might establish insurance programs against security-related losses while helping to improve cyber security standards. Government agencies might help set marketplace standards through procurements that emphasize security improvements. The institutions that set public policy could establish standards by law, improve law enforcement against cyber crime, or subsidize research and development in improved security measures. However, the potential threat of future regulation might, in some cases, encourage the private sector to head off the regulation by improving its security performance. Standards bodies could help identify and achieve consensus on the most appropriate and effective security standards. In any case, standards and the incentives to adhere to them should be established not merely for their own sake, but in rational proportion to the harm they are intended to preclude.

---

[22] Internet Engineering Task Force, http://www.ietf.org/overview.html .

[23] Internet Corporation for Assigned Names and Numbers, http://www.icann.org/.

[24] Business Software Alliance, http://www.bsa.org .

[25] BITS, a division of the Financial Services Roundtable, http://www.bitsinfo.org/ .

An apparent disadvantage of the Motivating Secure Behavior approach is that it seems to address only the guardians and the victims, but not the attackers. On the other hand, the concept of deterrence (see above, p. 23) is about providing disincentives to attackers, and therefore might in principle be folded into this approach. A particularly vexing kind of attacker is that under the direction of a nation-state. There was some discussion not only of how national adversaries might be deterred, but whether they might be engaged in ways that lessened their motivations to attack and increased their desires to cooperate.

Another disadvantage of the focus on Motivating Secure Behavior is that it is vague about exactly what technologies developers, vendors, buyers, and users should be "incentivized" to create, sell, buy, and use. The implicit assumption is that with the right performance standards adopted and widely accepted, the marketplace will produce the necessary technologies.

Cyber Wellness

Of the three explored approaches to thinking about future cyber security, the "Cyber Wellness" approach is the one which mostly applied a single metaphor: that of human health maintenance. It is also the one that had the widest scope, with analogies from human health that could be applied both to the technical and behavior dimensions of cyber security. The Cyber Wellness approach attempts to take a whole-system perspective on cyber security. Its objective is to keep the population (of users and networked systems) as healthy as possible: resistant to attacks, resilient under stresses, avoiding dangerous environments, treatable if diseased, able to limit contagions. Much responsibility for personal (local) wellness depends on individuals, but various levels of corporate and public health management, from the local to the international, are equally important. Table 1 presents an overview possible mappings from the human wellness to the Cyber Wellness domain.

Table 1: Human Wellness And Cyber Wellness Analogies

Human Wellness Concept	**Cyber Analog**	**Comment**
Personal health	Individual computer security OR	User functionality is PC or server centered
	Security of "avatar" or mobile agent	User functionality is software agent centered
Natural immune system	Security measures built into software or hardware	Built-in security still rare in computing
Healthy personal behavior	User practices "safe" computing	Focus on user taking responsibility for protecting "health" of computing persona
Health education	Cyber security education	
Frequent check-ups	Malware scans or other diagnostics	
Infectious diseases	Viruses, worms	In both cases, large array of effects on the system is

"Normal" distribution of pathogens Bioterror attacks Biowarfare Dormant vs. active pathogens	Day-to-day hacker activity Concerted action by non-state actors to damage particular targets State-sponsored acts to achieve "military" objectives Back doors or other latent malware	possible
Emerging diseases	Zero day attacks on discovered vulnerabilities	
Epidemics	Botnets; contagious viruses	
Immunizations	Employment of protective software or hardware	
Medical treatment	Application of diagnostics and repair and replacement of software or hardware	
Doctors	System administrators	
Medical Specialists	Cyber security specialists	
Public health surveillance and epidemiology	Network security monitoring, analysis, and reporting	In both cases, may be done at local, regional, national, or international levels
Public health protective measures: warnings, quarantines	Warning programs (e.g. DHS-sponsored US-Computer Emergency Readiness Team), Isolation of "infected" systems	"US-CERT is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities disseminating cyber threat warning information coordinating incident response activities."
Medical research	Cyber security research	

This approach shares with the Motivating Secure Behavior approach an emphasis on the role of individuals in behaving in ways that are protective of their security, as well as providing systemic education and incentives to encourage them to do so. Thus, individuals need to be alert to and avoid risks, maintain their immunizations, have regular "check-ups" to look for incipient problems, seek specialized treatment when appropriate. In this paradigm, users are not blamed for being "stupid," but helped to care for themselves. Even more than the "Motivating" approach, however, Cyber Wellness encourages thinking about the interactions of all the components at all levels of the "health" maintenance system.

An issue raised during discussions of the Cyber Wellness metaphor or them was whether it could suggest adequate responses to malevolent, intelligent attacks, given that most human health problems (except use of bioweapons) were not in that category. One answer to this potential objection is that, at least in cases of infectious disease, humans are "under attack" by organisms that, though perhaps not intelligent, are highly configured to penetrate our defenses and cause us damage of some kind. They also frequently have the ability to rapidly adapt to our responses to them. From the perspective of keeping individuals and populations healthy, the question of whether intelligence and malevolence are involved is moot.

It is possible to consider many ways in which the Cyber Wellness approach could be implemented in software and hardware.[26] One of the issues stressed by the group exploring this approach is that, as has frequently been observed, security should be "baked into" information technology systems, not—as has been the rule thus far—added on later almost as an afterthought. This observation leads to the question of how to make the transition to more inherently secure systems. At this workshop, participants adopted a working premise for the sake of discussion: the future of networked computing lies in mobile software agents representing individual users—agents they labeled "avatars."[27] According to the National Institute of Standards and Technology (NIST) Computer Security Resource Center,

> Mobile agents are autonomous software entities that can halt themselves, ship themselves to another agent-enabled host on the network, and continue execution, deciding where to go and what to do along the way. Mobile agents are goal-oriented, can communicate with other agents, and can continue to operate even after the machine that launched them has been removed from the network. [28]

In the Cyber Wellness approach, the avatar is the user's presence in computer networks, and is the primary entity whose "health" is monitored and maintained. The avatar may also be supported by other, autonomous mobile agents that monitor agents and platforms, detect and warn of suspicious or malicious activities, and take corrective actions. Such agents might comprise a distributed "sensor" system that provided greater surveillance and warning capabilities than are available in the current CERT model.

Each avatar might have a "wellness" index, perhaps resembling today's personal credit scores, that is apparent to other avatars and to host platforms; this index would then be used to limit or expand the avatar's freedom to operate in the system—with the riskiest avatars being quarantined entirely. In this way, each user has a direct incentive to keep his or her avatar in good health. Security is a distributed, rather than centralized, function.[29]

---

[26] For example, an entire literature has developed in the past 15 years or so on applying the principles of biological immune systems to the design of new operating systems, applications, and hardware. For one introduction, see the web site "Artificial Immune Systems" at http://ais.cs.memphis.edu/ .

[27] In the online computer gaming world, the "avatar" has meant a virtual represent*ation* of a person, rather than a represent*ative* of the person, which has usually been called a "software agent." The workshop group synthesized these two concepts into one.

[28] http://csrc.nist.gov/groups/SNS/mobile_security/mobile_agents.html . The concept of mobile agents emerged in the professional literature in the early 1990's. For an expanded description of the concept, see Jeffrey M. Bradshaw, Chapter 1. "An Introduction to Software Agents" in Software Agents (Cambridge, MA: MIT Press, 1997), pp. 4-45, available at http://agents.umbc.edu/introduction/01-Bradshaw.pdf . A search of Google Scholar returns about 12,000 articles on mobile agents published since 2003.

[29] Workshop participants also pointed out that avatars could incorporate the "HENRY" benefits of heterogeneity: there would be multiple types of avatars, they might operate and travel unpredictably.

The idea of "baking security in" as networked computing makes increasing use of mobile agents sounds more sensible than continuing to adding on security measures after new software and hardware are developed and fielded. Doing so, however would face significant technical challenges. As the NIST Computer Security Resource Center has pointed out,

> The mobile agent computing paradigm raises several privacy and security concerns, which clearly are one of the main obstacles to the widespread use and adaptation of this new technology… Mobile agent security issues include: authentication, identification, secure messaging, certification, trusted third parties, non-repudiation, and resource control. Mobile agent frameworks must be able to counter new threats as agent hosts must be protected from malicious agents, agents must be protected from malicious hosts, and agents must be protected from malicious agents.[30]

Note that, as indicated in this quotation, not only must the avatars carry security protection, but the hosts in the new paradigm would have to be protected just as much as do the computers in the networks of today.[31] Although building security into avatar-oriented computing would be challenging, there is a growing literature on mobile agent security.[32] In fact, the NIST Computer Security Division quoted above has itself a research program on that subject.

As desirable as it may be to "bake in" security, however, the Cyber Wellness approach rejects both the hope that some future end-state of perfect security will be reached and the fear that anything less than perfection is useless. Instead, it accepts that maintaining cyber security will be a long-term, continuing, adaptive process.

Given the costliness of the current U.S. medical care system, one might reasonably ask how Cyber Wellness could be affordably maintained. The answer is that the latter system should be developed going forward in ways that avoid the costliest faults of the former. It is now widely recognized that prevention, disease management, and public health measures are, from a broad perspective, more cost-effective than expensive interventions in acute cases. (And, in contrast to the human health case, "terminally ill" avatars or host platforms may be euthanized—or programmed to self-destruct—without major ethical problems. Not only could they be "resurrected" in a safe environment, but they might exist in multiple instantiations, with intact copies stepping in to perform the functions of infected avatars.)

---

[30] *Ibid*.

[31] A concept mentioned during the workshop was the Trusted Platform Module:

TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

Trusted Computing Group, "Trusted Platform Module (TPM) Summery," at https://www.trustedcomputinggroup.org/groups/tpm/Trusted_Platform_Module_Summary_04292008.pdf .

[32] For an overview of the security issues and of possible means of addressing them, see Michael J. Grimley and Brian D. Monroe, "Protecting the Integrity of Agents: An Exploration into Letting Agents Loose in an Unpredictable World" at http://www.acm.org/crossroads/xrds5-4/integrity.html?searchterm=mobile+agents. See also Wayne Jansen and Tom Karygiannis, *NIST Special Publication 800-19 – Mobile Agent Security* at http://csrc.nist.gov/groups/SNS/mobile_security/mobile_agents.html and Ambrus Wagner, "Implementing Mobile Agent Security In An Untrusted Computing Environment," 8th International Conference on Telecommunications, June 15-17, 2005, Zagreb, Croatia.

V. Conclusions

Whether used consciously or unconsciously, metaphors are integral to human thought and communication. As with other subjects, this is true in discussions of cyber security. Analyzing the metaphors implicit in the current mainstream of cyber security thought can illuminate the assumptions, logic, and perhaps the limitations of that thought. Experimenting with alternative metaphors can lead to different perspectives on the problem and may even stimulate creatively different ways of dealing with it. In the workshop reported here, participants were inspired to explore three broad concepts for approaching cyber security in the future: one emphasizing the utility of heterogeneously composed computer network systems in defending against cyber attacks; one stressing the importance of finding the right incentives to motivate information technology users, managers, vendors, suppliers, and developers to behave in ways that would make systems more resistant to attack; and one taking a metaphorical "wellness" view of cyber security that might enable a holistic design for "baking" better security into the next generation of information network systems.

Some final observations of workshop participants were that those responsible for setting future directions for cyber security need to

- have a bold vision of where we want to go, then figure out a *gradual* adoption/implementation strategy;
- accept and sustain a strategy through the inevitably gradual and evolutionary process that will ensue; and
- show benefits for users and operators, not just push solutions that aren't seen as beneficial outside the security world.

Annex: Participant Biographies

Sandia Cyber Fest Participant Biographical Profiles

External Participants

Brent Backman is the Cyber Advisor at USSTRATCOM's Global Innovation and Strategy Center, where his main focus is collaboration and innovation with private sector experts to provide the best solution to tough issues across all USSTRATCOM missions. He received a BS in Management Information Systems from the University of Nebraska at Omaha's Peter Kiewit Institute of Technology, an MS Degree Certificate in Information Operations from the University of Nebraska at Lincoln, and is currently finishing an MA in Communication from the University of Nebraska at Omaha. He is a Graduate of the Information Warfare Application Course, Basic Communication Officer Training, and has been accepted in residence to Squadron Officer School. In February 200, he joined the Department of Defense's Palace Acquire Program, where he worked across many of USSTRATCOM's Mission areas in a wide range of responsibilities including: the Information Management Division, the Ballistic Missile Defense System in the Engineering Technology Division, The Commander's Action Group, Space and Global Strike, and J8 Capability & Resource Integration, the J8 Director's Action Group (DAG), and J004's Legislative Division.

Steve Burbeck holds a BA from California State University at Long Beach (1969) in Mathematics and a PhD from the University of California at Irvine (1979) in Mathematical/Cognitive Psychology. He retired from IBM in mid 2005 and is currently an independent consultant. Prior to retirement, he was a Senior Technical Staff Member in IBM Healthcare and Life Sciences acting as liaison with researchers in bio-tech and academia who use computing to better understand complex biological systems. From 1980-88, he directed bioinformatics, statistics and computing at the Linus Pauling Institute of Science and Medicine in Palo Alto, CA. In 1988, he joined Apple Computer as Product Manager for Object Oriented software technologies. In 1990, he and his family moved from Silicon Valley to the Research Triangle Park area in North Carolina. In the first half of the '90s he was VP of Technology at an Object Oriented Software Consulting company. He joined IBM in 1995 as a Senior Consultant in Object Oriented Technology. Two years later, he moved to IBM Research to work on adaptive and self-configuring systems (now called Autonomic Computing). He then moved to the IBM Software Group to work on emerging technologies such as XML, Linux, Open-Source Software, peer-to-peer computing, Web Services and Service Oriented Architectures. In 2002 biology beckoned again and he joined the relatively new Life Sciences Group.

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, Adjunct Professor of Informatics, and director of the Center for Applied Cybersecurity Research at Indiana University, and a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams LLP. He is a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals; a member of Microsoft's Trustworthy Computing Academic Advisory Board; and reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information. He served as counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities. He is the author of many articles and books, including *Privacy in the Information Age*, *The Internet and the First Amendment*, and *Privacy in Perspective*. In 2007 Computerworld listed him as the only academic on its list of "Best Privacy Advisers" in the United States and Europe.

Charlie Catlett is Chief Information Officer at Argonne National Laboratory, Division Director of Argonne's Computing and Information Systems Division, and a Senior Fellow of the Computation Institute at the University of Chicago and Argonne National Laboratory. From 2004 through 2007 he was Director of the NSF

TeraGrid project, a $150M initiative to operate and enhance a distributed "Grid" of information technologies at nine major supercomputing centers and universities. From 1999 to 2004 he directed the State of Illinois funded *I-WIRE* optical network project, designing and deploying a dedicated optical fiber infrastructure to interconnect ten locations in the Chicago area and downstate Illinois. From 1999 through 2004 he founded the Global Grid Forum, an international technical standards body with participants from over 40 countries. Prior to joining Argonne in 1999 he was Chief Technology Officer at the National Center for Supercomputing Applications, where he had worked since 1985. With Larry Smarr, he co-authored a seminal paper "Metacomputing," in 1992 in the journal Communications of the ACM, which described the concept of "Grid" computing. In 1996 he was a co-Investigator, along with Smarr, Rick Stevens, Dan Reed, and Ian Foster, of the $180M NCSA Alliance project, in which the term "Grid" was first coined. During the 1980's and 1990's his focus was primarily on high-performance networks and distributed systems. He was a member of the team that deployed and operated NSFNET in 1986 and is a computer engineering graduate of the University of Illinois at Urbana-Champaign.

John J. Dziak is co-founder and President of Dziak Group, Inc., and Dziak Associates Inc., consulting firms in the fields of technology transfer, intelligence, counterintelligence and security, and national security affairs. His clients are found in industry, the Intelligence Community, and the Department of Defense. He has served over three decades as a senior intelligence officer and executive in the Office of the Secretary of Defense and in the Defense Intelligence Agency, with long experience in weapons proliferation intelligence, counterintelligence, strategic intelligence, and intelligence education. He received his PhD from Georgetown University, is a graduate of the National War College, and is the recipient of numerous defense and intelligence awards and citations. He is also a professor at the Institute of World Politics, where he teaches graduate courses on intelligence; has taught at the National War College, Georgetown and George Washington Universities; and lectures on intelligence and foreign affairs throughout the U.S. and abroad. He is the author of the award-winning, *Chekisty: A History of the KGB* (1987); numerous other books, articles, and monographs, the most recent of which is *The Military Relationship Between China and Russia, 1995 – 2002* (2002); and is currently preparing a book on counterintelligence.

Deborah Frincke joined the Pacific Northwest National Laboratory in 2004 as Chief Scientist for Cyber Security. Prior to joining PNNL, she was a Professor at the University of Idaho, and co-founder/co-director of the University of Idaho Center for Secure and Dependable Systems. She also co-founded TriGeo Network Systems, whose original products were based on her early research. Her research spans a broad cross section of computer security, both open and classified, with a particular emphasis on infrastructure defense and computer security education. She is an active member of several editorial boards, including: *Journal of Computer Security*, the *Elsevier International Journal of Computer Networks*, and the *International Journal of Information and Computer Security*. She co-edits the Security Education Board column *for IEEE Security and Privacy*, along with Matt Bishop. She is a steering committee member for Recent Advances in Intrusion Detection and Systematic Advances in Digital Forensic Engineering. She is an enthusiastic charter organizer of the Department of Energy's cyber security grass roots community. She received her PhD from the University of California, Davis in 1992.

Seymour E. Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of the Center for International Strategy, Technology, and Policy and Co-Director of the Georgia Tech Information Security Center. Goodman studies international developments in the information technologies and related public policy issues. He has published well over 150 articles and served on many government and industry advisory and study committees. He has been the International Perspectives editor for the *Communications of the ACM* for the last 17 years, and has studied computing on all seven continents and more than 80 countries. He recently served as Chair of the Committee on Improving Cybersecurity Research in the United States, National Research Council, Computer Science and Telecommunications Board, National Academies of Science and Engineering. He was formerly the director of the Consortium for Research in Information Security and Policy (CRISP), jointly with the Center for International Security and Cooperation and the School of Engineering, Stanford University. He has held appointments at the University of Virginia (Applied Mathematics, Computer Science, Soviet and East European Studies), The University of Chicago (Economics), Princeton University (The Woodrow Wilson School of Public and International Affairs, Mathematics), and the University of Arizona (MIS, Middle Eastern Studies). He was an undergraduate at Columbia University, and obtained his PhD from the California Institute of Technology where he worked on problems of applied mathematics and mathematical physics.

William (Bill) Hunteman, Jr. is the Chief Information Security Officer for the Department of Energy, with responsibilities for DOE policies, practices, cyber training, and technical cyber security activities, including cyber security enterprise architectures and technology development. He has over 40 years' experience in cyber security, high performance computer operating systems, and high performance computing and networks. He has spent most of his career working in the DOE national laboratories. He has been leading the cyber security working group in developing the recently approved cyber security revitalization plan and in guiding implementation of that plan. He has led several cyber security technology development projects, including intrusion detection systems, expert systems to analysis security plans and networks, and the development of secure high performance networks. He has served in a variety of management and project positions, most recently as the NNSA Cyber Security Program Manager and the Program Manager for the Integrated Cyber Security Initiative, tasked to define and deploy the NNSA enterprise secure network across the nuclear weapons complex. He has a BS in Mathematics and an MS in Electrical Engineering/Computer Science.

Carl Landwehr is Program Leader for National Intelligence Community Information Assurance Research at the Intelligence Advanced Research Projects Activity, on assignment from his position as Senior Research Scientist at the University of Maryland's Institute for Systems Research. His IARPA programs aimed for dramatic improvements in the overall trustworthiness of National Intelligence Community systems by focusing on accountable information flow, including technologies for privacy protection, and large-scale system defense. He also serves as Editor-in-Chief of *IEEE Security & Privacy Magazine*. His research interests span many aspects of trustworthy computing, including high assurance software development, understanding software flaws and vulnerabilities, token-based authentication, system evaluation and certification methods, multi-level security, and architectures for intrusion tolerant systems.
Don Petravick is head of the CCF Department at Fermi National Accelerator Laboratory. The Department has responsibilities for Computer Security, Data Management, and Networking. He is also interim Security Officer for the Open Science Grid.

Walter (Walt) M. Polansky is a Senior Advisor to the Associate Director for Advanced Scientific Computing Research, in the Department of Energy's Office of Science. He has over 25 years of experience managing research programs over a wide-range of scientific disciplines and technologies, including high-powered laser systems, novel energy concepts, high-performance computing systems, high-speed networks to enable scientific research, applied mathematics, computer science and the computational sciences. In 2003-2004, he was the Acting Senior Information Management Executive for the Office of Science, the principal official in SC for information technology, information management, and cyber security. There, he ensured that information technology throughout the Office of Science (approximately 270 investments, ranging from desktop systems to Leadership Computing facilities) was acquired and managed in accordance with the Federal Information Security Management Act, the Clinger-Cohen Act, DOE Directives, and guidance from the Office of Management and Budget. He is currently serving as a Department of Energy representative on inter-agency cyber security panels and is working with the Office of the Under Secretary for Science to develop a cyber security R&D strategy for the Department, an action from the DOE Cyber Security Summit of 2007. He has a PhD in Physics from the University of Cincinnati and a BS in Physics from Rensselaer Polytechnic Institute.

Neil C. Rowe is Professor of Computer Science at the U.S. Naval Postgraduate School, where he has been since 1983. He has a PhD in Computer Science from Stanford University (1983), and E.E., S.M., and S.B. degrees from the Massachusetts Institute of Technology. His main research interest is the role of deception in information processing, and he has also done research on intelligent access to multimedia databases, surveillance systems, image processing, robotic path planning, and intelligent tutoring systems. He is the author of over 140 technical papers and a book.

Keith T. Schwalm is a consultant in the areas of information security, homeland security, critical infrastructure protection, and computer forensics. He served for eight years as a special agent with the U.S. Secret Service, focusing on electronic and high-tech investigations. He served as a member of the Electronic Crime Special Agent Program, with assignments in the Albuquerque Resident Office, Financial Crimes Division, Office of Congressional Affairs and the Homeland Security Division. He was Director of Infrastructure Protection to the President's Critical Infrastructure Protection Board at the White House from 2001 to 2002. He was a founding director of the Science and Technology Directorate at the Department of Homeland Security, managing the Secret Service and Cyber Security R&DTE Portfolios. He holds a BA in Political Science from the University

of New Mexico and a MS in Computer Science from James Madison University. He is a Certified Information Systems Security Professional and Information Systems Security Management Professional, is a certified New Mexico Department of Public Safety Instructor, and has a certification pending for ISO 27001:2005 lead auditor.

Anil Somayaji is an Assistant Professor in the School of Computer Science at Carleton University. He received a BS degree in mathematics from the Massachusetts Institute of Technology and a PhD degree in computer science from the University of New Mexico. He has served on the program committees of the USENIX Security Symposium and the New Security Paradigms Workshop, among others. His research interests include computer security, operating systems, complex adaptive systems, and artificial life.

Eugene H. Spafford is Professor of Computer Science, Professor of Electrical and Computer Engineering (courtesy), Professor of Communication (courtesy) and Professor of Philosophy (courtesy), all at Purdue University. and. He holds the degrees of BA in Mathematics and Computer Science from State University of New York at Brockport, MS and PhD in Information and Computer Science from Georgia Institute of Technology, and DSc (honorary) from State University of NY. His current research interests are focused on issues of computer and network security, cybercrime and ethics, and the social impact of computing. He is the founder and executive director of the Center for Education and Research in Information Assurance and Security (CERIAS). This university-wide institute addresses the broader issues of information security and information assurance, and draws on expertise and research across all of the academic disciplines at Purdue. He has received recognition and many honors for his research, including being named as a Fellow of the ACM, of the AAAS, and of the IEEE. He has been awarded status as an Honorary CISSP (Certified Information Systems Security Professional), by the (ISC)2 and named as a member of the ISSA's Hall of Fame. In October of 2000, he received the field's most prestigious award: the NIST/ NCSC National Computer Systems Security Award. He holds numerous other professional awards as well awards for his teaching from Purdue, NCISSEE, and the IEEE Computer society. Among many professional activities, he is chair of ACM's U.S. Public Policy Committee and is the academic editor of the journal *Computers & Security*.

Alfred C. Yen is a Professor of Law at Boston College Law School, Law School Fund Scholar, and Director of the Emerging Enterprises and Business Law Program. He is a nationally known scholar who has published numerous articles about copyright law, the Internet, Asian-American legal issues, and law teaching. His recent works include "Third Party Liability After /Grokster/," which appeared in the *Minnesota Law Review* and a forthcoming new casebook on copyright (co-authored with Professor Joseph Liu) entitled *Copyright: Essential Cases and Materials*, which will be published by West Publishing in 2008. He received his BS and MS from Stanford University and his J.D. from Harvard Law School.

Sandia National Laboratories Participants

Rob Leland [Host] is Director, Computing and Network Services. He completed undergraduate studies in electrical engineering with a minor in mechanical engineering at Michigan State University. He attended Oxford University as a Rhodes Scholar and studied applied mathematics and computer science, completing a PhD in 1989. He then joined Sandia National Laboratories and pursued research in parallel algorithm development, sparse iterative methods and applied graph theory. In 1995 he served for one year as a White House Fellow advising the Deputy Secretary of the Treasury on technology modernization at the IRS. Upon returning to Sandia, he led the Parallel Computing Sciences Department in developing algorithms and software tools for the laboratory's supercomputing efforts and also served as a member of Sandia's Advanced Concepts Group studying long term national security issues. In 2002 he became the Senior Manager responsible for Computer and Software Systems, the group which developed the Red Storm supercomputer system. In 2005 he became Director of the Computing and Networking Services Center at Sandia, a 650 person organization responsible for operation of scientific supercomputing and enterprise computing platforms, voice and data networks, desktop support, and cyber security for Sandia's New Mexico site.

Robert M. (Mike) Cahoon, Manager, Cyber Security Dept.

Stephanie Castillo is the Cyber Technical Expert at the Office of Counterintelligence, Sandia National Laboratories (SNL). She has a Master of Science in Management Information Systems from the University of Arizona and a Bachelor of Business Administration from the University of New Mexico. She has worked at

SNL for the last six and a half years. She spent the first five years developing information solutions for SNL organizations and external customers.

Rebecca D. Horton is Senior Manager in the Information Systems Analysis Center at Sandia National Laboratories. Joining Sandia in 1984, she has worked in safeguards and security programs for both domestic and international applications. She worked as Senior Manager for Advanced Security Technologies Program Office in the Security Systems and Technology Center; managed the Entry Control and Contraband Detection department (a technology-based group involved in Research, Development, Testing, Deployment and training and program development for High Explosives Countermeasures); and was Program Manager for the International Nuclear Materials Protection Program and for the On-Site Monitoring R&D Program for Arms control and Nonproliferation. She worked on a temporary assignment at DOE Headquarters supporting the Office of Arms Control and Nonproliferation on international work in a number of countries on the physical protection of nuclear materials and on international safeguards. Prior to management, she worked on video image and signal processing technology development and implementation projects for Domestic Security at DOE sites and for International Safeguards for the International Atomic Energy Agency. She has a BS/EE degree from New Mexico State University and a MS/EE degree from Stanford University.

Munawar (Monzy) Merza, Cyber Monitoring & Policies Dept.

Steven Rinaldi manages the Effects-Based Studies Department in Sandia National Laboratories' Information Systems Analysis Center. He joined Sandia National Laboratories in April 2002, and was the Joint Program Director of the National Infrastructure Simulation and Analysis Center until April 2003. He undertook his current position in February 2005, and is responsible for advanced information system assurance programs, agent based systems, and software integration. Prior to joining Sandia, he served on active duty as an Air Force officer, holding numerous positions in the USAF science and technology community, with assignments in the White House Office of Science and Technology Policy, the Pentagon, Headquarters Air Force Materiel Command, and the Air Force Weapons Laboratory. He also served as a military exchange scientific officer at Ecole Polytechnique, Palaiseau, France. He retired from the Air Force in June 2002 with the rank of Lieutenant Colonel. He received a Master's degree in electro-optics and a PhD in physics from the Air Force Institute of Technology. He is a graduate of the Defense Language Institute, Squadron Office School, Air Command and Staff College, School of Advanced Airpower Studies, and Air War College.

Bridget Rogers, Manager, Systems Technology Dept.

Edward B. Talbot is Manager, Sandia National Laboratories, Computer and Network Security Department, which is responsible for Sandia California's network security operations (wired and wireless), the network security architecture, the Center for Cyber Defenders (CCD) program, and information security research. The department performs vulnerability analyses of networks and networked systems, provides operational support for third parties, and develops prototype systems for combating terrorism. He graduated from the DeVry Institute of Technology, Phoenix, with a BS in Electrical Engineering Technology in 1976. Upon graduation, he was employed by Sandia, where he worked on the development of the B83 bomb. In 1986, he obtained an MS in Computer Science at University of California at Davis. Over the years, he played leading roles in several other nuclear weapon programs, including the W89 (a cruise missile alternative warhead) and the W87. In 1996, he was appointed to the Fissile Material Disposition Program as the Lead Systems Engineer. In 2001, he was promoted to Manager of the Advanced Systems Department of the California Weapons Systems Engineering Center

Sandia Facilitators and Note Takers

John C. Cummings is a management consultant who retired from Sandia National Laboratories in 2008. He worked at Sandia for 32 years. He was a senior manager in the Advanced Concepts Group (a small think tank) and also served as the Director of a project on process control systems security research for the Institute for Information Infrastructure Protection (I3P). He was on assignment from Sandia in Washington, DC from 2003-2005 as the Director of the R&D program for critical infrastructure protection for the Science and Technology Directorate of the Department of Homeland Security (DHS), where he was Chair of the Infrastructure Subcommittee (of the National Science and Technology Council) and led an interagency effort to create the first National Plan for Research and Development in Support of Critical Infrastructure Protection. Just before that, he was the Deputy to the Chief Technology Officer at Sandia. He is a member of the Science Advisory

Committee the DHS Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California and of the American Physical Society Division of Fluid Dynamics. He has recently served on panels of the Defense Science Board and he was the U.S. representative to the International Atomic Energy Agency working on the mitigation of hydrogen combustion hazards in nuclear power plants. He received his BS, MS, and PhD (1973) degrees from Caltech.

Kathryn Hanselmann is a member of Sandia's Partnership Development & Business Intelligence group and currently works with the Information Operations Center supporting business planning. She holds an MBA from the University of New Mexico's Robert O. Anderson Graduate School of Management and joined Sandia in 2000.

Tom Karas is a Principal Member of Technical Staff at Sandia National Laboratories and a member of the Strategic Studies Dept., within the Institutional Development Center, since 2007. For 8 years he was a member of the Sandia Advanced Concepts Group, where he as worked on such diverse issues as bioterrorism, public health surveillance, border security, energy policy, transportation policy, the international security implications of global climate change, nuclear weapons policy, and, the implications of applying converging nano-, bio-, info-, and cognitive technologies to enhancing human cognitive capabilities. He began work at Sandia in the Systems Analysis Center, where first task was a review of the role of the Labs in the context of U.S. federal R&D Policy, followed by several projects relating to strategic nuclear arms control. For 13 years before that, he was at the Congressional Office of Technology Assessment (de-funded in 1995), where he participated in and directed extensive studies on space policy, missile defense, arms control verification, and proliferation of weapons of mass destruction. He holds a PhD in political science from Harvard and a BA in the same subject from Yale.

Judy Moore holds a PhD in mathematics from New Mexico State University (Infinite Abelian Groups), an MS in Mathematics from Texas A&M University (Point Set Topology) and a BA in Mathematics from North Texas State University. She spent more than 26 years at Sandia National Laboratories as a researcher and manager of research efforts—mostly in the field of information security and analysis. She began in 1981 as a researcher in cryptology and authentication and served as a mathematical consultant on a wide range of Sandia projects, especially in the command and control (C2) of nuclear weapons, where she specialized in both the design and analysis of C2 protocols. In 1990 she became a technical manager of groups which developed secure software systems for nuclear weapons use control systems, developed advanced concepts for nuclear weapon C2 systems, and performed cryptographic research and development. She served as a spokesperson for Sandia in "Information Surety"—a term coined by Sandia to refer to the balancing of information security, integrity and availability. From 1999 to 2006, she was a member of the Advanced Concepts Group, a "technical think tank," exploring the future problems of the nation and the way in which Sandia can contribute to solutions to those impending problems. In that role she developed with another researcher, John Whitley, an innovative workshop design for large scale brainstorming known as a "Fest." She is often sought for the design and facilitation of these Fests. Her last role at Sandia before her retirement early in 2008 was managing R&D in information assurance and information analysis techniques. She now does technical consulting in math, cyber security and workshop design as well as math education activities.

Lori Parrott is manager of the Strategic Studies Department, within the Institutional Development Center at Sandia, which conducts analyses and studies of national security-related concepts and issues for Lab leadership. Before joining Strategic Studies, she was a member of Sandia's Advanced Concepts Group, managed Sandia's corporate strategic planning and executive councils, and also served as lead Congressional Liaison for the laboratories. She holds a Masters of Science in Science Communications from Rensselaer Polytechnic Institute in Troy, NY, and a Bachelors in Earth Science (Geology) from Iowa State University.

Ricky Tam is a Senior member of the Technical Staff in the Business Development Support Office in the Sandia California Site Business Office.

Drew Walter is a Senior Member of the Technical Staff at Sandia National Laboratories, where he assists Lab executive leadership in exploring and defining long-term strategies as a member of the Strategic Studies Department. His current portfolio includes assisting in the development of a Lab-wide cyber security message and strategy. Before joining the department, he spent three years with Sandia's Security Systems and Technology Center designing and analyzing security systems for nuclear weapons and other applications, with

customers including the Department of Defense, Department of Energy, other government agencies, and private industry. His projects included several efforts to integrate cyber and physical security assessment methodologies for high consequence applications. Prior to joining Sandia, he earned a BS and MS in Mechanical Engineering from the Rochester Institute of Technology.

Distribution

2 MS 0899 Technical Library, 9536 (1 electronic and 1 paper copy)