Towards a National Information Strategy

Aligning Responsibility, Authority, and Capability to Provide for the Common Defense

1 September 1999

CENTER FOR INFORMATION
STRATEGY AND POLICY

SAIC
An Employee-Owned Company

SAIC strategies Group
Creating Knowledge, Integrating Solutions

Towards a National Information Strategy:

Aligning Responsibility, Authority, and Capability To Provide for the Common Defense

Jeffrey R. Cooper

1 September 1999

The Center for Information Strategy and Policy
Science Applications International Corporation
McLean, Virginia

Mr. Cooper is Director
Center for Information Strategy and Policy
and Chief Scientist,
The Strategies Group
Science Applications International Corporation.

The original research and report were produced under contract to the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence.
Contract Number GS-35F-4461G
Task Order Number DASW01-97-F-1475
Cleared for Open Publication 15 April 1999.
Revised 24 August 1999

All views and opinions expressed herein are
those of the Author and
do not necessarily reflect those of the
Center for Information Strategy and Policy (CISP)
or Science Applications International Corporation (SAIC).

This study is one in a series
sponsored by the Center for Information Strategy and Policy (CISP)
at Science Applications International Corporation (SAIC).

Understanding Information Warfare: Another View
Jeffrey R. Cooper

Kodak Moments: Inescapable Momentum, and the World Wide Web
Has the Infocomm Revolution Transformed Diplomacy
Dr. Stephen Cambone

The Radio Revolution
Christopher Burton

The Emerging Infosphere
Some Thoughts on Implications of the "Information Revolution"
Jeffrey R. Cooper

Copies of these may be obtained from:
http://www.cisp.org/
or by writing to:
Center for Information Strategy and Policy
Science Applications International Corporation
1710 Goodridge Drive, MS 1-9-3
McLean, Virginia 22102

Table of Contents

Section

Figures

Towards a National Information Strategy:

Aligning Responsibility, Authority, and Capability To Provide for the Common Defense

Jeffrey R. Cooper
Center for Information Strategy and Policy
12 August 1998
(Revised 24 August 1999; revised for publication 1 September 1999)

I. Introduction

The Information Revolution,[1] as with previous technological "disruptions," promises to bring another in the series of fundamental transformations in how society functions—across all its important dimensions. This is a revolution that has the potential to improve global welfare substantially, at the same time that it complicates our national security activities. It will create a radically new and different environment; in particular, the information age threatens to disrupt prevailing patterns of responsibility, authority, and capability—including how we plan and execute critical national security tasks. Unfortunately, the differences from our old circumstances, although profound, may be hard to recognize at first

[1] We define the Information Revolution as the significant increases in the combined capabilities (speed, reliability, effectiveness, and efficiency) to sense, gather, process, correlate, manipulate, compute, replicate, store, transmit, and communicate. For a lengthier exegesis, see Jeffrey Cooper, ***The Emerging Infosphere***, Center for Information Strategy and Policy, McLean, VA, October 1997.

glance;[2] and this opaqueness will significantly complicate framing needed policy initiatives to forge a new alignment of powers.

The United States is entering an increasingly communications-rich and information-dependent environment in which all of society is critically dependent on the proper functioning of its information systems (including communications). The economic, technological, and political dimensions of power, now recognized as key components of national security (along with military strength), are also heavily dependent on information and advanced information systems. In the developed world, individuals, organizations, or governments will not be able to choose to remain apart from the interconnected network of systems and relationships if they wish to function as part of society. An over-riding feature of this new environment, therefore, is "reciprocal dependency"—denoting sharing not only in the mutual benefits but also becoming both reliant on the information web in which we are all enmeshed and vulnerable to the actions and behaviors of others, whether intended or unintended. While this feature of reciprocal dependency may not be new, the speed and intensity of its occurrence do set it apart, as do the immediacy of the linkages to distant and unknown parties.

Along with benefits in which many will share, all revolutions impose costs on some parties—inevitable social realignments and redistribution of power create losers as well as winners. Benefits from the Information Revolution will not come without costs either. Beyond the issues of realignment and redistribution, a successful information culture must address four other sources of tension that arise from particular competing equities.[3]

- The first of these is that enhanced efficiency and increased effectiveness come at the price of a system that may only be dynamically stable.
- The second source is the "reciprocal dependency" of a society that is fully interconnected and thus vulnerable to the mistakes or malice of any of its participants.

---

[2] Exactly because we are living through these changes, it may be hard to discern how much has changed—to some extent because many of the external forms appear little altered. Walking into almost any office, the similarity of the objects—the desks, the chairs, the telephones—to those of the 1950s (or even earlier) hides the immense changes in processes and relationships galvanized by the new information technologies. It is a good example of the "boiling frog" story beloved by management consultants.

[3] While some might term these as four elements of a "Faustian bargain," this would almost certainly convey too strong a negative flavor with respect to the potential costs. As Alexis de Tocqueville observed about a free press: "Whoever should be able to create and maintain a tribunal of this kind would waste his time in pros- ecuting [sic] the liberty of the press; for he would be the absolute master of the whole community and would be as free to rid himself of the authors as of their writings. In this question, therefore, there is no medium between servitude and license; in order to enjoy the inestimable benefits that the liberty of the press ensures, it is necessary to submit to the inevitable evils that it creates. To expect to acquire the former and to escape the latter is to cherish one of those illusions which commonly mislead nations in their times of sickness when, tired with faction and exhausted by effort, they attempt to make hostile opinions and contrary principles coexist upon the same soil." Alexis de Toqueville, ***Democracy in America***, Book 1, Chapter 11. Hypertext edition, American Studies @ The University of Virginia, <http://xroads.virginia.edu/>, Hypertext Projects, <http://xroads.virginia.edu/~HYPER/DETOC/1_ch11.htm>.

- Third, interconnected systems and massive databases offer unprecedented access to information about almost everything, including most sensitive facts about individuals' private lives and organizations' internal matters; but the ability to access information remotely also offers an unparalleled veil of anonymity to knowledgeable users who may have malevolent intent.
- The fourth tension stems from the need to balance the benefits that come from a continuing flow of innovations against the innovators' refusal to accept responsibility or liability for their products.

The scope of these challenges demands not piecemeal attempts at solutions but a more integrated approach to addressing an environment that is being fundamentally transformed.[4] Therefore, to adapt successfully to this new information-dominated environment, we must create an entire culture appropriate to living with a technology that has the potential to threaten both individuals and society as a whole. Finding agreement on some common ground among the many parties at interest concerning how to balance the four sources of tension appears to be an important first step. Actions by government to foster trust are crucial so that a cooperative regime can be built.

Culture means accepted and ingrained behavioral norms and patterns of behavior, including appropriately supportive and reinforcing legal and formal structures. Thus, culture implies an underlying consensus among society's members on values; currently, there is little evidence that such a common sensibility exists concerning the shared as well as individual vulnerability to our the evolving information environment. Perhaps this is because we are still in a "pre-community" stage of sensibility, focused primarily on our own individual concerns, the systems that we interact with directly. We are not yet ready to take the necessary measures as a community and to address our collective security needs because we do not fully appreciate our circumstance of "shared risk" from reciprocal dependency.[5] In most cases, there is only a fragmentary understanding of these factors; and even less appreciation of the implications that will flow from them. However, here and there, some individuals, groups, and organizations have begun to show some appreciation of these issues and the complex interplay among them. Recent reports by the National Research Council[6] and the establishment by the government of the Computer Emergency Response Team (CERT) at Carnegie-Mellon University are hopeful signs of growing awareness, but widespread understanding remains elusive. Despite the issuance of Presidential Decision Direction-63 in May 1998, addressing the issues raised by the Presidential Commission on Critical Infrastructure Protection (PCCIP), there has been little real progress in either the public or private sectors in mitigating even the most critical vulnerabilities.

---

[4] Without wishing to sound too "New Age," it does seem important to grasp the impacts of the phenomena together, in a "holistic" or "Gestalt" manner.

[5] Moreover, there will be some who are unwilling to accept the concept of sharing risk collectively and others simply unwilling to participate in collective defense.

[6] National Research Council, ***For the Record: Protecting Electronic Health Information***, Computer Science and Telecommunications Board (CSTB), Washington, DC: National Academy Press, 1997.

Yet Americans should understand, better than most, the implications of revolutionary changes. Our nation was birthed by the American Revolution, not the American Revolt: we did not just change the ruling regime; we created an entirely new political (and later economic) system—and a new culture as well. Again, as observed by de Tocqueville:

> *They have all a lively faith in the perfectibility of man, they judge that the diffusion of knowledge must necessarily be advantageous, and the consequences of ignorance fatal; they all consider society as a body in a state of improvement, humanity as d [sic] changing scene, in which nothing is, or ought to be, permanent; and they admit that what appears to them today to be good, may be superseded by something better tomorrow.*[7]

In a sense, the Information Revolution may be recapitulating many of the social and economic phenomena of the Industrial Revolution, especially as it developed in 19th century Britain. As industrialization proceeded, there was a huge migration of the rural population to factories. This process changed the underlying social and economic structure of Great Britain, not least because of far-reaching urbanization. Longstanding social bonds and class restrictions of rural towns and villages were broken, and new social and commercial mechanisms developed to deal with encounters between previously unacquainted parties. Cities provided a space for diverse interactions and transactions, often fueled by these same new commercial arrangements, between people of different social classes that had rarely occurred in pre-Industrial England. Evolving procedures (including rules of etiquette) and new commercial arrangements had to address a degree of anonymity that simply did not exist previously in English village life. Moreover, cities had to evolve entire organizational structures that had not been needed in smaller, more settled communities, including the naming of streets and eventually the numbering of houses to help find people and businesses. The importance of intermediary institutions, such as banks and equity markets, and "trusted transactions,"[8] such as letters of credit, to facilitate business and financial interactions that demanded trust but in which personal or family familiarity as a guarantee was lacking between relatively unknown parties grew significantly. Furthermore, political structures and power balances, as well as economic institutions, needed to change in order to reflect new circumstances of wealth and influence, the result of redistributed power and social realignment.

Any assessment of the role of government and the extent of its legitimate functions, including how it exercises its powers, cannot ignore these types of changes. Of the many impacts that the Information Revolution portends, three are worth noting in this regard: from information scarcity to abundance, from top-down control towards coordination mechanisms, and from restricted one-way communications towards many-to-many networks. All of these have profound

---

[7] Toqueville, ***Democracy in America***, Book 1, Chapter 18.

[8] I want to thank Stephen J. Lukasik for this interesting notion.

political (as well as economic and social) effects. Thus, a key element in developing a national information policy and strategy suitable to living in the Information Age is to realign responsibility, authority, and capability consistent with the current transformation. *Responsibility* is defined here to mean the inherent obligation to address the problem. *Authority* is defined as the legitimated power to address the specified problem; it is granted through explicit delegation by the people (or, in some systems, seizure by *coup de main*), and it may possessed by several holders concurrently. Finally, *Capability* is the physical potential or expert competence to address the problem. Agreement on these issues must, however, be achieved within the bounds of our social compact if an acceptable solution is to be found.[9] How this is accomplished—that is, the choice of where to vest these powers and which instruments to use—must be consistent with our nation's political beliefs, economic system, and social fabric.

While many societies might choose, on the basis of their perceptions of efficiency and effectiveness, to place all these powers in the hands of the national government, the tradition in the United States has been to diffuse authority among levels of government (federal, state, and local) and, indeed, retain many powers in the hands of the people themselves. Whatever the frictional losses, Americans prefer foregoing the arguable advantages of centralized decision-making, believing that there is less risk in minimizing the powers granted to government.[10] Consistent with our federal form of government, even where the people are prepared to grant government the authority, the public often prefers to disperse that authority among many government hands; and this multi-level government involvement introduces substantial additional complexity. In many cases, rather than simply selecting among the various authorities, the choice is to grant concurrent authorities, thereby creating an intricate web of federal, state, and local relations that must be accommodated in any new initiative.

Therefore, solutions to these critical choices appear not in granting government more authorities and providing additional capabilities, especially through one or two pieces of broad legislative reach, but rather in learning how to induce, not order, appropriate actions by all the relevant players, most significantly individuals and private organizations. Civil society must be prompted to accept responsibility, perhaps through liability and contract enforcement, and employ its capabilities to protect its equities, not rely on government to protect vital information services.[11] By doing so, civil actors will also make a major contribution to

[9] This is an argument fundamentally about values and may be out-of-sync in a world that now demands econometric analysis of policy issues.

[10] Many, if not most, Americans would further argue, rather convincingly, that centralized decision-making is, in fact, less efficient as well as more dangerous. See David Brin, ***The Transparent Society***, Reading, MA: Addison-Wesley, 1998.

[11] At the same time, civil society should demand that governments facilitate, not hinder, appropriate self-help measures. At one point during the formulation of the Digital Millennium Copyright Act, reverse engineering, the process by which software code is deconstructed for a variety of legitimate research and development purposes, would have been deemed illegal. For a discussion, see Barbara Simons, "Outlawing Technology," ***Communications of the ACM***, 41 (October 1998), pps. 17–18.

addressing our national vulnerabilities; and very importantly, to the extent that private entities address these important needs, the less excuse there will be for intrusive and heavy-handed government intervention.

To a very large degree in the United States, the capabilities along with the necessary authorities to protect information and information systems, even those performing vital societal and national security functions (except for those clearly owned and operated by governments), already lie in the hands of private owners and operators. What is needed is for these powers to be exercised—in self and national interest. It should be noted that these perspectives on distributed power and more voluntary coordination are not fully shared around the globe; therefore, it is to be expected that these different perspectives will give rise to significant tensions as international agreements to reduce information vulnerability and enhance information security are sought.

II. The Problem of Public and Private Roles

It was not until the Great Depression in the 1930s, well into the 20th century and more than a full hundred years after the Industrial Revolution began, that the alignment of responsibility, authority, and capability among public and private actors was adjusted to conform with the altered political, economic, and social realities of the Industrial Age. Working out our arrangements for the Information Age will likely take a substantial period of time; adaptation to revolution is, by necessity, a long-term process. How we choose to realign and balance these three critical powers tells us much about our view of the social contract.

Communism and National Socialism employed authoritarian versions of the social contract in order to overcome the problems created by advanced industrial economies. Communism took responsibility from the people and lodged both authority and capability within the Party (as the vanguard of the proletariat), by fiat giving it control through state ownership of the means of production over the vast capabilities in the hands of the Soviet Union. Nazi Germany, on the other hand, although also favoring centralized (in the Reich) as opposed to individual responsibility, left most production capabilities in private hands—but gave the state sufficient (and often lethal) authority to mobilize the nation's resources. Franklin Roosevelt, on the other hand, intended to perfect a democratic social contract appropriate to the Industrial Revolution by realigning responsibility, authority, and capability consistent with his vision of American values. Despite many calls from the left and the right to place far more powers in government hands, Roosevelt's "New Deal" version of the social contract gave the government not total but sufficient regulatory and tax authorities to force the private sector to exercise its capabilities to meet the national responsibility for social welfare. While Social Security transferred this function to the government, most other functions (such as strengthened anti-trust and price controls) were exercised by regulatory oversight of private entities.

Consistent with that notion of separated powers, the critical triumvirate of powers—Authority, Responsibility, and Capability—for protecting the nation's information infrastructure is currently diffused among many actors in the United States. Even within the government domain, these powers must be shared among federal, state, and local levels; and at each level, there may be several institutional claimants. Rarely are the magnitudes of these three powers properly balanced, and even less frequently do the same entities wield a consistent share of the powers, making it feasible to exercise them effectively. Moreover, this imperfect overlap, not unlike our constitutional separation of powers, is viewed differently by each of the key actors in this area—the people, the government, and most of the commercial sector—with respect to how much of each power resides, or should reside, where. And it is these differing perspectives—grounded in fundamentally disparate appreciations of the critical equities at stake—that make it difficult to reach agreement on the best way to address our national information infrastructure protection problem.

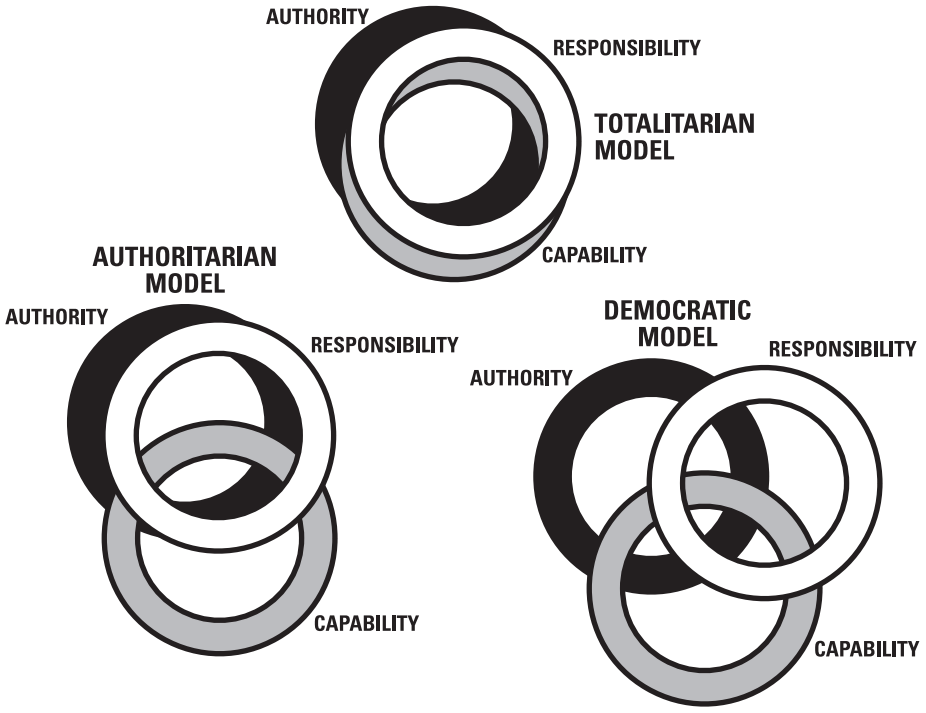

Figure 1. Social Compacts and Configurations of Power

A. The National Security Problem and Government's Role

Governments do have important, but clearly circumscribed, roles to play with respect to the use of information and the protection of information and information systems. These potential roles encompass a wide range of areas and activities; and it is important to disaggregate and distinguish among them, especially to understand the historic and legal limitations. Most clearly recognized and widely

accepted among these responsibilities for the federal government are instances of direct national security threats, such as overt attacks by a hostile foreign power against military information systems. Probably next, in terms of overall acceptance, would be law enforcement powers related to protection to the civil information systems critical to the national infrastructure against terrorist threats and against criminal activities, such as extortion threats, which are consistent with other existing protections for private property.

However, direct government involvement in protection of information itself (other than safeguarding classified and other government-owned information) raises difficult problems with respect to both propriety and public acceptance of a government role. Especially given our historic First Amendment protections for speech (as broadly understood in light of court holdings), direct government involvement in protecting private information raises uneasy issues that may be better left alone. In this area, perhaps the most important and acceptable government role lies in establishing appropriate legal frameworks and structures that facilitate individual and collective self-defense.

Existing legal authorities granted to the government in sensitive areas such as national defense, intelligence, and law enforcement offer a range of potential models that could be applied to information. At one end, the McMahon Act of 1954 (Atomic Energy Act of 1954, as amended) granted the federal government sole and complete authority over atomic weapons *information* as well as materials, including the authority to use deadly force for its protection. Somewhat less inclusively, the Internal Security Act gave the federal government, among other authorities, the right to control access to specified facilities; and this also required people entering those facilities to allow a range of intrusive searches that would not otherwise be permitted absent "probable cause." At the other end of the spectrum, lethal force against criminals is authorized but only in limited and specifically defined circumstances, and there are strong constitutional protections against government intrusion (or even investigation) without probable cause.

There are currently, however, substantial difficulties even in defining the most appropriate federal government role in protecting information and information systems related to its traditionally recognized mandate for national security. *Mandate* usually implies a coupling of authority and responsibility. During the Cold War, within the then traditionally understood context of national security, the U.S. government clearly had such a mandate; in the post-Cold War era, however, that coupling is substantially less clear. Today, the federal government is not accorded either overt authority over or explicit responsibility for protection of the entire national information domain—although it is important to recognize that it is likely to be held accountable for any major disruption. This combination of antithetical views creates an unusually complex terrain over which national information policy must navigate. And as a result of two distinct changes in our national attitude, defining appropriate roles for both public and private entities is extraordinarily complicated.

First, national security in the United States has been historically understood to mean primarily defense against physical attack by external military forces (although during the Cold War prevention of ideological infection and subversion became an additional element). Governments have historically held a monopoly of the means of legitimate violence, the classical expression of sovereign power; and they have often held a real monopoly on the ability to wield violence on a large scale. Coupled with the clear constitutional mandate for the common defense, the U.S. government, therefore, was (and, as importantly, was seen to be) uniquely competent to address national security problems, especially when they presented themselves in the classic forms of overt threats by a hostile foreign government. When it is clearly a direct hostile foreign threat to national security, the federal government holds a significantly more coherent set of powers (the central shaded area representing the area of congruency or overlap), as notionally highlighted in Figure 2 below, than in the diffused separation of powers model previously shown in Figure 1.

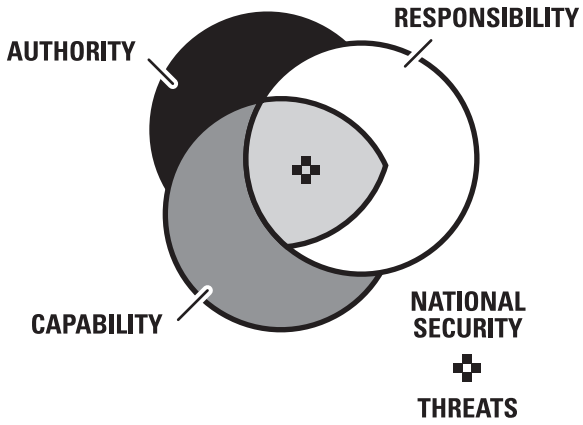

Figure 2. National Security Powers Are More Concentrated

However, an increasingly important information policy issue includes the use of information to enhance national power and influence—"soft power"—as well as the creation of an appropriate environment for responsible information behaviors by private parties.[12] In these areas, the appropriate government role is less clear. In addition to the traditional application of force with military instruments, the economic, technological, political, and social dimensions that were long regarded as adjunct elements of national power and influence are now recognized as key components of national security. This influence has been termed "soft power."[13] In particular, the information component is increasingly viewed as a major

[12] These information behaviors include, among others, limitations on access to pornography, privacy of medical information and other sensitive personal information, corporate information and lobbying on behalf of foreign interests; all are frought with extraordinarily contentious disagreements over government's legitimate interests and powers.

[13] Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," ***Foreign Affairs,*** March/April 1996, Vol. 75 No. 2, pps. 20–36.

element of national influence, both directly and as it undergirds the other components, providing the key links among the other elements of critical national infrastructures.

Information technology makes new kinds of political and economic interactions possible. New technologies to disseminate knowledge and ideas, including socio-cultural concepts. They also affect relations among actors and affect the political process within state actors by providing tools to increase the efficiency and accountability of the state's leadership or governments. Thus, they tend to democratize organizational processes. Perhaps the most significant component of "soft power" arises not from government information activities but from those undertaken by the private in pursuit of its own interests, economic or otherwise. In employing information as an essential component of national influence, however, it is not clear that most Americans would accord government the sole right to speak for the American people. Therefore, as national security has acquired a significantly broader (and more diffuse) meaning, government efforts in the information domain have been increasingly hobbled by this growing lack of clarity as to where are the boundaries of the national security domain.

The problem is now particularly acute because a critical element of national security is the entire national information infrastructure (NII)—no longer just the government-controlled defense information infrastructure (DII). About 95% of DoD message traffic flows over the public switched telephone network; and as an actual exercise demonstrated, both unclassified public and secure DoD information resources are at risk from external and internal attacks.[14] In today's information technology domain, government no longer possesses the clear advantages in resources and expertise, much less a monopoly of these capabilities, needed to address threats to our national information systems.[15] While the government has always relied upon the national telecommunications infrastructure, until recently most sensitive operational communications employed a separate (and largely government owned, controlled, and operated) DII that was effectively segregated from the national information infrastructure.

As we look towards the future, moreover, the military will increasingly become simply one more user of commercial systems and services that flow from a seamless national and global information infrastructure (GII). National security users will no longer be isolated within a distinct DII, but inextricably dependent on the NII; and government powers will inevitably diminish still further. As illustrated by recent spectrum allocation decisions, military users and national security equities are no longer automatically accorded priority of interests. Furthermore, in addressing the entire range of threats to or through the informa-

[14] The exercise, ***Eligible Receiver***, which took place in 1997, was widely reported in the U.S. and European press in 1998.

[15] However, while the reality has changed with respect to the possession of technical capabilities, the perception lingers on that government does possess unrivaled secret capabilities—perhaps fostered, and not unintentionally, by those, both in government and outside, with agendas to be served by this view.

tion domain that could affect national security, the real threats are not likely to be either a classic overt attack across a demarcated border or a covert act of subversion by an identifiable foreign state. Although most Americans undoubtedly assume that the federal government has sufficient powers in the national security domain, the coherence of these important powers is significantly less than it used to be when the boundaries of the national security domain could be more clearly delineated.

Unfortunately, as a result of the view that safeguarding national security is primarily a government responsibility, we have been forced to adopt one of two existing models that rely on government action for addressing threats to the nation's critically important information infrastructure. Neither, in light of the new factors, is now a particularly satisfactory approach in dealing with the new information challenges. Under these older models, government responses to malign activities can take, in general, one of two response forms: First, they can be within the *law enforcement/criminal justice* paradigm in which prosecution of the offender is the primary objective. Second, they can be within the *national security* paradigm, wherein effective responsive action to prevent harm is the preferred rejoinder. The American criminal justice model, with its goal as the apprehension and successful prosecution of the offender, is especially sensitive to Constitutional and legal constraints on investigative and prosecutorial powers. It must weigh carefully the balance between apprehending the guilty and protecting the rights of the innocent. It is, therefore, particularly careful to satisfy issues of "probable cause" and "chains of evidence" so as not to contaminate a successful case.

Moreover, the criminal justice paradigm is still fundamentally an *ex post* model, despite recent attempts to expand information gathering before crimes are committed—one focused on prosecution of malefactors, that operates best after the crime has been committed. The American national security model, on the other hand, especially in its post-Pearl Harbor incarnation, establishes vigilance and prompt, effective intervention as the dominant priorities in order to prevent irreversible damage. Exactly because of the stakes, action under the national security model does not wait until after fact. As a result, however, there is greater likelihood that innocent bystanders as well as the guilty may suffer damage from the response. With the difficulty of distinguishing between accidents, malicious acts, criminal activities, foreign intelligence operations, and hostile actions by foreign states, the *multiple* response regimes substantially complicate *effective* responses. Moreover, the suitability of either of these models is significantly compromised by the diffusion of powers.

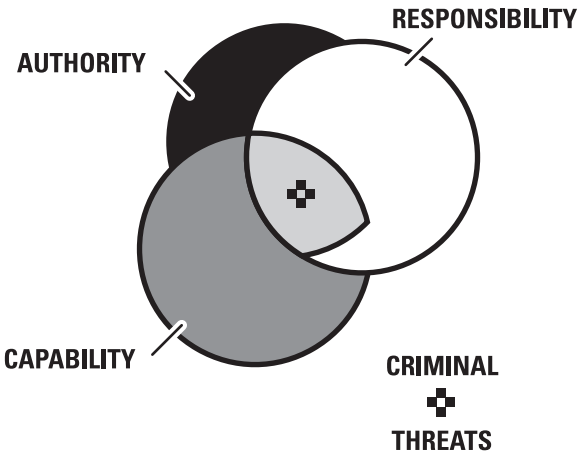

Figure 3. More Coherence of Critical Powers in Some Areas

As one looks at the map of critical powers for addressing criminal threats to information, notionally illustrated in Figure 3 above, there is less coherence among the powers than in the direct national security case shown previously. Authorities are dispersed among a variety of government agencies—federal, state, and local; and those authorities are further constrained by strong constitutional restrictions designed to protect civil rights. Furthermore, many of these government actors who hold authorities have extremely limited technical capabilities to deal with information-related crimes. Perhaps most importantly, the American people are unwilling to lodge as great a concentration of powers in government hands for this problem as for direct threats to the national security.

Exactly because the American people believe that the federal government holds the preeminent responsibility for safeguarding national security, however, most people also assume that the federal government is responsible for protecting the information infrastructure as a matter of national security.[16] Yet few members of the general public understand that the federal government lacks either the statutory authority over most elements in the NII or the physical and technical capabilities to protect against attacks since most of the physical infrastructure is outside direct government control. Some in government, however, have seen these limited powers versus the perceived needs as an opportunity to expand their authority; as a result, they sought increased authorities in order to execute those perceived responsibilities in spite of their lack of capabilities.[17] Much of the private sector, however, finds this course of action to be profoundly unsettling, perhaps most of all those in the information technology sector.

[16] This is not unlike consistent beliefs, shown in national survey data of the American public, that the U.S. possesses a working ballistic missile defense system capable of protecting the continental U.S.

[17] Unfortunately, by failing to realistically portray the capabilities that government does possess, and sometimes continuing to cloak itself in the Cold War-carryover of technical omnipotence, the government has allowed the private sector to retreat from its responsibilities to protect the common defense.

For a variety of reasons (including a pervasive distrust of many government agencies), there is now substantially less inclination to grant the government formal protective *authority* over the parts of the national information infrastructure that lie outside of government's direct control. Moreover, even if government today had the authority, it lacks the capability (the ownership or management of the physical systems) to address most threats to national security that could arise through information systems. Not only has deregulation of the telecommunications sector removed many of the authorities that government previously possessed, but also the resulting decentralized industry structure has made it significantly more difficult for government to harness the technical capabilities that do exist by exhortation or calls to industry leadership. These are not the "good old days" when government could call upon Ma Bell to fix communications infrastructure problems affecting national security and expect quiescent federal and state regulatory bodies to pass those costs on to the consumers.

As a result of these trends, with respect to protecting the nation's information infrastructure from other than overt attacks by a hostile foreign opponent, the critical triumvirate of powers—Authority, Responsibility, and Capability—as notionally illustrated in Figure 4 below, is currently diffused among many private and public actors, and levels of government as well, in the United States. Indeed, the shaded area in Figure 4 probably represents, albeit conceptually, the government's very limited set of coherent powers with respect to protection of the national information infrastructure when the threat is other than direct attack.

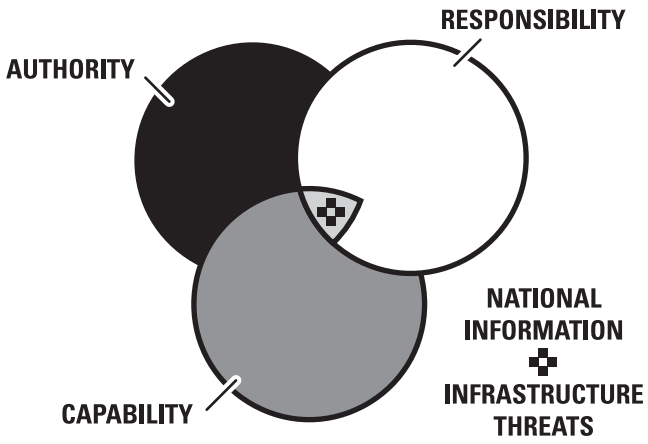

Figure 4. Critical Powers Are Widely Separated

While we often think in terms of these three sets of perspectives (government, industry, and the public), there are, in fact, actually at least four views as to where the critical powers should be vested. Within the commercial sector itself, the information technology providers exhibit distinct interests from commercial IT users and, therefore, present a very different fourth perspective. In general, the information technology sector has attempted to maintain a position that denies any legal responsibility for the performance of its products, thus shielding itself from potential liability concerns. It relies on mandatory contractual agreements

by the purchasers to remove any traditional "implied warranty" for its products. Especially as advanced information devices have diffused rapidly throughout society and become mass-market items, this traditional attitude held by suppliers towards responsibility for their products needs careful review. Serving a mass market implies that these items are now being used by a wide range of ordinary people without special training or specialized knowledge and the products should, therefore, have been designed as appliances.[18] There is a critical distinction between tools and appliances, and between their users; and there should be a difference in the responsibility of those who supply these two classes of products that reflect these important distinctions. While strongly recommending that government not directly intervene, the government could take measured steps to facilitate market pressures (including its own purchases) that reinforce vendors' attention to security and vulnerability concerns and support court cases to test the bounds on these important public policy issues.

In industry's overall view, dealing with threats to national security, including to the NII (and to the DII embedded within), is clearly the government's responsibility alone; and industry does not wish to be saddled with responsibilities in this area.[19] This attitude is now widespread despite the fact that American industry has, in the past, accepted that it is a key participant in protecting the nation's security. There are many reasons for this position, but the most salient appears to be concerns: 1) that the national security mission is beyond the private sector's capability (and certainly responsibility); 2) that based on such a role, mandated, but unfunded, regulatory requirements for information protection might be created; and 3) that liability for failures in information assurance might then accrue, even to those who tried in good faith.[20] At the same time, it certainly does not appear that industry is prepared to grant the government additional authority or capability since industry believes that would be an unwise intrusion into private sector affairs. This view on additional government powers, in fact, extends well beyond the national security problem, although that is clearly a crucial dimension of the overall information vulnerability problem. However, the perception of government competency (with respect to information issues) that exists in many quarters, and the pervasive impact of government edicts and actions (compared with those of almost any other actor), together creates a situation in which many

[18] See pps. 35–42, in Burton, ***The Radio Revolution***, for a discussion of how new innovations are progressively adopted throughout society. If we are to allow almost anyone to use interconnected information devices, then they should be appliances, which are intuitive and not require significant expertise for proper functioning, especially if they carry substantial externalities for the rest of society. If, on the other hand, we are not prepared to address and mitigate the vulnerabilities from reciprocal dependency, we should examine other mass-market models such as the automobile—one that does require licensing for use exactly because of the potential for adverse societal impacts from accident or misuse.

[19] This was clearly expressed by many in the IT sector during the deliberations of the President's Commission on Critical Infrastructure Protection (PCCIP).

[20] Recent legislative initiatives to provide "safe harbor" protection for companies that make good faith efforts to address their Year 2000 problems might be a useful model. There is a careful balance that needs to be recognized, however, between prompting useful efforts and spurring "moral hazard" by making the safe harbor too attractive.

other actors feel that addressing the diverse range of important information policy issues can easily be left until government takes the lead.[21]

Indeed, the different perspectives on who holds the important powers (and who should hold them) exist throughout the domain of information-related problems; and the farther any problem is viewed as being legitimately related to direct national security concerns, the greater the tension over the governmental role, and especially over the granting of additional authorities to government.[22] While there are important roles for government in other information matters "less serious" than national security, the same problem of lack of correspondence of these three powers is even more in evidence. It would be useful to examine in some detail how, for a spectrum of information-related problems (perhaps ranging from "noise" through major system disruptions), responsibility, authority, and capability are apportioned among the holders of these powers: from individuals and organizations in the private sector, through specific government entities, to society as a whole. By conducting this examination, we can begin to understand how profound the divergence is among these critical powers of where they really reside.

At the level of "noise," we are dealing with low-level but annoying activities and misdemeanor criminal incidents, such as simple "breaking and entering" into information sites or illicit "not-for-profit" software copying—the information analog to shoplifting in degree of seriousness. While some vandalism may occur (such as defacing a website), equivalent to spray painting graffiti in the physical environment, no serious or long-term damage is intended. At this level, immediate response to an incident is very likely to be in the hands of individual or organization whose system has been disrupted or damaged since we are unlikely to provide sufficient and sufficient law enforcement resources for police to be ubiquitous. However, we could create a Hobbesian world in which all actors must take any measures in self-defense of themselves or their property that they deem appropriate. If we are to reject this approach, then it is essential that society establish both rules of behavior and appropriate legal sanctions to warn potential transgressors and to establish enforceable norms, and must also provide the necessary enforcement mechanisms. At the same time, although society itself is likely to take only a passive stance in terms of protecting others' property (like the bystander on the street during a crime), enforcement and prosecution authorities must be exercised by capable hands if the anticipated norms are to be upheld.

At the other end of the incident spectrum where significant disruption to society is threatened, even beyond national security incidents, here too the authority

[21] Or, at least, some might argue that their actions should be left unfettered until government develops a policy.

[22] Trust relationships in the information area between government (both executive and legislative branches) and industry have diminished greatly, sparked by many serious disagreements over policy, including the Communications Decency Act, intellectual property issues, and, of course, encryption policy. See "The Great…Debate," ***Business Week***, March 9, 1998, p. 38.

and capability for remediation if not prevention lie largely in private hands.[23] At this level are incidents (natural or human disasters) that could threaten the functioning of critical information-dependent infrastructures, such as national telecommunications, regional power and water services, or rail transportation, leading to substantial disruptions, immediate physical damage, and potentially significant loss of life and bringing society to a halt. In most cases, the private owners of these systems will have to take the protective or remedial activities themselves; and in large-scale incidents they may be aided by cooperative agreements with peers to supply assistance. For example, while National Guard and local emergency services personnel responded to massive power and telephone service outages in the wake the eastern ice storms in January 1998, it was the crews from the privately owned companies that actually brought the systems back into operation. Instructively, the power of the federal government to force companies to address their Year 2000 problems lies, in most cases, in education and exhortation, not in the authority to compel action directly. But creating corporate liability, including directors and officers, for lack of Y2K diligence, as the Securities and Exchange Commission (SEC) did in establishing a mandatory 10(k) reporting requirement as a material matter, can be an effective way of bringing financial self-interest of private parties to bear on a potential national problem.

In between these two poles of severity, there is a range of potential problems, in which we have placed illustrative markers at four points: competitive advantage, entity survival, system-level disruption, and national security problems (which has already been discussed extensively). Competitive-advantage incidents might involve misuse or theft of key intellectual property (such as a trade-secret drug manufacturing process) or intentional disruption of a company's key information or just-in-time manufacturing systems (by a competitor or extortionist). While both civil and criminal statutes relevant to these threats exist, prosecution of these types of incidents rests largely in the hands of the affected parties.[24] Incidents threatening entity survival could arise from willful, intentional destruction of critical databases and systems or to their loss from negligence or stupidity. Again, society draws the line with respect to the standards of fair play; but in most cases, vigilance must come from the interested party. Finally, system-level threats are similar in character to those that could affect society as a whole, but are simply more restricted in scope and scale.

While the public may believe that protecting the national information infrastructure from major systemic disruption is a federal responsibility, they are not likely to appreciate how circumscribed are the federal authorities and capabili-

[23] There are certain key infrastructures, such as the air traffic control system, where both authority and capability lie in government hands; but these instances are relatively rare. If the incidents involving other infrastructures were carried out by terrorists, then the government would have authority but would probably not possess the physical remediation capability.

[24] Concern over the magnitude of the potential losses, not only to the particular company but to national economic competitiveness, led to the Economic Espionage Act of 1996, which put strong federal criminal sanctions in place.

ties.[25] Furthermore, most capabilities (technical expertise and physical equipment) for information systems reside in private hands; and increasingly, with deregulation, they also lie outside of effective government control mechanisms. And, more and more, while we may be able to identify who holds these powers for the discrete pieces of our national information infrastructure, it is difficult to tell who holds them for the system as a whole.

From an overall viewpoint, we are likely to find that, for any level of information problem, these powers will lie dispersed in different hands; and there may well be cross-cutting equities that divide sector peers. Furthermore, the solution is not to make these powers more coherent (or even to clarify the boundaries) or concentrate them in the hands of one entity—especially that of the federal government. Indeed, this would simply trample over serious issues of federal/state/local relations, much less run counter to current sentiments on increasing federal powers in the information domain. Rather, more tractable solutions might result from building cooperative structures among the key parties—government, industry, and the public (and within each group). For example, at the level of information "noise," problems in the information domain are akin to low-level street crimes or shoplifting; they may include classic hacking or cracking, corruption of web-sites, small-scale software piracy, or similar problems. Just as with shoplifting, we are unlikely to post information policemen in each store or site to deter these activities. The first line of defense will be the owners or operators of the systems affected. But their effective response must be underwritten by societal norms and laws that make these activities, just like shoplifting, not only a crime, but also a generally perceived violation of acceptable patterns of behavior.[26] Furthermore, we must allow the owner to apprehend the offender (with all the potential issues of false arrest and liability for violations of rights); and, most importantly, we must press for effective enforcement and prosecution—committing the government to taking these crimes seriously.

Ultimately, in these areas, the government's paramount responsibilities are: 1) to provide "rules of the road" that foster respect for appropriate behaviors and establish behavioral norms; 2) to allow other parties to accept their appropriate responsibility and exercise their capabilities; and 3) to commit to vigorous prosecution when criminal information incidents occur. Over the past several years, legislative actions to define criminal activities with respect to information systems, coupled with increasingly effective and publicized prosecutions for violations of those rules, have begun to establish societally acceptable guidelines for behavior.

[25] For example, the Telecommunications Deregulation Act of 1996 removed the ability of the federal government to impose a "fitness test" (for technical, financial, managerial, or ethical competence) on telecommunications service providers (TSPs). It, furthermore, required that the regional telephone operating companies allow TSPs to hook-up wherever technically feasible.

[26] Simply criminalizing low-level information offenses runs the real risk, as did Prohibition, of engendering widespread disregard for the law. The more important aspect is to create strong social norms against these behaviors so that they are not tolerated; resort to law is the sanction, not the barrier. Good examples are the strong social barriers in Switzerland to littering or fare-jumping on public transport.

These actions by government are crucial to building trust, which is the essential element of a cooperative regime; and, therefore, they underpin the overall framework for collective self-defense by the entire information community. Without non-government entities and private individuals playing a major role in securing the information infrastructure, it is clear that government will not be able to execute its responsibilities for information-age national security. Indeed, given the current lack of coincidence among the three critical powers of responsibility, authority, and capability, private users may have the best opportunity to align them in dealing with information problems throughout the entire spectrum of potential incidents. Private entities may be able to accomplish prevention and remediation of many impacts within the context of an "information community" most efficiently and at least cost.

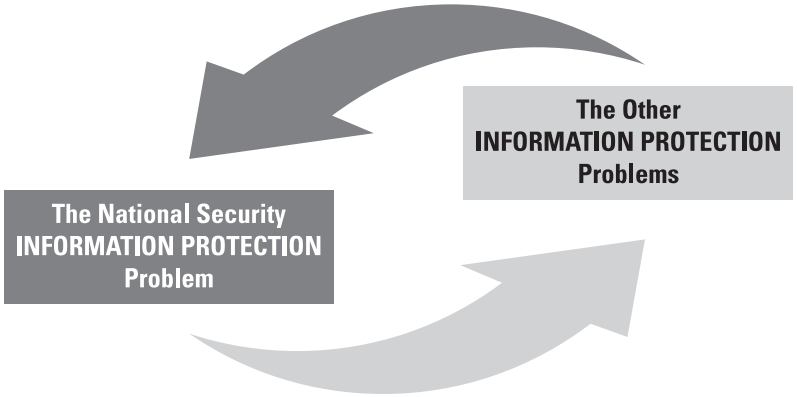

Figure 5. The National Security Conundrum

In this new information environment, while formal delegation of authority to the government, at any level, might be the conceptually simplest solution, within the context of the American social contract, it would not be easy or feasible to adopt this approach for protection of the web of information-related activities; and, moreover, it is not clear that such delegation would be effective even if it were attempted. While government holds no monopoly of expertise in this area, it does have a potentially valuable role to play in helping to validate those sources of capability—both expertise and physical tools—in the private sector that both parties can use to protect themselves. Knowledge about those capabilities is important in understanding where best to vest authority.

B. The Conundrum of Private Responsibility

One of the less remarked consequences of the Cold War's "long twilight struggle"[27] was the transformation of the American notion of the Common Defense. As noted previously, we were born as a militia-based nation; and throughout most of our history, we maintained only a very small standing army,

[27] See Michael J. Hogan, ***A Cross of Iron: Harry S. Truman and the Origins of the National Security State,*** Cambridge: Cambridge University Press, 1998.

supplemented as needed by conscription or short-term volunteer military forces. However, the perceived Manichean nature of the superpower conflict set in motion forces that created a huge national security apparatus, with a very large standing military force. In the wake of the Vietnam War, the United States abandoned conscription and created a fully professional military. As a side effect of this change, national defense was increasingly seen as solely a government responsibility—specifically a federal government responsibility—and one that was too technical and abstruse for the common citizen. Moreover, especially with the nuclear overhang, while a national security failure threatened every citizen, involvement with national security seemed tangential to citizens' daily lives.

Having just come out of that Cold War era, the government itself is still wrestling with the new meaning of national security and how far its writ extends in this new environment. The debates over the past few years about whether there is an appropriate role for government intelligence agencies in assisting private businesses is symptomatic. Therefore, it is perhaps not surprising, as we have recently entered the Information Age, that private organizations as well as most individual Americans do not yet appreciate that their role and responsibilities with respect to the national defense are once again shifting. In this new environment—a global infosphere in which nearly all elements are increasingly and seamlessly connected—the reality is that most individuals and private organizations do have major impacts on national security, either through acts of commission or omission in the information domain.[28] Once again, as they did at the time of this nation's founding, the American people and the civil society of which they are a part will have to play more direct roles in "the common defense," befitting a militia-nation. Although it is probably too early to expect this to be fully perceived in the near future, it is important that steps be taken now to indicate the implications of an information-dependent society so that the American people once again will be prepared to assume this more direct role in their own defense; education about these important issues should be a priority on the federal information agenda.

The interplay of the altered character of national security and the relationship of information to it produces two key, and self-reinforcing, connections. First, not only the military, but also the economic, technological, and political dimensions of power—all of which have become heavily dependent on information and advanced information systems—are now recognized as key components of national security. Second, it is not easy to understand how closely the inexorable progression of advanced information technologies is tying defense and other government information systems, and the critical national infrastructures, to all information infrastructure users—both domestically and internationally. And this is creating a single global infosphere of seamless reciprocal dependency. It will clearly take time before individual citizens and private organizations appreciate

[28] Some members will choose, or be forced by circumstances, to remain largely unconnected. And some other sophisticated users may choose to exist as "islands" in the stream—able to control the terms and circumstances of their connectivity.

and internalize this profound transformation in the meaning of national security and their now inextricable inter-relationship with it.

It is not necessary for this transformation to be complete or fully comprehended, however, before private entities can begin to play a more constructive role that assists and enhances national security.[29] Nor must businesses and individuals accept explicit, even if partial, responsibility for national defense before they can take concrete measures that will significantly help in securing information vulnerabilities that could threaten the nation's fundamental security.[30] What is required is a careful explication of their own self-interest—even narrowly defined and without calls to patriotism. At the macro level every user is increasingly dependent on the proper functioning of information systems, as well as of the other critical infrastructures that rely on them in a closely-coupled, complex system which lies outside of our individual control and management. Therefore, while there are limited measures that individuals may undertake to provide protection and resilience (such as firewalls and other access controls, user authentication, back-ups, and file encryption) and so reduce their exposure to disruptions in these systems—completely protection from the adverse effects of widespread disruptions to public systems is unlikely. Furthermore, this vulnerability should not blind us to the fact that at the micro level we are also increasingly dependent on information systems that we do control. But even these cannot be segregated from the national or global information infrastructures without losing much of the value created by advanced information technologies.[31]

This situation, in essence, creates an "information commons"—in which there are few barriers to entry, and in which involuntarily shared risks and exposure to the consequences of the acts of others are automatic. In other words, these same characteristics of an information-dependent society—the advantages of nearly instant connectivity and access to a wealth of information resources—also create a series of "security and vulnerability externalities" that result in an extremely high degree of reciprocal dependency among all elements of the community. Under these circumstances, even accidents and negligence, much less malicious acts by others, can create serious, even catastrophic, impacts not only on individuals and private entities but also on the nation's general welfare and common defense.

---

[29] Complicating such efforts to harness commercial capabilities to enhance national security may be the ongoing process of multilateralization and globalization. As more companies see themselves as "global citizens," there is a corresponding decrease in definability of corporate nationality. Indeed, there may well be cross-cutting national loyalties at play. Therefore, focus on corporate self-interest and commercial advantage rather than appeals to "support the flag" will be essential to getting the commercial sector to address security and operational vulnerabilities.

[30] This is really not that much different than settler families on the American frontier defending their homesteads from hostile attack; it substantially reduced the overall problem of defending the frontier.

[31] The duality of the vulnerability has profound implications for all users, but especially for organizations that provide critical products or services—whether energy and water, emergency services such as fire and police, national security, telecommunications and financial transactions, or other critical business functions. Plans for providing both continuity and restoration of services must look well beyond those components or segments that an organization directly controls.

All information users actually have self-interested reasons, therefore, to recognize the potential society-wide consequences of information disruption or corruption. Moreover, they need to appreciate how little government is able to shield them from these consequences (although government may have a central role in ameliorating them). However, in spite of this crucial dependency on interconnected information systems and recognition of its potential dangers, only a few commercial sectors (such as banking and finance) or private individuals have taken steps to address their vulnerabilities or prepare ameliorative responses for when disruption or damage does occur.[32] This should not be totally surprising in light of our experience with Y2K preparation; until the SEC made Y2K a mandatory Form 10(k) reporting item as a "material factor," there was little attention from senior executives in most commercial sectors. This is the reason why the entire private sector must adopt significantly more rigorous practices of care in how they deal with information and information systems.[33]

In essence, we have adopted these new information capabilities as key elements of our national infrastructure (for government, industry, and private citizens) and implicitly treated them as if they functioned like old fashioned utilities under regulated rates of return—with near-zero outages and guaranteed availability—when, in fact, due to the nature of deregulated or unregulated industries, unless the customer demands (and is willing to pay for) it, they make no special provisions for availability, security, robustness or resiliency. Users of these information systems also need to recognize, however, the potential impacts of their own activities on others. As a result, *all* users of information systems need to accept responsibility for their own actions and consequences of their activities; and at the very least, they should be prepared to take minimal steps to shield themselves from the consequences of others' actions. While it may be difficult through legal or regulatory mechanisms to force users to take measures to protect themselves,[34] there may be more creative opportunities to force actions that would safeguard innocent third-parties (perhaps through liability mechanisms) from the mistakes or malevolence use of these systems.

It is unlikely that Americans will be prepared to grant the federal government additional powers before United States experiences a major cyber-attack by a hostile foreign power or terrorist group. This would correspond almost exactly to the pattern after the World Trade Center and Oklahoma City bombings with the passage of the Counterterrorism Act.[35] Thus, prior to such a major catastrophic

[32] Several incidents over the past few years raise concern in this regard: in the face of system outages that have affected VSAT and frame relay availability (often used for credit card verification), many retail stores found themselves unable to process sales and they had no back-up procedures.

[33] Unfortunately, in the absence of stronger forcing functions, many are not likely to take these injunctions seriously until they experience such incidents; there are limits to the power of education and exhortation.

[34] As the limited results of exhortatory anti-smoking, drunk-driving, and seat-belt campaigns testify.

[35] Similar comments have been made by the U.S. emergency medical community with respect to preparations for handling a major chemical or biological incident such as the Aum Shinrikyo attack in Tokyo on March 20, 1995.

incident (perhaps a "Cyber World Trade Center" attack) that would demand immediate federal intervention, government's most important role may be in enabling or encouraging a set of perceptions that helps to instill a sense of responsibility, as well as competence, within non-governmental entities so that the substantial capabilities in their hands can be exercised effectively. This must be a multi-part effort designed to induce the private parties responsible for information systems not only to accept their proper responsibilities, but also to use the authorities and capabilities that they possess. Moreover, these activities must help to create the perception among information systems users that other parties will take their responsibilities seriously and will actively respond when collective self-help is needed. Importantly, the government may struggle with these steps because they require that the government openly acknowledge its limited role and capabilities.

Private users have direct incentives to address threats to their own interests; and to a large extent, securing against these threats would dramatically simplify the government's task in addressing what are clearly national security threats. To the extent that private actors—both individuals and organizations—can be encouraged to undertake responsible actions, these measures will foreclose a substantial fraction of potential trouble sources that could propagate and have societal, not just private, impacts—including serious adverse impacts on national security. Moreover, reducing the number of anomalous incidents, lowering the "noise" level, will also reduce the complexity of the national security problem by allowing government to easily recognize the more serious or malign activities—such as acts by hostile nations, terrorists, or criminals—that are in its domain of authority. Perhaps more importantly, careful, responsible use of information systems by private parties will reduce the number of potential access points for actors with malign intent.

It is not sufficient to recognize abstractly that an information security problem exists. Spurring effective activity in the private sector requires creating interests and concerns by all stakeholders for the specific implications for their own organizations' health and viability. There are two broad categories of potential incidents or activities that non-government parties must protect against. First, there are the criminal or clearly malign activities—by hostile nations or terrorists—in which a legitimate government role in terms of responsibility is fairly clear. Second, there are those activities that result in unintended harm, *i.e.*, not clearly criminal, but requiring an appropriate legal framework so that civil remedies can be successfully employed.

Within this second category, there are three distinguishable classes of situations that require attention. First, there are situations in which involuntary exposure to careless but accidental acts of others, where problems that do arise due to negligence give rise to liability on the part of the careless. An example of this class might be the corruption of a patient's medical records due to failure to adequately maintain and back up databases. Second is the class of situations in which involuntarily shared risks are created by simple coincidence of activity (as opposed to situations voluntarily entered through contracts). For example, loss of

telephone service caused by use of a telephone exchange shared with America Online (AOL) when it is inundated by users.[36] Third, there are situations in which a mutually accepted contract nominally "governs" the potentially dangerous activity and the apportionment of liability. In many cases, it is not clear that acceptance by the consumer of the contractual terms has not been effectively coerced.[37] It is with respect to this latter group of three situations that the private sector should be galvanized to take action in its own interests.

Creating a system that would allow interested parties to share, discreetly and securely, information concerning security incidents would be useful in helping to focus resources—both R&D and operational—where needed.[38] This type of system would need to be sufficiently comprehensive to provide an accurate picture of the problem, but it would also demand mechanisms to safeguard privacy concerns and potential liability of individual commercial users. The Anonymous Incidents Reporting System (AIRS) that was created to identify air traffic control safety problems is a useful model. This system, set up at NASA (under the guise of aeronautical safety research) rather than the FAA (under which it would have been seen to be safety enforcement) allowed the incidents to be reported, catalogued and evaluated so that patterns could be determined and safety priorities established.

Finally, there is an issue of a larger responsibility to society by those who produce the goods and services on which the rest of society depends. During the Industrial Age, we developed the notion of products that carried an implied warranty: they were, at the very least, supposed to perform their stated function. We assumed that automobiles travelling at sixty miles an hour on an Interstate would not simply stop; nor would airplanes regularly fall out of the sky. By the end of the Industrial Age, commercial vendors (except for the tobacco industry) were no longer prepared to fight on the ground of *caveat emptor*, and were, therefore, prepared to take a large measure of responsibility for their products.[39] Most people in the late 20th century, moreover, even if they cannot explain exactly how an internal combustion engine works or an airplane flies, have a better intuitive grasp of the functioning of Industrial Age mechanical devices than they do of the workings of computers and advanced telecommunications systems. As a result, we as a society are now even more dependent on "guilds" that make and maintain

[36] This is what happened in many areas of California in December 1996 when AOL initiated "flat-rate" access pricing; estimates are that 20% of call attempts by other public-switched telephone network users could not get a dial tone.

[37] If there are no real alternatives to the Windows operating system for Intel-based PCs, it is clear that the consumer has no effective choice as to whether to accept the terms of the software license.

[38] A well-publicized, broader effort beyond that provided by CERT at Carnegie-Mellon University, seems necessary. It may be that activities resulting from PDD-63, such as the proposed nationwide InfraGard initiative proposed by the NIPC and the sector-oriented ISAACs, will be useful vehicles.

[39] Indeed, in today's litigious society, manufacturers are responsible for even the most improbable uses of their products. This results in safety notices such as "Warning: Do not drive with sunshade in place" (on an automobile windshield's sunshade) or "Do not pull toboggan behind car" (on a toboggan).

these new information creations, but that are loath to acknowledge or accept responsibility for their special role—other than to continue to innovate. Part of fostering an appropriate culture and creating an information community must be to have all members with major stakes take responsibility for their actions; getting the information technology sector to accept its social responsibility, for their creations without losing its capacity for innovation, is essential. Indeed, it would not be too strong to suggest that the internal behavior patterns of the IT culture must be adjusted to align them with their core role in society.

III. Navigating a New Environment

The Information Revolution is creating a new environment overflowing with opportunities and potential benefits—for governments, for commercial organizations, and for individuals. For governments, it has created an important new resource in the domestic economy,[40] as well as new sources of national power and influence abroad. For commercial entities, it is opening nearly endless possibilities for improving existing business practices and for developing new strategies to create value. For private individuals, it is altering how we communicate, how we are educated, how we earn our livelihoods, how we are entertained, and how we conduct almost all of our daily tasks. At the same time, it is creating complex new vulnerabilities in our critical infrastructures; it is also empowering a range of new actors, and opening doors for them to strike directly at our national vulnerabilities, as well as a range of other strategic targets. It is inevitably changing relationships among many traditional actors, but it is especially altering traditional power relationships, especially those related to organizational scale.

A. Characteristics of the Altered Environment

The Information Revolution is changing how we relate to the world around us. Most of our personal activities and businesses still deal with physical objects and mass (atoms not electrons), but increasingly we relate to them indirectly. We see and operate them through layers of surrogate information (such as "glass cockpit" representations and synthetic force feedback tools), rather than perceiving the environment first hand and controlling the objects directly through hard physical linkages. Furthermore, we are increasingly conducting the intermediate production steps even on physical goods by manipulating symbology or synthetic representations rather than the physical items themselves. For example, Boeing's new design and production processes for the 777 do away with paper drawings, mock-ups, and "hard-tooling" in favor of machine tools controlled directly from the integrated design and production computers. As noted by Nicholas Negroponte, there are tremendous gains in effectiveness and efficiency from manipulating electrons rather than atoms; but the obverse is that these representa-

[40] What economists call a factor endowment.

tions are evanescent and more subject to corruption than more concrete physical objects—unless due care is taken.[41]

Similarly, more of our critical infrastructure and business systems are being operated in real-time (and remotely often automatically as well), so that we are increasingly dependent on the continuously reliable functioning of our information and information-based control systems. In most cases, key functions of society are performed more efficiently than before; but our critical systems and infrastructures appear to be less stable than when they were less dependent on real-time operations and control systems. Increasingly, users are creating closely-coupled, continuously operating systems and networks with sensitive feedback loops in which there is no "down-time" to repair disruptions without disrupting important functions.[42]

There are likely to be fewer "local" problems as disruptions will probably be more widespread as they propagate due to interconnectivity.[43] These systems cannot be operated "hands-off" but must be continuously and actively controlled; they are only stable dynamically—they may not degrade gracefully if the primary control system fails.[44] These linked systems are also more complex and certainly less predictable than when they were independent due to the massive interconnectivity (and poorly understood non-linearities and cascade effects that result from closely coupling these networks). However, they may not necessarily be less robust since massive interconnections and redundancies from alternate service providers create a degree of resilience that the older configurations did not have. Additionally, the decentralized nature of the new systems adds to the resiliency compared with earlier centralized systems, even as decentralization complicates coordination and increases the chances for "emergent behaviors."

These are tensions that cannot be ignored as we as a society become more dependent on them. The bad news about these extraordinarily complex systems is that predicting their behavior and preventing substantial disruptions from affecting large numbers of interconnected users is very difficult. The good news is that this same difficulty should hamper those with malevolent intent seeking to disrupt the system from being able to know exactly where or how to accomplish their goals.

Even less appreciated than these changes are the impacts of an increasingly interconnected, globalized, open, and most frequently packetized digital commu-

---

[41] And there is much anecdotal evidence that people may be sloppier in many work habits since correcting "digital mistakes" is so easy.

[42] Previously unconnected national stockmarkets, for example, have evolved into a near-continuously operating global market in which there is little breathing space to recover from unusual events.

[43] But as the likelihood of widespread regional or national failures increases, it is also likely that these problems will be seen as a federal government responsibility.

[44] As pointed out by Charles Perrow, overlaying redundancy and back-up systems to assure system operations is no guarantee of proper functioning, and in many complex systems may only result in increased risk of unexpected failures. Charles Perrow, ***Normal Accidents: Living with High-Risk Technologies***. New York: Basic Books, 1985.

nications environment—especially the compounded implications of these factors when considered together. The very features that make digital systems attractive, including cheap and easy replication as well as relatively effortless transmission, create new possibilities for misappropriation and misuse. The old analog electronic environment was one of dedicated switched circuits in which different applications employed different frequencies and waveforms and traveled over separate, distinguishable paths; in that environment, there was relatively little chance of cross-talk corrupting data or inadvertent interference among different media. The new digital environment, on the other hand, creates near-ideal conditions for propagation of unintended events, or for easy access by those inclined towards malicious acts. In the old information environment, the focus on security was to protect against loss or theft of information. In the new world, security (and the appropriate legal structure to support it) may be as much about assuring that unwanted information is not introduced, whether by accident or malign intent.[45]

As a result of the different properties exhibited by information from most traditional physical resources, increasing dependence on it should foster very distinctive practices.[46] This new era, for example, has already spawned significantly different business models—such as giving away commercial software, trust-based sales practices like shareware, and free upgrades.[47] These must be taken into account as we seek to understand and create an appropriate culture, including a supportive legal structure. Our legal concepts for both criminal penalties and civil liabilities, in many cases, however, are still largely based on the monetary value attributed to the information that is stolen, corrupted, or otherwise damaged.[48] This is an Industrial Age construct that perceives the value of information only as it is embodied in physical products.[49] Thus, compensation for accidental destruction of a database would probably be based on the value of the time and materials that went into its creation (compensatory damages); even in the case of intentional destruction, a tort, the basic compensatory damages would be based on the cost of the information destroyed. New case law will address these needed changes over time, but slow evolution of the legal regime is likely to make it difficult to fully resolve some critical vulnerability issues in the short term.

---

[45] At a more strategic level, the ability to disseminate information widely becomes a significant political issue in less democratic societies, and between them and more open nations.

[46] See Jeffrey Cooper, ***The Emerging Infosphere***, Center for Information Strategy and Policy, McLean, VA, October 1997.

[47] It has also hatched less praiseworthy practices such as releasing products known to be flawed or incompletely tested and relying on consumers to vet the products by finding the bugs. Release of Version 8.0 of the Macintosh operating system with recognized flaws that would be corrected only partially in Version 8.0.1 and only completely in 8.1 is an example of using the paying consumer to do beta-testing.

[48] And this is often derived from the amount of effort or resources required to produce the information, rather than from the "value added" opportunity cost—that is, the value that could be generated from the "information potential" or value of exclusive possession.

[49] For example, corruption of sensitive medical data, accidentally or malevolently, could have life threatening effects. And just as with medical malpractice, damages for "pain and suffering" might go well beyond lost earnings.

In an Information Age, however, we should appreciate that there is intrinsic value in the information itself, and that should be reflected in the way we treat it.[50] For example, if a thief steals a database and publishes it across the Internet, while the thief may be forced to pay compensatory damages based on time and materials costs, this will in no way make the victim whole since the real value in the database is intrinsic—the victim has lost the exclusive ability to exploit the informational potential. Like money, or perhaps even more pointedly, priceless fine art, information deserves to be treated with respect—not just guarded from theft. In most cases, there should be a requirement for care or "due diligence" in its treatment when it is in one's possession, going beyond a passive "no harm" supervision. We are in a period in which the greatest information threat may not be what is taken, but what is left behind, unknown to the owner and user of the information-based system. Protecting the integrity of the information, as well as the security of the systems, must become an obligation, ingrained in daily practices and behaviors.

B. Different Values

The distinctive practices and values that will develop will also shape a new culture. If we step back from the immediacy of these changes and look beyond the digital techno-flash, we might find it easier to recognize that many aspects of our new behaviors reflect an earlier craft-based culture—and because of the values associated with that type of culture, this fact should have profound implications for how we understand the nature of this new era—what efficiency and effectiveness really mean. We are in the process of redefining the nature of work and altering the types of activities at each level of organization. During the Industrial Age, white-collar managers traditionally worried about cognitive decisions and administration while secretaries and typists performed the more menial, manual labor of converting those ideas into formal documentation. We made a critical distinction between cognitive and manual effort. Now, with computers and desktop publishing, white-collar managers create their own documents while former secretaries increasingly are responsible for understanding the key administrative processes. Less noticed among these changes is the increased attention to the creative "look" of the documentation by the managers. Indeed, the renewed attention to fonts and color illustration in everyday business documents is very reminiscent of the illuminated manuscripts of the Middle Ages—a period in which intellectual effort and physical document creation were intimately related.

In our haste to adopt the latest in information technologies and wring maximum efficiency from the new capabilities, we have abandoned habits and traditions, such as writing letters and memoranda, built over centuries, if not millennia. For twenty-five hundred years, elite communicated through formal (and often reasonably permanent) written instruments to pursue government, business,

[50] Indeed, it is not unusual for artifacts to acquire a "culturally constructed" or attributed value as opposed to a monitarized measure of worth. On the American frontier, the fact that horse theft was often punished by hanging reflected not the monetary value of the horse, but its worth as a cultural icon because of the sense that the owner's well-being or even life depended on his horse.

and personal objectives, leaving vast treasure troves of archivable records. Patterns of behavior included thoughtful composition, careful editing and restricted circulation. Information and its approval was traditionally used as a control mechanism in hierarchical organizational structures. For example, the clearance process on State Department cables ensured that all interested parties, including senior officials in State as well as other departments, had an opportunity to review all external communications. While collaborative software can facilitate formal procedures, email and instantaneous messaging cut across hierarchical structures and through formal procedures—these new communications techniques dissolve many of the control procedures that were central to Industrial Age forms of practice, including traditional forms of editorial judgment and oversight.[51] Business process re-engineering (BPR), in fact, uses information technology as the enabler of fundamental process and structural changes, looking to facilitate new procedures that are more efficient in the context of the new information-based capabilities; these demand both new organizational structures and a cultural re-orientation.

The value system of the Industrial Age stressed complex bureaucracies; formal hierarchies; division of labor; rigid standardized, formalized, and impersonal procedures; top-down control; mass production; maximized efficiency (measured in output per unit of input); economies of scale; and uniformity.[52] In particular, if we were to assume that the mechanistic and procedural values of the Industrial Age will be propagated into this new era, we would look towards enhancing processes and improving measures of merit based on these factors. However, if the Information Age fosters a different set of cultural values, then we will see new goals and behaviors evolve that are appropriate to this new culture. There is already significant anecdotal evidence that the Information Society places a restored emphasis on collaboration, communication, individuality, initiative, choice, heuristics, learning, craftsmanship, style, and control of one's own work product. One import is that these different practices and values will have to be taken into account in developing security practices and codes of conduct; indeed, any information culture that develops must embody and reflect the habits and values that are integral to the new culture.

Therefore, as we begin to understand the profound differences that this new age is spawning, we should also accept that it will require different measures to accurately assess utility in the new context being created by the Information Revolution.[53] Many of the measures we are currently using, however, still reflect

[51] With near-instantaneous many-to-many communications, these collaborative processes become technically more feasible; it becomes easier to check facts and correct editorial and other errors. But ensuring validation of the product that goes out depends less on technology than procedures and behaviors and here is where the difficulty lies.

[52] Max Weber and Frederick Taylor probably best expressed the values of, and created the canon for, the later stages of the Industrial Age.

[53] For example, in the later stages of the Industrial Age, as we began to understand that the value of money (and its analogues) was related not only to the size of the stock but how quickly it circulated, we developed measures to gauge the velocity of money, such as M_2, in order to assess the health of

the values and objectives of the previous Industrial Age. Not only may they fail to truly evaluate the benefits of the new practices, but they may also hide the potential downsides of new patterns of work and life that have only incompletely evolved at this point. It is important, even if extraordinarily difficult, to recognize that we are in the midst of these changes—that by our actions we are constructing a future not yet created, or even fully imagined. Therefore, without the luxury of looking back upon a transformation completed and understood, it may be hard to discern the real benefits and real costs of these changes that are now only partially in evidence. As we try to develop appropriate ground rules for this new culture, a careful, textured, evolutionary approach is probably better, for these reasons, than a constructing a detailed plan that could turn into a blunt instrument. For those few actors who do recognize the depth of the transformation now underway, however, it is an appropriate time to take actions that can place a solid foundation underneath the structures that will be created.

C. Cultural Analogies

One way to look at the collective impacts of the Information Revolution is to think of these phenomena as the creation of a new environment which will, in turn, demand a new culture. The development of a new culture is not unprecedented in American history—even in our relatively recent history; one only has to think about the dramatic changes in business practices and social etiquette caused by the widespread introduction of the telephone to perceive the creation of a new culture. Indeed, major changes in technology often spur new patterns of social organization that in turn demand a new culture, *e.g.* the development of new behaviors and norms appropriate to the altered conditions. This process goes beyond learning how to use the new tools to the more encompassing issue of the "social construction" of technology—that is, the matrix of social, economic, and political considerations that determine how technology is developed and for what purposes it is applied.

The focus on the development of culture emphasizes that the *processes* of societal adaptation to a new technology are crucial in developing ways to address the difficult choices among the values that are in tension. *Process* implies a progressively achieved outcome rather than simply a clearly perceptible end-state or result that can be accomplished all at once, and this suggests that recognizing where we are in the process may be important to understanding the best way to proceed. The three analogies outlined below can serve as useful mental models for how society adapts to new circumstances and provide useful lessons, as well as signposts of progress, for us as we face this transformation.

Settling the American Frontier

As settlers extended the American frontier into uncharted and dangerous areas (in which Army forts did not exist for protection), a three-stage progression was

the economy. In a similar fashion, we need measures to assess the velocity of information in order to more accurately gauge the well-being of the new economy.

common in the development of communities from mere collections of individual settlers. In the first stage, as early settlers established their individual homesteads, each family was responsible for its own subsistence and protection. During this stage, settlers were often isolated from each other and individual self-defense (by families) was the norm since no organized, or outside, means of assistance or protection existed. In the second stage, clusters of population were created with the arrival of more settler families; and along with denser settlements, a sense of community developed. As trust increased through the development of personal relationships, a collective responsibility for reciprocal assistance and protection was accepted by most members. The American notion of "civil society" as an alternate locus of responsibility, as well as authority and capability, sets us apart from those societies that either depend upon family and clan ties, or upon the government, for ameliorative activities. Moreover, it is worth noting that we began our national existence with a militia-based military force and depended on citizen-soldiers, not professionals, to fight our wars until only very recently.[54] This characteristic reliance on the ordinary citizen to perform important public functions is also well captured by the notion of the Western posse, a collective duty to participate actively in law enforcement.

Finally, in the later stage of these frontier settlements, the community often recognized the need for the professionalization of many key functions. It then formally delegated its inherent law enforcement powers with a grant of authority to a sheriff appointed by the community.[55] Interestingly, a frequent concomitant to the delegation of authority was abandonment of personal and collective responsibility by members of the community—as illustrated in the film ***High Noon*** until just before the end of the film. In the film, the townspeople abandoned the sheriff in the face of danger, only at the end recovering their responsibility to fight for the norms they wanted. While it is a work of fiction, the resonance of ***High Noon*** as an American cultural icon owes much to audiences' recognition of the intrinsic truth of this situation in our national experience. Functions delegated often became the sole duty of the hired professional; and individual citizens then avoided participating in these activities, even when they had previously performed them as a community responsibility. It is worth noting, however, that, perhaps for this very reason, we have been very careful about what functions we do delegate to government, and to what level.[56]

This analogy suggests that there is a broad spectrum of structures that could be adopted as models for protection of an "information community."[57] These range from:

---

[54] And even now, this ingrained element of our national character is reflected in the political power of the National Guard, the modern incarnation of the Minutemen.

[55] A variant was the appointment of a U.S. Marshal who held authority from the territorial leadership.

[56] One element that distinguishes the American political system from most others is that powers not explicitly delegated remain with the people.

[57] The concept of an "information community" will be discussed in Section IV.

1) leaving protective measures in individual hands as a matter of retaining personal responsibility (individual self-defense); to
2) accepting the responsibility for protecting the community's interests and retaining the authority in the community's hands (collective self-defense); to
3) shifting the authority for community protection to the government (formally delegated authority).

The real issue is probably not to choose among them as exclusive options, but how to dynamically balance among them; and this choice depends fundamentally upon several crucial factors: first, where one wishes to retain responsibility as opposed to authority; second, how much authority the community is prepared to place in someone else's hands; and third, where the capabilities to ameliorate problems are lodged. As will be discussed in a subsequent section, the abstract choices are complicated significantly by legacy choices and the realities of where capability exists.

After the Chicago Fire (1871)

Another interesting analogy is the reciprocal dependency that exists in cities and towns because of the danger of fire. Regardless of what any individual building owners do to protect themselves against the scourge of fire, they all remain vulnerable to accidents caused by the sloppy practices of other building owners and occupants. Prior to strict fire codes, even exemplary individual behavior could not avert vulnerabilities imposed by others. Indeed, every city dweller was dependent on the good practices of all other members if fire was not to devastate the entire community. This threat initially imposed normative responsibilities for care that were later formalized, deepened, and codified by fire codes in order to protect all members against acts unintentionally triggered by one of them.

The devastation caused by the Chicago fire brought home the vulnerability of urban areas to disasters caused by accidents or carelessness. As a result, both fire codes and mandatory fire insurance coverage became common throughout the United States.[58] Fire codes establish a minimum set of standards and practices that are enforceable by criminal law, not just civil tort actions. Fire insurance provides a mechanism to transfer liability for harm from the individual to the collective in return for a usually explicit commitment to adopt, as a minimum, fire code standards and other safety measures. Cost savings often accrue to insured parties who are prepared to take measures beyond the minimum standards; indeed, many property and casualty insurers have built specialty practices in advising on risk reduction measures. Subsequently, when electricity became common and electrical devices spread throughout homes and workplaces, electrical codes were also adopted to govern the application of this new technology (and especially to prevent fires). Perhaps most relevant as a potential model, certification that

[58] Japan and many European countries, as a result of their greater physical vulnerability to the effects of urban fires, have substantially tougher criminal penalties for failure to observe fire protection standards. Moreover, the almost uniformly harsh legal treatment of arson recognizes the issue of involuntarily "shared peril."

electrical products met safety standards was lodged by common agreement in Underwriters Laboratories (UL®), a private organization created by the insurance companies but accepted by local building code authorities.

These structures are useful models for addressing our information vulnerability problem since they create private, but government-sanctioned, collective self-help mechanisms to deal with the problems, rather than take a mandated, government-controlled approach. In fact, the National Information Assurance Program (NIAP), recently established jointly by the National Security Agency (NSA) and the National Institute for Standards and Technology (NIST), will follow the UL® model by certifying private laboratories to conduct testing and certification of information protection hardware and practices.

The Automobile Society

When the horseless carriage was first introduced in the United States around the turn of the century, today's complex of road networks, traffic signals, automobile service facilities, and laws governing operation of the new transportation medium did not exist—nor were they imposed quickly. Rather than preemptive statutes, custom and habit, such as direction of travel and possession of right-of-way, developed. These were then codified into traffic laws, following the "rules of the road" that had already been accepted by the community.

Even the "rules of the road," however, appeared as matters of common practice only as situations arose that demanded predictability or specified behavior. It is worth noting that these rules usually developed first in cities where propinquity made the actions of others matters of potentially serious consequence. Creation of traffic laws only followed the recognition that consistent rules were needed and that common practices had already developed. Battles over speed limits, motorcyclist helmets, and driving ages still reflect differences in local sensibilities and acknowledge that some common agreements on key traffic issues do not yet exist.

More recent pressures for more uniform national behaviors in the matters of seat belt usage and drunk driving illustrate some of the same issues with which information protection must grapple, and they may provide useful food for thought. Until federal pressure for mandatory seat belt use occurred (with local enforcement encouraged by threatening loss of federal highway funds), use of seat belts in the U.S. varied dramatically from region to region due to the belief that this was a matter of individual choice and local tolerance. In much the same fashion, attitudes towards drunk driving have historically been largely a matter of local opinion.[59] As the exogenous costs—"externalities" to economists—of these behaviors became more widely appreciated, however, these attitudes began to change; these activities impose costs on the community at large, not just the careless individual.[60]

---

[59] The threat of loss of federal matching funds for highway construction has also been used as a point of leverage in pressuring stricter local enforcement of both drunk driving and seat-belt usage.

[60] First, not wearing seat belts substantially increases the likelihood of a driver losing control in an accident and causing damage or injury to other vehicles or bystanders. Furthermore, in an era of

This is, in fact, the very same situation in which we find ourselves living in a co-dependent information society. Increasingly, these types of activities—ones dangerous to others—run afoul of tightening community intolerance for "reckless disregard" of norms and laws designed to protect the common welfare of the entire community. Society should be no less intolerant of similar types of information abuses that could endanger others. Within the information domain, tensions between local identity and personal choice, on the one hand, and attempts at federal pre-emption or imposition of uniform national standards, on the other hand, have already created significant tensions. Increasing globalization, with its attendant standardization and homogenization of behaviors as well as products, may deepen tensions even further. Concern over "American cultural hegemony" may already be as widespread as concern over our present unchallenged military advantage.

D. Creating a New Culture

The Information Revolution is creating a new environment that demands appropriate new behaviors—no less for the commercial sector, other organizations, and individuals, than for governments; but it is clear that few parties that have yet recognized this need. The new environment demands a degree of care in our everyday actions and interactions with still-new technologies, exactly because we have not yet assimilated or fully internalized them or their potential consequences (or because they are not yet discovered). First, if, as this paper posits, we are entering an information-dependent environment, where the imaginable benefits of that technology are substantial, but in which society is critically dependent on the proper functioning of its information systems, then we require a culture appropriate to living with a valuable, but potentially dangerous technology. Culture implies patterns and expectations of behavior as well as an appropriately supportive set of legal and formal structures.

Second, because we have not internalized new behaviors, we still need to think consciously about how to act appropriately instead of relying on our instinctual or automatic reactions. We are, in a sense, not unlike an American who finds himself transplanted to London and must consciously think about which way to look while crossing the street. Even though we are familiar with the relevant technologies, we cannot just trust our instincts in dealing with them. Under these circumstances, explicit signposts for proper behavior (like "Look Right" and "Look Left" signs on many London streets in tourist areas) are extraordinarily useful. Moreover, since we have not yet developed an intuitive sense of the consequences and implications of actions in the new environment, explicit reminders of these non-intuitive factors—especially on how their consequences may impinge

skyrocketing medical costs and third party or government coverage, the increased costs of expensive trauma injuries to the unbelted are transferred to the rest of the community. Similarly, when drunk drivers more often than not ran off rural roads and killed only themselves, most communities were prepared to tolerate this kind of reckless behavior. When innocent pedestrians or occupants of other vehicles began to suffer significant injuries as a result of drunk drivers, many communities became rapidly less accepting of these collateral costs being imposed on the community as a result of individuals' reckless behaviors.

on others—may be very useful in fostering appropriate behavior. Even though we are seventy years into the era of commercial aviation, aircraft crews still use checklists to assure that no important action is inadvertently forgotten. Similar principles could be applied to the operation of information systems.[61]

Since potentially severe consequences could flow from interactions with information and information-based systems, we need patterns of and norms for behaviors appropriate to this new circumstance of extreme sensitivity to information. Yet we certainly do not wish to smother creativity and impede everyday use of these important tools by widespread government intervention and stringent over-regulation. At the same time, we probably cannot afford a totally laissez-faire approach with these important problems. We recognized that many adverse consequences could flow from our society's use and dependence on the automobile only very late. By that time, many patterns of behavior and adaptation were already established that have proved difficult to change. On the other hand, we recognized very early that potential dangers could similarly arise from widespread use of civil nuclear power and took absolute regulatory control through federal pre-emption.

Despite the superficial relevance of the nuclear example, however, the reality that information is so widespread and used in such diverse ways throughout our economy and society creates a very different perspective.[62] Given the pervasiveness of information and information systems, we should think very carefully about whether to make protecting them fundamentally a government responsibility, or to grant government broad authority, as we did with atomic power—even given the potentially serious adverse societal consequences of misuse of information and information systems. In particular, it would appear impossible, on both constitutional and political grounds, to give government, at any level, such broad regulatory powers over information itself. On the other hand, there do appear to be important roles for government in facilitating the development of an information-sensitive culture. Effective self-regulation by the private sector, however, requires self-discipline and sufficient comity among competing interests to allow compromise and building upon common ground; and these qualities are not in evidence today. Resolving these issues will require careful balancing among competing

[61] For example, simple measures such as automated reminders, "Save Now" or "Back-Up before Shut-Down," are easy to understand in this context. More complex interactive procedures for security and reliability are not difficult to imagine; and the increasing computational power arriving in all new hardware and software could be applied to these important objectives rather than to increasing the marginally "useful" features often found in new "bloatware." If these measures are to be effective in the private sector, they must be relatively transparent to the user and consistent with work practices and behaviors.

[62] There are many (especially in the executive and legislative branches) who have argued that information deserves treatment similar to that initially accorded atomic energy—a strong and preemptive federal role in its fostering and protection. The model breaks down, however, but not because information systems are unimportant to national security, nor because they are not potentially dangerous when carelessly used, nor because they could not be employed malevolently. Rather, the apparent similarity ignores how deeply information systems, unlike atomic energy, have penetrated the entire fabric of society.

equities; and until there is greater awareness by all parties of the stakes, many of these problems are not yet ripe for judgment.

While this paper cautions against adoption of the American civil atomic power model, there are, however, several lessons of the nuclear culture that are extremely relevant. In particular in the information domain, we also require an appropriate culture that demands assigning full responsibility for the consequences of potentially disruptive, if not catastrophic, activities. This obligation implies two key cultural properties: *attribution* and *accountability*.[63]

Attribution denotes the ability to identify or know who did what action; it does not connote a standard of proof nearly as stringent as "beyond a reasonable doubt" that would be needed for successful legal prosecution.[64] This suggests that both technical and procedural measures that allow messages and actions to be ascribed to the party that initiates them, even if the content of information remains private, would be useful. Developing this type of capability is probably a worthwhile area in which government could spur research interest.

Accountability, on the other hand, denotes the assignment of responsibility, and it creates a duty to be subject to reporting, explaining, and justifying. This suggests that societal norms and an appropriate legal structure are needed in order to apportion and assign culpability, both civil and criminal, for information activities that pose adverse impacts on other parties—and that the full impacts and costs of these activities need to be identified. In both areas, governments can provide critical enabling support as part of a serious public-private partnership to address the key problems.

In an environment in which anonymity of action, while important for protecting privacy, raises substantial security concerns and may facilitate malevolent activities, the ability to remove the veil of anonymity—by attribution of those actions that have produced the adverse consequences—is extremely important. Technical or procedural controls that require positive identification before accessing sensitive information or performing critical operations are clearly feasible; and these can be used to maintain audit trails for records access.[65] This would facilitate assigning civil liability or criminal culpability where carelessness, error, or malevolence caused disruption or corruption; it would, moreover, serve an important deterrent purpose, helping to reduce the incidence of such incidents.

---

[63] Another facet of atomic energy experience is also relevant as a powerful negative example— the limitation under the Price-Anderson Act of liability from atomic power plant accidents that was designed to foster investment by reducing the risk from a not fully understood technology. With reduced liability incentive to assure a focus on safety by the builders, owners, and operators of the atomic power plants, primary reliance was placed on detailed government-developed standards and procedures, coupled with oversight through special-purpose regulatory agencies

[64] ***Webster's Encyclopedic Dictionary*** defines attribute (v.) as, "…to consider as made by, esp. with strong evidence but in the absence of conclusive proof…"

[65] Several key hardware and software vendors are likely to include such features as intrinsic elements of their future products. However, as the case of the secure embedded ID number of Intel's Pentium III chip recently demonstrated, these are likely to be very sensitive and extraordinarily contentious measures.

For example, hospital personnel might be required to use something similar to an encrypted identity and authenticator card[66] before entering or accessing personal patient data. Higher levels of certified authorization (carried by the same Fortezza card) might be required to alter medication orders. For prescribing or administering narcotics or doing high-risk procedures, even higher levels of "trust" or practices such as two-person rules (long used in the nuclear community) might be adopted.

These types of mechanisms, since they enable attribution of action, provide *ex post* audit trails, in addition to restricting who can conduct these activities. Attribution without strict accountability, however, will not address the need to create a responsible society. Individuals and organizations must understand that they will be held accountable for their actions—and that sanctions will be serious. Enforcement of liability for actions is essential if effective protection, rather than rhetoric, is the goal.

E. "Why Don't We Lock Our Information Doors?"

While the new information landscape is difficult to comprehend, we could help ourselves to better understand some of its critical environmental features, as well as our own present cultural attitudes towards advanced information technologies, if we posed the rhetorical question, "Why don't we lock our information doors and windows?" Answers to this question can illuminate features of the new environment that we have as yet neither fully understood nor internalized in our everyday behaviors. And these individual behaviors are important exactly because of the very high degree of reciprocal dependency in these new circumstances.

Many of us probably grew up in communities where we did not need to lock our doors in order to protect our valuables when we left our houses; we certainly didn't need to lock our doors to protect ourselves when at home. In most cases, there were no perceived threats; the behavioral norms—outside major urban areas—were so strong that vandalism or burglary were not considered to be a major problem, much less violence in our own homes. Few people today, especially urban dwellers, would leave their homes unlocked when unoccupied; and most would certainly lock their doors when at home. These changes highlight a range of unfortunate alterations to our civic circumstances that affect how we live our daily lives and conduct our everyday business. In light of the steps we take today to ensure our personal safety and protect our physical property, however, it will be enlightening to examine how we treat our information systems.

Using Caller ID and firewalls as information-age surrogates for locks on doors and windows, let us then look at the answers to the above. More specifically, why are most of us willing to allow the "entry" of a telephone call (that links us to the outside) without knowing the identity of the caller and what they want, when we would not open our front doors to an unknown person ringing our doorbell? Pondering this question suggests four basic reasons why we exercise significantly

[66] Fortezza, developed by the National Security Agency (NSA), is one such type of security card.

less care in our daily information activities than we do in other aspects of our daily life.[67] First, most people currently will not assume that the call could pose a direct threat to their immediate information environment.[68] Second, many will not recognize that they possess information objects of value susceptible to attack. Third, most fail to recognize that external communications and links to a globalized information network represent a potential danger to the wider information infrastructure in which they are embedded. Fourth, very few will immediately accept the need to exercise care in their daily information activities as a matter of societal responsibility; but most would be careful if they thought they were carrying and could transmit a contagious disease. The telephone does not represent a dire threat today. But we must appreciate that everyday behaviors will have to adapt as serious threats eventuate from our interconnected information systems.

With respect to the first point, while most Americans would acknowledge the potential danger to their personal safety from burglary and mugging, few would recognize that cyber-cognates of these street crimes might directly affect them. Yet malicious vandals, thieves, and con-men (as well as graffiti artists) all currently exist in cyberspace; and cyber-terrorists and state-sponsored information warfare should not be unexpected in the near future. While hacking, on-line credit card fraud, and international bank embezzlement are widely recognized as problems (along with artistic Web-page reconstruction), most individuals believe that these types of malign activities pose more of a threat to companies and governments than to individuals. Furthermore, while most companies are aware that on-line financial transactions and credit card verification could be sources of concern, there are few indications that they recognize the broader dangers to their operations or very survival, that could stem from reliance on networked information systems. Yet, companies that rely on these systems, or on digital intellectual property for competitive advantage, represent as tempting a target for sophisticated criminals, intent on extortion or theft, as more obvious financial assets.[69]

Regarding the second issue, few people appreciate how much of value (including sensitive personal and proprietary information) is now accessible in many homes (and businesses) as a result of commonly-used information systems. It is not unusual for individuals to keep their most sensitive personal records on their home computers (including lists of passwords and PIN numbers) and use their computers to access their bank, stock, and mutual fund accounts. Businesses also increasingly maintain their records electronically and many are almost totally reliant on real-time, on-line transaction processing systems for their basic business functions. In addition, many professions and industries have adapted their operations and production processes to computer-controlled paperless systems (such

[67] These concerns should increase significantly as new technologies such as digital subscriber lines (xDSLs) and especially cable modems become commonplace: these systems are "always on" and could allow routine third-party access to any connected equipment.

[68] This paper will draw a distinction between micro and macro information environments. Micro environments are those directly under user-auspices; the macro-environment includes those elements beyond the user's direct control but to which users are inextricably linked.

[69] The Willie Sutton principle on robbing banks—"because that's where the money is"—is apropos.

as used by Boeing to make its most advanced commercial aircraft). The more devices incorporate interconnected digital technologies, the more these could become attractive targets for criminal (or terrorist) attack.

Third, most of our ingrained attitudes towards potential dangers from modern information systems were shaped when our principal information systems were the telephone, radio, and television. The perception was that the worst that could happen was loss of service or an annoying, but manageable, intrusion (such as a sales call at dinnertime or a truly bad TV show).[70] And to large degree, the telephone is still seen by the public as an instrument simply for voice communication—even though the "telephone system" itself has been transformed into a complex data network in which voice is increasingly becoming an adjunct to more sophisticated applications.[71] However, as a data network connecting any addressable device, including home computers with modems and any locally-connected peripherals, communications links both promise new opportunities and threaten as yet unrecognized dangers. In the not-so-distant future, many home systems and appliances will be linked and remotely operable through computer and telecommunications networks. Furthermore, the traditional computer science separation between data and instructions is rapidly disappearing as object-oriented programming and often self-activating macros or "active applets" (such as used by the increasingly widespread Java language), become common practice. As a result, messages may no longer be simple communications but have the capacity to operate important computer-based functions or corrupt sensitive personal or business information (as with the insidious MS Word "macro viruses.")

Fourth, and finally, few individuals appreciate the degree of society's information reciprocal dependency, the consequences of vulnerable information infrastructures, the opportunity for access to the networked infrastructure that their own systems offer, or their responsibility for helping to minimize vulnerabilities by assuring that their systems are not misused (even indirectly). Just as we noted how a community responsibility was recognized by city-dwellers due to the dangers from urban conflagrations, we might also consider the example of urban high-rise apartment dwellers. There is a strong socialization process that enforces locking the front door after entry and not opening the outside door to strangers, especially via "buzzing them in." There the responsibility is clear; perhaps it should be equally clear in the information domain.

IV. A Pride of Ameliorative Measures

As a result of the foregoing analysis, the private sector must address three broad categories of threats to the proper functioning of essential information systems

[70] This, however, ignored the very real information that could be obtained when the phone was answered. A burglar or stalker could determine whether the home was occupied, the gender, and possibly the age of the person answering.

[71] The telephone system began as a circuit-switched, analog voice network; and while voice still remains as its core, it has switched almost entirely to a digital system. Moreover, it is now overlaid and interconnected with a fully digital, packet-switched IP router network that is more suitable for data.

and services and be prepared to deal with the inevitably diverse impacts. First, as in many other domains, situations of involuntary exposure to the negligent acts of others should be rectified by assignment of proper liability or by the creation of a "no-fault insurance" program if society as a whole is unprepared to force users themselves to pay for information externalities created by their activities. Second, in those situations in which involuntarily shared risks are created by normal, as opposed to negligent, behavior, the model of fire codes along with property and casualty fire insurance practices may also be an appropriate guide for information protection by the private sector.[72] Third, with respect to information-related activities, the computer hardware and software industry continues to rely on "imposed" contractual acceptance of risk by the customer to shield the companies from potential liability for their products' faulty operation. Since it is becoming difficult to avoid using information-based products, it is becoming difficult to avoid being affected by products that fail to perform properly.[73] Perhaps it is time to overturn, as a matter of public policy, the acceptance of this practice—especially as both hardware and software are increasingly and invisibly incorporated into every manner of product. We may not wish to force, by regulatory or legal measures, software and hardware vendors to assume liability and, thereby, run the risk of slowing innovation; but users of those systems should have strong incentives to demand improved security and operational functionality or to take mitigating measures against serious themselves, both for their own sake as well as for the welfare of the entire interconnected community. Fundamentally, what is required is the development of a self-recognized information community (or perhaps more properly, information communities) that builds upon common values and interests and strengthen the feeling of and mechanisms for collective self-help.

A. Creating a Framework for Private Action

While the federal government clearly has paramount responsibility for safeguarding national security, and governments at all levels share the responsibility for prosecuting criminal activity, there are three reasons they cannot perform these functions in the information domain without substantial assistance from private individuals and organizations. First, appropriate activities by private actors are crucially important because private actors, in reality, hold most of the technical and physical capabilities for preventing potentially adverse information incidents or ameliorating their consequences. Second, as governments increasingly become buyers of commercial information and telecommunications services, this reliance on private capabilities by the government will continue to grow even with

[72] There are some incipient signs of insurance company interest in this type of scheme with recent announcements offering Y2K liability covers; such privatization of risk, which could lead subsequently to securitization of this area, would be an attractive alternative to government regulation. Pressures from the SEC or the Financial Accounting Standards Board (FASB) to explicitly account for potential information-related financial liabilities would do much to spur corporate interest in risk-avoidance and risk-sharing mechanisms.

[73] This may be an especially complex issue in addressing software that is available on the Internet, such as freeware and shareware. These products, if contaminated with lethal viruses or other serious faults, could act as "attractive nuisances."

respect to protecting government's own critical information systems. Third, exactly because information is sensitive and information systems so pervasive, private parties are not likely to extend the government writ so as to give government additional, and necessarily intrusive, authorities for information protection sufficient to allow the government to perform these functions successfully. Indeed, current suspicions that the government is seeking controls on encryption, not only for export, but also to allow intrusive domestic investigations and access to sensitive information, are not far below the surface of much industry opposition to these proposals.

To the extent that private entities attend to their own vulnerabilities (acting solely in their own interests), they will go a long way towards ameliorating the nation's information security problem. Private actors, however, will require additional government help in order to make their private activities more effective in protecting both their own and society's equities in information. While governments are not the most important actors in creating a viable information culture, they have the power to either hinder or enable essential private activities. Figure 6 below, highlights a range of actions that the federal government could take to facilitate the development of a safe and secure information-dependent culture by the other important actors, including state and local governments. Among these steps should be incentives and assistance for state and local governments to acquire expertise, facilitate local initiatives, and remove impediments to useful private activities.

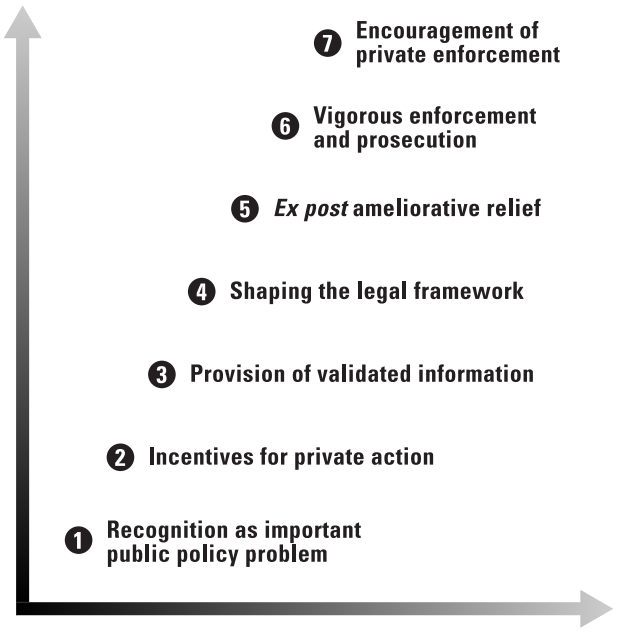

Figure 6. Facilitating Actions for Governments

First, given the potential consequences of breakdowns in the information infrastructure, the government should make information security an element of

public policy concern, and encourage private entities to undertake socially beneficial actions in this domain. There are a range of mechanisms that could be used to exercise this encouragement. For example, just as it has recently done with the Year 2000 problem, the SEC could require companies to report, in their 10(k) filings, potential liabilities from disruption to or corruption of their information systems. This action would place information vulnerabilities directly on the agenda of every corporate board and highlight potential shareholder exposure.

Second, if we believe that there are not sufficient incentives for private entities to take appropriate actions on their own, then federal and state governments could create incentives (modeled on existing tools used for other socially desired activities) for businesses, other organizations, and individuals to acquire and use effective information security systems. These incentives could include expedited tax write-offs of expenditures for specified equipment, tax credits for information protection investments, or even direct subsidies by government by providing such equipment and training at reduced costs. Not only incentives and exhortation ("the bully pulpit"), but education about the range of information vulnerability problems, and providing technical support to the public and industry would be very useful measures in fostering appropriate private action.

Third, the federal government could assist in numerous ways in providing information that enables private entities to make appropriate choices of effective information protection systems. Government could, on the one hand, as it has done with electric utilities and selected R&D consortia, provide exemption from its anti-trust restrictions in order to allow exchange of sensitive information among competitor organizations. The Information Warfare Panel of the 1997 Defense Science Board (DSB) Summer Study on Transnational Threats specifically recommended creating an "IW 411" for the government so that affected parties would have a recognized and validated source of information that they could call upon for information protection.[74] This notion would extend that concept to allow the private sector to access those trusted sources. Another mechanism that extends beyond providing validated information would be to foster the creation of third-party validation and certification of information protection systems and procedures, modeled after, for example, Underwriters Laboratories. Coupled with strong oversight from property and casualty companies that issue liability and business continuity insurance, this could be an extraordinarily effective mechanism to induce appropriate information protection behavior.

Fourth, aside from passing and enforcing new laws, the government has numerous opportunities, through selected interventions in appellate court cases, among other vehicles, to shape the legal framework by which private parties adjudicate their civil disputes. For example, the government could seek standing to intervene through *amicus curiae* briefs to shape how courts interpret and apportion liability arising from information incidents. Similarly, the government might

[74] There are already several private activities (such as the Internet Engineering Task Force [IETF], the Internet Operators [IOPS], the Cross Industry Working Team [XIWT], and the Internet Society [ISOC]) that could serve as nuclei for this type of initiative.

seek to address the public policy issues arising from information technology companies' refusal, through contractual licenses, to accept responsibility or liability for failures of their products.

Fifth, government could provide ameliorative relief for a wide range of potential information disruptions, including, for example, significant expansion of the Computer Emergency Response Team (CERT) operated by Carnegie-Mellon University and support with military Reserve and National Guard units for physical restoration of critical information facilities. Again, the DSB Summer Study also recommended establishing an "IW 911" facility that would enable government users under information attack to have a simple and widely available emergency response option; this idea deserves investigation for broader application.

Sixth, and perhaps most importantly, government assistance is needed in setting clear boundaries so that the most disruptive illicit activities are made clearly illegal and therefore subject to strict criminal prosecution—even if enforced by the vigilance of private parties. It appears to be absolutely essential for government to enforce the norms it has established or else it simply engenders disrespect for all controls on inappropriate behaviors. This course suggests that government might be wise when dealing with malign information activities to adopt the "broken windows" approach to law enforcement, popularized by former New York City Police Commissioner William Bratton in his successful campaign to reduce street crime.[75] The "broken windows" model argues that tolerating low-level, petty offenses, rather than reserving law enforcement focus and capabilities for more serious crime, actually encourages more serious criminal behavior and breeds widespread disregard for enforceable standards of behavior. It also significantly degrades the quality of life for the average citizen. In addition, many of the petty offenders were found to be involved in more serious crimes as well; therefore, taking them off the street for these offenses served to reduce their opportunities to commit other crimes and thus reduced the incidence of more serious offenses.[76]

While not all hackers and crackers engage in more damaging illicit activities, it is not unlikely that many also commit more serious information crimes. Strong measures against these low-level activities can help to define the bounds of acceptable behavior in this new culture and not encourage hackers to press the limits of on-line respectability.[77] Moreover, there is evidence that "zero tolerance" enforcement acts as a useful deterrent beyond simply not encouraging malign activities.[78] From a national security perspective, there is a real advantage in substantially reducing the number of information incidents so that more serious activities and

---

[75] See William W. Bratton with Peter Knobler, ***Turnaround: How America's Top Cop Reversed the Crime Epidemic***, New York: Random House, 1997.

[76] Less remarked but also important, arresting perpetrators for petty crime established "probable cause" for a physical search that often turned up evidence of additional crimes.

[77] Some of the issues associated with computers and network security, including the potential that hackers and crackers represent are discussed in Charles C. Mann, "The Mole in the Machine," ***The New York Times Magazine***, July 25, 1999, pps. 32–35.

[78] "Hacker Magazine Says Avoid Military Systems," ***Defense News***, March 9–15, 1998, p. 2.

patterns of behavior can be more easily identified by an information indications and warning (I&W) system.

Finally, the government could encourage even more direct information protection activities by private parties—clear government approval to allow, if not foster and assist, private enforcement and then support with vigorous criminal prosecution would be useful. In many respects, private parties in the United States have a freer hand with fewer legal restraints—especially Constitutional constraints on search and seizure, and requirements for probable cause—than does the government, and this may be particularly true in the information protection area. Therefore, in many circumstances in which government's exercise of its authorities are constrained, private parties may be more effective; and there are likely to be many activities in which private action will be more timely or effective regardless. Moreover, in the United States there is a long, even if not totally savory, tradition of self-help and private enforcement—from the Pinkertons to modern-day bounty hunters and private security guard forces in many communities. More recently, investigation and enforcement against illegal importation or counterfeiting of trademarked goods, audio and video tape piracy, and illicit software copying have all been spearheaded by the concerned private parties. This type of collective self-help regime may be a useful model for private enforcement activities in the information systems protection domain. To the extent that information malefactors tend to be repeat offenders, "taking them off the street" serves a broad social purpose. Furthermore, vigorous enforcement, especially if it is proactive, may serve to discourage many potential offenders who might otherwise be tempted if the costs looked low.

Even in other domains, for preventing or interdicting many *per se* criminal violations, today it is incumbent upon the interested private parties to take action since government cannot be everywhere. Moreover, especially with the pervasiveness of information technologies, we would not likely be willing to have government everywhere that we needed protection. This is not unlike the situation of storekeepers with respect to shoplifters: in most jurisdictions, it is private actors, not the police, that take initial action to forestall or apprehend shoplifters. As noted above, this type of "self-help" model exists already with private enforcement of many laws infringing on intellectual property. For such private action to be effective, however, it needs to be supported with vigorous prosecution by the government. These activities provide one potential element for an appropriate information culture built upon a series of collective information protection "self-help" arrangements that might include the elements discussed below.

B. A Pack of Collective Actions

The global infosphere implies a seamlessly interconnected network with nearly unlimited access points—well beyond the capability of any government or group of governments to successfully secure on their own—with the largest proportion of the potential entry points into this network residing in private hands. These entry points include not only telephones and computer terminals but also routers, hubs, switches, and other elements of worldwide telecommunications

systems. However, controlling access in order to protect private interests is likely to be a more tractable approach to solving the larger problem of securing national and global information infrastructures than attempting to have governments control access.

To help create an appropriate information-dependent culture, private actors have a wide range of instruments available both to increase public awareness of information assurance needs and to enhance the quality of information protection. No individual measure will "solve" the range of problems that must be addressed; therefore, a multi-pronged thrust is needed. Both preventive and remedial measures are valuable; but as yet, on technical grounds, there are no clear reasons for choosing an appropriate balance between these elements. It is not apparent, moreover, that these measures need to be neatly integrated; nor is it clearly advantageous that these measures be part of a carefully thought-out architecture. Indeed, most successful cultural adaptations to technological revolutions have been piecemeal and evolutionary. In concert, however, these measures could address some of the more troubling aspects of our present information vulnerability. The measures suggested below would help to create mechanisms to control unrestricted access to the information networks and enforce concern for information integrity by creating a structure in which access to networks or to information itself is consistent with trust levels of users and their protected environments.

Create a Climate of Concern

It is essential that all elements of society be energized to recognize the potential vulnerabilities from information dependence and act to ameliorate problems before serious dangers eventuate. Education about the potential dangers from information vulnerability and the range of potential threats is important. Yet private entities by themselves may find it difficult to assist in creating broad public awareness of the potential consequences to society of disruptions to information systems; they are likely to need to make use of the government's ability to speak with authority and credibility. Some of government's most effective tools are the power to highlight and the ability to exhort, like Teddy Roosevelt's "bully pulpit." Helping the less aware members of society recognize the problems that exist and their self-interest in addressing those problems is a crucial first step.

This thrust for increasing awareness should include the creation of joint industry-government bodies or government-sanctioned private bodies, similar to the Financial Accounting Standards Board (FASB) or Underwriters Laboratory, that could begin to define and enforce standards of practice—that is, standards for appropriate behavior and methods of measuring progress—in reducing information vulnerabilities. One potentially useful model is the series of industry-education seminars and roundtables held around the country in the 1980s to combat a raft of bank robberies. With the cooperation of banks and industry associations, cooperating law enforcement agencies—the FBI, Treasury Department, Department of Justice, and local U.S. Attorneys—laid out the magnitude of the growing problem and highlighted steps that individual banks could take to reduce their own vulnerabilities by procedural as well as technical changes. Thus far, American

information system users appear, as is often the case, to have initiated such useful cooperative programs with a focus on only the hardware side of the information security problem (such as the National Information Assurance program noted earlier). We lag significantly in addressing what may be the more critical problems on the human behavior side—to develop and disseminate practices and procedures for appropriate information-dependent behavior and processes. These activities could be coupled with actions by government agencies such as the Treasury, Defense Department, the Federal Reserve Board, and the SEC to mandate certain levels of information security or at least due diligence, in the private businesses that must deal with them.

Because of the increasing centrality of information to corporate value, there should be a strong shareholders' interest in seeing that companies assess their vulnerability to information activities, including negligent practices, as well as their value extracted from information-related activities. Internal audits (supported by third-party validation) should include a clear focus on due diligence and use of "best practices" in information assurance. While the initial impetus for these measures would be self-protection, the long-term maintenance of "trust relationships" with other organizations that are also dependent on information systems would be linked to appropriate practices and effective self-enforcement. Adoption of these mechanisms can be prodded by selected government actions such as SEC regulations.[79] Pressures to adopt good information protection practices should emanate not only from stockholders and insurance companies to forestall potential liability, but also due to even stronger pressures that could come from other businesses, if companies became reluctant to deal with entities that were careless in their information practices. This could easily occur as more companies create strategic partnerships or business relationships that require close linkages between computer and telecommunications systems (not unlike the inventory and production systems originally pioneered by Wal-Mart and its suppliers).

Adopt Stringent Internal Codes of Conduct

Codes of conduct for information use and information systems behavior must be put into practice at individual companies and organizations (including control of access to network capable systems), and they must be effectively enforced. Recognition of their own interests in practices and standards—information security equivalent of fire codes—to mitigate against accidents or malevolence initiated by others will facilitate their spread to other reciprocally dependent parties.

However, good housekeeping must begin at home with major system users. First, government should set an example, through well-publicized adoption of appropriate information protection practices that will serve to indicate its awareness and concern for the problem. Second, major system users in both industry and academia must establish practices and procedures that not only safeguard their own systems, but that also do not allow their systems to be used for harmful

[79] See subsection "Create a Trust Certification System" for a discussion of how such relationships could be formalized.

or illicit activities directed at other information systems. New hardware and software technologies that are likely to be included in the next generations of commercially available systems should help substantially in this regard. In order to facilitate the creation of a technically sound but flexible approach, definition and use of "best practices" as a basis for due diligence requirements is needed. These measures should include standards and protocol requirements for access, such as the evolving electronic data interchange/electronic commerce interchange (EDI/ECI) standards.[80]

Adopt "Zero-Tolerance" for Careless or Disruptive Activities

As noted previously, the "broken windows" or "zero-tolerance" approach to enforcement has proven effective in reducing the incidence of low-level disruptive behaviors. It also has helped in significantly reducing the frequency of more serious crimes. Likewise, there are good reasons to believe that similar practices in information protection would yield parallel results. First, strict enforcement sends a clear signal that misbehavior will not be tolerated. Second, it disrupts the patterns and teaching of "asocialization" that can serve as a training ground for more serious disruptive activities. Third, it simply takes many of the malefactors "off the streets;" and since studies consistently show that repeat offenders commit a large fraction of all crimes, it significantly reduces their opportunity to commit subsequent acts. The Air Force, with a "get tough" policy on hackers, has apparently persuaded many in the hacker community to look elsewhere for attractive targets.[81]

There are fundamentally four actions that need to be taken against these types of illegal or hostile activities: deter, prevent, prosecute, and remediate. Deterrence involves establishing clear demarcation lines that define prohibited activities and providing credible threats that sanctions will be applied against violators. Prevention includes measures taken both to identify potential offenders and to deny or thwart the prohibited activities. Prosecution includes both responsive actions taken while the activity is in progress and actions taken subsequently to catch the offender. Remediation includes actions taken to restore the affected systems or activities with minimum disruption to society; it serves two important purposes. Remediation builds confidence among users and deters perpetrators. In support, the government must undertake those actions that are directed primarily against perpetrators or occur outside of private information enclaves; and as with shoplifting, it is likely to be a private responsibility to take initial action inside of these enclaves, and perhaps outside as well. What will be required for effective implementation of any of these steps, given the complex landscape, is cooperative actions among all parties.

Having themselves adopted effective internal information protection measures, individuals and organizations should, out of self-interest, create pressures for

[80] As of this writing (August 1999), one of the more interesting developments in this domain is the release of FinXML 1.0, a standard data interchange language for capital markets in July 1999. See <http://www.finxml.org/>.

[81] op. cit., ***Defense News***, March 9–15, 1998, p. 2.

others to cease potentially dangerous behaviors; and these must include both public and private sanctions. Societal pressure is often needed to make government willing to enforce and prosecute "low-level" crimes, whether loitering or shoplifting; and treatment of "information offenses"—unless they involve large sums of money or potential compromise to national security systems—has been no different. Not only changed attitudes, but also increased technical awareness and understanding, are desperately needed on the part of law enforcement and prosecutorial agencies. For non-government violators, outside pressure for stringent treatment of breaches of "codes of conduct" may be necessary. These could include being subject to widespread community sanction—the information equivalent of shunning—or potential for loss of "trust certification." Moreover, oversight by outside parties, whether auditors, liability insurers, or certification agents, needs to become accepted practice in the information protection domain. This also needs to be coupled with the development of a powerful constituency for demanding strict liability for information malpractice or negligence, including treatment of sensitive information in their care. These measures, however, cannot be implemented at the federal level alone; therefore, model laws and changes to the Uniform Commercial Code (UCC) that could serve as the basis for complementary changes in state statutes should be developed as these concepts evolve.

Create a Trust Certification System

At the same time, we should begin to establish a system of private third-party (but government-accepted) "trust certification" ratings for information system users.[82] Developing an array of "trust-creating" or assuring mechanisms such as "certificates of information trust," issued by trusted private entities (such as a third-party trust broker), that would allow access both to privately restricted, higher-security domains and to the upper levels of a stratified quality of service information network would have two advantages. First, these measures would significantly restrict access by unknown, careless, or untrustworthy users—thereby reducing the numbers of information incidents and the noise with which an indications and warning system would have to deal. Second, they would create strong incentives, in terms of both cost and quality of information services, to create and exercise effective information protection programs.

Conceptually, this structure would build upon a combination of financial auditing, commercial credit reporting (such as Dun & Bradstreet), third-party bond rating, fire insurance company rating, and on-line check-cashing approval systems that have been developed over the past hundred years as cultural elements essential to living in a complex Industrial-Age economy. These systems essentially build certification structures under trusted third-parties that replace the first-hand knowledge of the other party that was common before industrialization

[82] Given the very strong negative reactions in the private sector to mandatory key escrow, and more recently to a government-run, nation-wide health identifier system, it appears the route of wisdom to allow this system to evolve in the private sector, as did an entire range of other "trust creating" mechanisms, discussed briefly below. Note that TRUSTe is an independent, non-profit privacy initiative with private sector sponsorship that offers an industry self-regulated approach to establishing privacy principles and to compliance with them. See <http://www.truste.org/>.

and urbanization. While they do not carry the force of law, ratings by the private bond rating agencies such as Moody's and Standard & Poor's (S&P) exert tremendous leverage over the behavior of commercial and municipal borrowers. Similarly, the threat of failure to obtain a "clean letter" from auditors can be a powerful inducement to good financial practices and reporting; and for information protection purposes, it could make other users loath to deal with organizations that demonstrate less concern and care. As part of a broad set of private sector mechanisms (that would also include hardware and software certification, information integrity standards and protocols, risk mitigation, insurance, incident response and recovery capabilities), these steps would begin to create the structures essential to an information-dependent society. Furthermore, as private initiatives, they would be less likely to become frozen and more likely to evolve in a manner appropriate to changing circumstances.

Vigorous Enforcement Through "Private Right of Action"

Beyond effective enforcement and prosecution by governments at all levels of statutory information-related violations, it would be useful if private entities could be enlisted to take strong action against information malefactors. Government investigative and enforcement activities, already complex due to the nature of many malevolent information incidents, can be even more difficult due to stringent legal procedures; private entities acting in their own direct self-defense may have more latitude for effective action. Models for this type of "self-help" or self-interested approach are common in American law; they include private security forces, bounty hunters, and the False Claims Recovery Act. However, not only must governments be willing to allow (and hopefully facilitate) these measures, but also private entities must see direct benefits in being vigilant and aggressive in their approach. Indeed, similar to approved R&D consortia (such as SEMATECH or MCCT), the government could grant limited anti-trust immunity and perhaps even financial incentives (such as tax credits or accelerated write-offs) for such collective self-defense activities that would add to the intrinsic benefits of being more secure. And these activities would nicely complement a "zero-tolerance" approach by government, thereby helping to reduce the overall load of malign incidents and assisting an effective I&W system for information attacks that affect the national security.

C. Potential Elements of an Information Community

Let us return to the notion of an "information community" with a distinct culture as an effective route to addressing the potential vulnerabilities of an information-dependent society. It is likely that this "information community" will be defined not by contiguity or proximity, but by common perceptions and coincident interests, even if not shared values. It may well be virtual, but it will be bound with a structure of trust relationships. The core of this community's belief system must be two-fold: not only respect for the intrinsic value of information, but also awareness of the potential vulnerability from reliance on it. Therefore, such a community would accept the responsibility to treat information like money and to accept a fiduciary duty to safeguard it.

A range of governmental mechanisms (both legal and regulatory) as well as structures within civil society could facilitate attribution and help create accountability—the key elements of a responsible information community built around trust. Attribution creates implicit accountability for acts through identification of the culpable party; accountability implies that sanctions will be applied (and also that the intrinsic responsibility will be accepted) if the acts are socially undesirable. Both elements may assist in deterring inimical activities; but attribution, through high confidence identification (enabled by encrypted digital signatures), also plays a crucial *ex ante* role in implementing more secure information systems in the new information systems model described subsequently. These characteristics can become the standard by which proposed information protection mechanisms can be judged.

It is important, however, for there to be sufficient clarity in identifying those activities that represent such a clear breach of society's norms so that they are recognized by all potential perpetrators as criminal, rather than merely careless or negligent. Hopefully, some, if not most, may be deterred by threat of criminal prosecution. While there are malign information activities that clearly need to be treated with the full weight of prosecutorial ardor, it is important, to the extent possible, that most activities resulting in harm be *penalized* but not *criminalized*—so as not to trivialize those activities subject to serious criminal sanctions.[83] An intense focus on preventing negligence, especially those that rise to the level of "reckless disregard" or "actual malice," is also essential; but these should largely be dealt with through a sanctioned private right of action.[84]

We can now assess the three models for protecting an "information community" noted earlier—individual self-defense, collective self-defense, and formally delegated authority—for their ability to foster these critical elements. The problem with the first model, leaving information protection in the hands of each individual, is that the entire community remains vulnerable to mistakes, misdeeds, or abdication of responsibility by others, without a concomitant mechanism to enforce "good behavior." The essential problem with the third option, formally delegated authority, is the apparent unwillingness of the American people (and the courts) to grant more authority over information to the government, especially since capabilities for prevention or remediation of information incidents are likely to be extraordinarily intrusive. The second model, collective self-defense, requires the creation of a community of self-recognized common interest. Thus, the first necessary step is the creation of a true "information community" whose members share a common concern for the magnitude and character of the information problem and accept a shared responsibility for its prevention and remediation. One advantage that collective responsibility may offer, in particular, is a means to

[83] Thus, strengthening the civil law domain in order to allow penalties to be levied by governments as well as private relief to be obtained is as important as creating a strengthened criminal law regime.

[84] And perhaps rather than establishing direct financial loss as the standard, recovery of damages takes into consideration the potential gains or opportunity costs of the mistreated information.

address protection of the network itself—those elements that might be thought of as an "information commons" outside of most users' direct control.

Underlying the construction of a workable "information community" are two critical properties. The first important property underlying this "information community" is the concept of differentiable "class"; but, unlike social class that derives from accident of birth, this class arises from the notion of trust. "Trust," in this context, revolves around the faith in the degree of care exercised by the user both in the operation of information systems and the treatment of information. Moreover, we should foster the use of "trusted transactions" which would allow us to deal securely with non-trusted parties.[85] As a matter of public policy (derived from the potential vulnerability of society to breakdowns in the information infrastructure), we should encourage the use of "best practices," with accountability and assignment of liability to effect compliance. As discussed in the previous section, one method of implementing the concept of class is to create third-party mechanisms to certify the trust level of a user; however, there are serious issues of universality and even "due process" if the system operates in private hands.

The second important property of this "information community" rests on the concept of stratified access and quality of service, both granted as a function of user "trust class"—the degree of trust accorded to a user. Within the government sector, we already have the models of NIPRNET (non-secure) and SIPRNET (secure), as well as earlier user-controlled high security networks such as the EAM dissemination system, that discriminated on the basis of security clearance and access needs. Within the emerging global infosphere, vulnerability of information systems can be significantly decreased by adopting a series of security measures designed to restrict access in both the private and government domains.

Creating a "Trust-Based Quality of Service" Concept

The current U.S. telecommunications system evolved from the telephone system as a regulated monopoly (after the 1934 Federal Communications Act) with not only "universal service," but also "common carrier" obligations. Even deregulation (under the 1984 and 1996 Telecommunications Acts) did not alter many long-standing concepts, such as non-discriminatory treatment, even though most advanced information systems are not common carriers.[86] These conceptual hangovers from old Industrial Age conditions now limit our ability to construct a new information systems model that is more appropriate to an age of information dependency, and reciprocal dependency on other users' information habits and practices.[87] While universal service and unrestricted access to information net-

[85] The model for a "trusted transaction" is a certified check or absolute bank draft; regardless of the credit-risk represented by the other party, the particular transaction is guaranteed by an instrument from a trusted third-party.

[86] Indeed, the efforts by the Administration and the FCC to hide the taxes on telephone users imposed to fund Internet access for schools, libraries, and hospitals are instructive.

[87] Some of the social constructs that have emerged from the Age of AIDS may be useful analogues; arguments about patients' rights versus those of society may well be echoed in this domain.

works may be in fundamental tension with a society that is totally dependent on a functioning information infrastructure, they do represent important political (and social) equities that cannot simply be ignored. How to successfully integrate these perspectives into a differentiated but equitable quality of service (QoS) system poses difficult but essential issue.

Core elements of a new model for information services (that go beyond that derived from historic telecommunications concepts) are based on the fundamental notion of voluntarily established associations (with common information values) and include the key features of: 1) "gated communities" or virtual information enclaves; 2) differentiated QoS, stratified not only by price but also by level of certified trust; and 3) a mechanism for trust certification. The first element creates an information equivalent of the gated residential community to which admittance must be specifically authorized by a resident. Just as these communities are built upon the notion of private property and the inherent right to restrict access, the information community concept recognizes that most information systems are private property and, therefore, subject to intrinsic rights of owners to set the terms of access. Moreover, private information systems do not include just the computers and information processing, but also most or many of the existing and planned telecommunications networks. These networks are not common carriers and, therefore, have the ability to establish stringent terms and conditions of service. In essence, therefore, allowing public use of these private properties is the equivalent of granting an easement: the property owner has the right to set and enforce the terms and conditions for the use of his property, as long as it is within the acceptable bounds of public policy. Furthermore, there is no inherent reason why security-conscious information systems users could not demand (as a condition of purchasing services) that their communications providers meet certain levels of security as one important measure of quality of service—one aspect of which could be restricting access to mutually acceptable users who agree to abide by information protection standards.

Enclaves built around these concepts would enclose: 1) users employing an agreed level of security through information protection standards; 2) the users' local computational and information resources protected as virtual dynamic enclaves; and 3) the communications systems linking the members of the community. In particular, unlike current practice, the telecommunications network would perform important security functions through access controls and differentiated bandwidth and routing priorities. These enclaves would be surrounded by firewalls and other security features limiting unrestricted access from the outside; inside the enclaves, communication among community members would be freer, consistent with agreed limitations depending on trust level. Users would be recognized by their high-security, encrypted digital signatures designating their trust level and providing access and priority rights to the holder. Holders of lower trust-level certificates (or none at all) would be subject to a variety of security-oriented restrictions, such as slower routings through multiple firewalls, increased scrutiny, mandatory decryption of messages, buffering, and other protective (and possibly time-consuming and costly) measures. Moreover, since these systems are

privately-owned and operated, they are beyond the reach of most constitutional constraints (with respect to probable cause and search) that might prevent government law enforcement agencies from back-tracking offenders; these restrictions would not prevent private actors from pursuing information offenders , in their own self-defense throughout their own network and even beyond.

Key to the functioning of the information enclave concept, however, is the third feature, the certificate of trust. This feature of the information enclave concept is built upon a series of structures that validate and certify levels of trust, reflecting the degree to which information protection practices and standards are met. Just like a borrower with a clean credit report, or a municipality with a Triple A rating from S&P, whose access to funds is better and costs of borrowing ae lower, organizations or individuals holding high-trust certificates would be granted preferred access and priority. This could mean that digitally signed and authenticated messages from AAA certificate holders would receive preferential access to high-speed backbones through segregated routers, without going through mandatory lower bandwidth firewalls. In order to reduce vulnerability to unauthorized use and denial of service attacks, routers and switches within the protected networks would have encrypted addresses, the capability to recognize digital signatures (in order to shut off unauthorized access), and the capability to dynamically and securely re-address critical nodes within the system.

It is important to distinguish between creating a government-mandated regime that discriminates and allowing a private regime that discriminates, but is created by private parties voluntarily agreeing to the conditions of service.[88] In a system established privately, the parties are creating a parallel information infrastructure, in essence, accessible and usable only by those agreeing to abide by the rules of the community. Moreover, unlike the telephone companies under common carrier provisions, alternate telephony service providers, Internet service providers, and operators of private data networks are not considered to be common carriers and are, therefore, already freer to offer differentiated levels and types of service that discriminate among classes of users. The new information system model, therefore, uses this flexibility as a crucial element of its foundation.

It is worth noting that such a system could raise significant concerns about "information apartheid," creation of information ghettos, and discrimination against those unwilling or unable to meet the standards for the higher levels of trust certification (an "information underclass")—especially as there may be claims that the discrimination is not on the basis of trust but socio-economic class.[89] Basic information services should be no differently than any other social welfare

[88] Even though one could conceive of a government-created regime that discriminates against certain users (for good public policy reasons such as limiting convicted felons access to guns), it is inevitably bound to surface the issue of competing political equities. For example, what would be the "due process" protections in creating the standards of membership.

[89] These issues have been discussed in ***Falling Through the Net: Defining the Digital Divide*** (released: July 8, 1999); this report by the National Telecommunications and Information Administration of the U.S. Department of Commerce updates two prior studies, one completed in 1995 and the second in 1998.

issue that involves unequal access to goods and services; and care should be taken against creating new and insurmountable barriers to participation in a society increasingly connected by information services. For this reason, it is important that this new set of systems be seen as an overlay, not a replacement, for the existing national information infrastructure, in which universal service and access are guaranteed. However, at the same time, it would also be unwise not to take measures that are vital to reducing the vulnerability of our national information infrastructure because they could aggravate existing inequities of wealth and status.[90]

V. The International Aspects

An "information commonwealth" would be, in fact, a natural extension to the international system of the information community concept. Common concerns and values quite naturally lead to the notion of an "information commonwealth" in which risks are voluntarily shared in return for a commitment by members to a set of consistent rules of behavior designed to minimize potential information vulnerabilities. One could think of this information commonwealth as consisting of a "borderless" inner core—an information "free trade area" in which there are few barriers to the free flow of information because all parties operate within a commonly protected operating environment under a consistent set of rules and behaviors. Surrounding the inner core would be a set of controlled entry barriers monitoring and restricting information flowing from external information sources. There might also exist a second level of only partially restricted information flows—from "associated entities"—allowed freer, but not unrestricted, access to the information commonwealth in return for operating within a controlled environment.

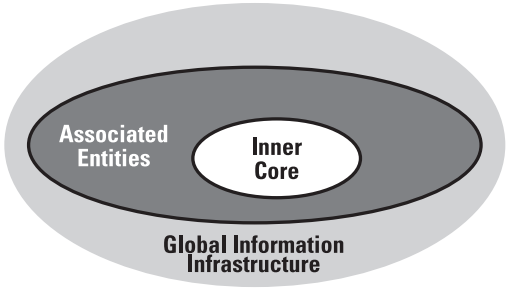

Figure 7. An Information Commonwealth

This second level would obviously not be as secure as the inner core; but it would be far less vulnerable than the completely uncontrolled external information environment. Finally, a series of high-security information barriers that are

[90] This issue arises frequently, often in conjunction with mandatory health and safety measures. It was raised, for example, when the legislation mandating automobile airbags was debated due to the substantial costs of these systems. Claims were made that this would unfairly discriminate against low-income families ability to afford automobiles—also an essential service in our society.

penetrable, but help to control external access as well as content of the information flows, would reduce potentially dangerous threats to the members' information systems. This concept is not unlike the Schengen Agreement (among many European Union members) that allows virtually free travel among member countries without border controls. However, unlike most free trade areas, an information commonwealth would represent levels of security, instead of geographic contiguity.

VI. Final Thoughts

The Information Revolution portends major transformations in all societal functions; and many of these will have substantial impacts on national security, especially as information and information systems become increasingly important elements in all these areas. This paper has not attempted to take a constructivist approach[91] in addressing the challenges posed to national security interests from this transformation; instead, it proposes cultural adaptation through evolution of social norms and behaviors as the preferred solution. Creating a new culture that effectively meets the needs of living in the Information Age, though difficult and time consuming, will be essential if we are to avoid major calamities stemming from our increasing dependence on information and information systems. While it should be obvious that such a culture must evolve and emerge rather than be imposed, it should also be apparent that influencing the direction of its development could help to ease the pains of these transformations.

Guiding the course of development, however, necessitates some understanding of what qualities we would like the new culture to possess and in whose hands we believe solutions to the challenges will best be found. A number of historical situations that exhibited features and problems similar to our present circumstances have been highlighted and briefly discussed in order to demonstrate that a variety of potential models exist for addressing the transformation; choice among these models can help lead the direction in which our adaptations evolve. How we choose ultimately to rebalance and realign the core powers—responsibility, authority, and capability—among the principal actors should be the subject of serious open discussion and debate.

[91] A constructivist approach would define in law *a fortiori* the boundaries of tolerance and desired patterns of behavior.