PUBLICATION

Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era

Peter H. Daly

June 2000

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

Peter H. Daly has been a consultant with Booz•Allen & Hamilton since October 1998. Previously, he was a senior executive and agency head at the U.S. Treasury and served on the President's Commission on Critical Infrastructure Protection.

ISBN 1-879716-62-3 **P-00-3**

June 2000

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
Bell Atlantic
BellSouth Corp.
The Boeing Company
Booz-Allen & Hamilton, Inc.
Carvajal S.A. (Colombia)
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
CyberMedia Convergence Consulting
CyraCom International
DACOM (Korea)
ETRI (Korea)
eYak, Inc.
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
GTE Corp.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
High Acre Systems, Inc
Hitachi Research Institute (Japan)
IBM Corp.
Intel Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Eli Lilly and Co.
Lucent Technologies
John and Mary R. Markle Foundation
McCann North America
MediaOne Group
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp. (Japan)
NMC/Northwestern University
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Siemans Corp.
SK Telecom Co. Ltd. (Korea)
Strategy Assistance Services
TRW, Inc.
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - Defense Intelligence Agency
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

James Adams
A. Denis Clift
Victor A. DeMarines
John C. Gannon
James J. Hearn
Robert T. Marsh
Bruce W. Moulton
Lionel H. Olmer
James M. Simon, Jr.

These reviewers and the Program's Affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

The purpose of this report is to discuss how the historical partnership between government and business is changing and to provoke thinking about what alternative forms of that partnership may be needed to manage the new national security risks of the post-cold war cyber era. The author's aim is to identify, describe, and analyze the issues, but, in keeping with the approach of the Program, neither to offer resolutions nor to try to predict what will happen.

Executive Summary

During the cold war years, as the political world froze into an east-west balance of power, the commercial world evolved into a complex, flexible network of business relationships that came to provide the basis of the global economy of the 1990s. From the end of World War II until the demise of the Soviet Union in 1991, the development of much of the United States's high technology, including the Internet, was driven by defense of U.S. security interests. Parallel developments in communications and transportation, however, transcended cold war tensions, by creating the basic infrastructure needed for an open global economy to mature, and bolstered U.S. security strategy, by encouraging development of freer markets as barriers to the spread of communism. This nexus of national security, which in those years was considered the exclusive province of government, and commerce, as carried out by banks and corporations, placed government and business in a sometimes volatile but always vital partnership born of overriding mutual interest and interdependence.

The end of the cold war substantially altered the dynamics of that partnership. Today, the world is preoccupied with economic development more than nuclear annihilation, and overall U.S. security may rely more on trade agreements than on control of territory or ideological compatibility. Economic development is the province of private enterprise more than government, and business, rather than government, tends to possess not only the money and technologies needed to make a global economy work but also most of the influence to write the new rules of competition. Consequently, the role and influence of government have dwindled. Yet government is not irrelevant: business needs it to establish the broad international frameworks of transparency and evenness in which business risk can be measured and managed and commerce can flourish. So, although the relative roles of government and business have shifted since the end of the cold war, the vital synergy between these two complex centers of power remains essential to U.S. national security.

In coping with this shift, the U.S. government national security apparatus may be caught in a kind of technological gap, with state structures created for the static cold war endeavoring to manage risks deriving from technologies created for a dynamic global economy. The new risk profile is shaped largely by dependence on advancing information technology that links nations, markets, and individuals in high-velocity communications networks. Today, this technology is created largely for commercial purposes and is much less driven by government-defined national security requirements than was true during the cold war. Moreover, its reliability depends on a complex and largely borderless supporting infrastructure capable of managing the huge and growing volume of transactions and communications necessary to carry out global business operations. Because the transcendent nature of this infrastructure tends to make traditional methods of national control obsolete, risks to its reliability present new challenges to both business and national security planners.

This report considers the major forces for change—economic globalization, advancing information technology, and the diminution of government—as they influence the respective national security roles of business and government that evolved during the cold war. It identifies key national security institutional stakeholders and addresses their traditional mission questions in light of changing conditions. For government, the military asks “who is the enemy?” Law enforcement asks, “who is the criminal?” For business, the financier asks, “what is the risk?” and the merchant, “where is the market?” These questions remain valid, but the national security challenges of the new technology-driven, economically more open, and ideologically more flexible world beg not only new answers but also new questions. Shifting boundaries between government and private enterprise and the displacement of state supremacy with commercial need are a reality that gives rise to the following complex questions: Who will gauge the risk? who will form the security strategy? who will choose among response alternatives if an attack occurs? who will assure readiness? and who will pay for it? Although wide agreement exists on the fundamental nature of the problem, agreement on appropriate solutions and the nature of new structures to deliver them remains elusive.

Contents

Chapter One

Introduction

During the troubled 1930s, in the hardscrabble Texas hill country of the Pedernales, a popular folk song told of a solitary traveler, a young man, looking to put down roots, find love, and build a good life on the land. When asked why he hoped for so much when times were so unsettled and the future so uncertain, he replied that he had no choice: "If'n I was to stop lookin' it would only hurt me worse."[1]

That line speaks volumes about the buoyant effect of enduring hope and offers a remarkably clear insight into the ways in which nations, institutions, and individuals often address uncertainty. Just as for that young man, the hope of reward and the possibility of regret influence much of what is done to cope with the risks of an unknowable future.

Since the mid-1970s, the new millennium has been almost everyone's favorite milestone and metaphor for change. But it was not much of a milestone at all, because real milestones mark fundamental alterations of societal structure, individual expectation, and cultural direction, and nothing of this kind occurred with the change of date on January 1, 2000. Yet such a milestone, has occurred in recent times: Christmas of 1991. On that day Mikhail Gorbachev resigned as president of the Union of Soviet Socialist Republics, and the USSR ceased to exist, bringing to an official close a half-century of cold war characterized by nuclear standoff and intense global ideological struggle, which reached into fundamental elements of life in the United States and around the world.

It is difficult to overstate the significance of that event. In the United States in the years following World War II, government structures, social values, and much of the economy were shaped largely by engagement in the cold war against communism. The immense risk presented by arsenals of nuclear weapons and the fear they ignited, both within this country and among its allies, of communist expansion led to a near obsession with national security within the U.S. government and in the U.S. public.

While the political world of those years was frozen into an east-west balance of power, the commercial world was evolving into a flexible and complex network of relationships that were to provide the basis for the global economy of the 1990s. During the cold war, the development of much U.S. high technology, including the Internet, was driven by the defense of U.S. security interests. Commercial developments taking place at the same time in communications and

---

[1] "Buddy, Won't You Roll on Down the Line," by Uncle Dave Macon. Recorded in Texas, 1930. Allen Brothers, Vocalion 02818, Victor 40024; original issue, Brunswick 292.

transportation, however, transcended political division, by creating an infrastructure in which an open global economy could mature, and bolstered U.S. national security strategy, by encouraging the development of free markets as barriers against communism. The connection between national security, acknowledged during the cold war as the province of government, and commerce, which was carried on by banks and corporations, was in keeping with the traditional U.S. approach to global policy—the pursuit of open markets as a path to American prosperity and security—and placed government and business in a sometimes volatile but always vital partnership born of mutual interest and interdependence.

The end of the cold war altered the dynamics of that partnership. Although the United States, in becoming the sole super power, still faced serious threats of direct attack, though now from a variety of sources, in the post-cold war world preoccupied with economic development the role and influence of government appear to be dwindling. At the turn of the millennium, overall U.S. national security seems to rely more on the opening of global markets than on control of territory or on ideological compatibility. In this altered environment, business tends to possess not only the money and most of the technology that make a global market function but also the influence to establish the rules of global competition. Yet government is not irrelevant to a global marketplace; business needs government to establish broad international frameworks of transparency and regulatory evenness in which risk can be managed and commerce can flourish. Similarly, although global commerce is now the focus of much attention, home-country political and economic influences may exert a greater effect on business development. Though the years immediately following the cold war have seen a shift in the roles government and business in national security, the synergy between these complex centers of power remains vibrant.

The importance of commerce to U.S. national security is not new. What is new is the dawning of the “cyber,” one dominant characteristic of which is the interdependence of activities and players once assumed to be separate. The post-cold war global economy, in which financial markets are coupled twenty-four hours a day and enormous amounts of capital can be moved with the speed of electrons, has, in the words of Federal Reserve Chairman Alan Greenspan, created “a very dramatic change in the whole risk profile of the world.”[2] This environment, which depends largely on information technology and a reliable supporting infrastructure capable of managing a huge volume of transactions and communications, challenges business and national security planners alike in new ways.

The United States is at once the most advanced developer and the most dependent user of this infrastructure, and it has much at stake, both economically and for national security, in identifying and managing the new kinds of risks. Assuring access to this infrastructure and making it worthy of confidence have emerged as principal elements of the partnership of business

---

[2]Quoted by Lawrence H. Summers, then Deputy Secretary of the Treasury, in a speech presented to the Chemical Manufacturers Association, Philadelphia, Penna., Nov. 9, 1998.

and government in the post-cold war environment and together raise a fundamental question: In the cyber era, to what extent will government and business each be responsible for infrastructure security?

In many important ways, the U.S. national security apparatus may find itself in a technological gap, in which state structures created for the static cold war are endeavoring to cope with risks derived from technologies created for a dynamic global economy. The situation is somewhat reminiscent of World War I, when the French cavalry, wearing breastplates of the kind used by Napoleon's army and deployed in formations designed for that time, charged mechanized weaponry such as machine guns, suffering tremendous losses with little gain. Then as now, military and government leaders confronted a world moving toward dramatic technological and political change and driven by forces they could neither predict nor fully comprehend.

In the post-cold war world, the creation of most high technology is driven not by traditional national security requirements but by commerce. For example, around 1980, about 70 percent of U.S. technological development was funded in one way or another by the federal government; today that figure is about 1 percent.[3] The displacement of ideology by commerce as the primary global organizing principle and the heavy reliance of government on private enterprise to create and deploy critical technologies present new conditions for U.S. national security planners:

- Economic, rather than military, crises now pose the most significant direct threats to U.S. security. The tighter and tighter coupling of world financial markets through global information infrastructures, increasing U.S. reliance on open global markets for prosperity, and the critical role of the U.S. in anchoring the global economy as a whole have made economic contagion both a reality and a risk, while military crises, in the absence of opposing bloc alliances, tend to be confinable.
- Although governments retain an important role, the development and protection of commercial technology is primarily a business problem, amenable to business solutions more than to public policies. This change suggests a new tolerance for security as well as privacy and a new style of command and control systems that are not exclusively under the jurisdiction of either the military or national security apparatus.

Is business ready for this new responsibility? Do traditional business risk models appropriately value enterprise dependence on the global information infrastructure, and, more important, do such models direct investment against the possibility and consequences of the failure of that infrastructure, whether deliberately caused or inadvertent?

This report examines the major economic and political changes and trends in the wake of the cold war and how they affect the relationship of business and government. It explores a range of traditional methods for coping with uncertainty and looks at their adequacy for dealing with a

---

[3]James Adams, former CEO of United Press International (UPI) and, in 2000, CEO of Defense, Inc., citing a source in the National Security Agency, personal communication to the author, Feb. 18, 2000.

new national security environment, one in which discontinuity is the norm and the calculus of national security is closer to the economic concepts of risk, reward, and regret than to computations of military balances of power. The report includes a discussion of the range of stakeholders, conflicts, and confluent forces involved in establishing a new style of national security partnership for government and business in the post-cold war cyber era.[4] Given that neither government nor business is a monolith, given that the mixture of public and private assets to be protected is highly complicated, and given also the difficulty of orchestrating actions in the private sector where a huge number of players interact in the marketplace, certain questions arise: Who will gauge the risks? Who will decide the strategy for national infrastructure security? Who will choose from among alternative responses when a crisis occurs? Who will assure readiness? And, finally, who will pay for it all?

[4]For an extensive discussion of approaches to defending the U.S. information infrastructure from attack, see Stephen Lukasik, *Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure* (Stanford, Calif.: Stanford University, Center for International Security and Arms Control, Institute for International Studies, March 1997).

Chapter Two

An Era of Discontinuity

One question: if this is the information age
how come nobody knows anything?[1]

For every president since Washington a primary responsibility has been the protection of the nation from attack. During the cold war, this responsibility was translated into a massive build-up of nuclear and conventional arms and the creation of a powerful national security apparatus, which extended beyond the military into law enforcement, intelligence, and scientific research. All other national activities, including business activities, were more or less subordinated to this supreme national objective, an objective defined through the political process and pursued almost exclusively by the federal government.

In almost half a century of cold war, the United States's overall national security strategy was relatively simple: mutually assured destruction. The rivalry between the two superpowers, the United States and the Soviet Union, dominated the rest of the world, and U.S. national security policy aimed at both containing Soviet expansion and achieving superiority in defense. The promise of retaliatory annihilation was the principal deterrent to nuclear first use by either power, as the Cuban missile crisis of 1962 showed. Many credit this policy, and the cost of the arms race it spawned, as a major reason for the ultimate demise of the Soviet Union.

The American obsession with communism and the concomitant specter of nuclear war came during a period of enormous national social and economic transition, and its effects ranged well beyond national defense strategy. Never before had the United States faced a threat of such magnitude, not even during the isolationist and xenophobic years preceding each of the world wars. In the decades following World War II, despite an expanding economy and a wave of idealism, Americans responded the cold war with pervasive anxiety about the future and a fear of foreign attack. Anyone who lived through that time can recall air-raid warnings and drills, two cold-war-inspired military involvements—in Korea and Vietnam—and the tremendous, budget-consuming growth of the government-business partnership that President Eisenhower dubbed "the military-industrial complex."[2] They can also attest to the impact of that experience and the values the time instilled, much of it still ingrained in the American perspective.

---

[1]Cartoon of cocktail party by Robert Mankoff, *The New Yorker* (April 20, 1998), 64

[2]President Eisenhower used this phrase in his "Farewell Address to the Nation," January 1961: "This conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence—economic, political, even spiritual—is felt in every city, every State house, every office of the Federal government. We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications. Our toil, resources and livelihood are all involved; so is the very structure of our society.

In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or

At the turn of the century, such traditional views of U.S. national security are being fundamentally challenged. In place of a clearly observable and comprehensible rivalry between two superpowers, a vague and complex mixture of forces has altered the conditions of global security, offering new uncertainties neither easily understood nor amenable to instruction by experience.

2.1 Economic Globalization

Who would have thought just ten years ago that the Moscow stock market—a term still strange to those who remember the cold war—could so drastically affect U.S. companies and share values as it did in late 1998? The consensus among experts then was that what had begun as a financial crisis in Asia was becoming a global economic problem as serious as any the international community had faced since the end of World War II. Rapid, large-scale capital withdrawal from emerging markets in Asia, Russia, and elsewhere posed an immediate threat to U.S. exports and the job growth that went with them. Equally ominous was the impact on U.S. financial markets, as the strategies of financial institutions turned to seeking quality and avoiding risk. Even the most respected U.S. companies found it increasingly difficult to raise capital on equity and debt markets, and some as a result revised their earnings projections downward and reduced their payrolls.[3]

Although a global marketplace offers new commercial opportunities, it also creates new forms of economic interdependence not addressed by regulatory regimes designed for an earlier era. In 1998, the awareness that the new global economy had made many of the old rules of international finance obsolete led such prominent financial figures as Federal Reserve Chairman Alan Greenspan, U.S. Treasury Secretary Robert E. Rubin, and, indeed, many global currency traders to uncertainty over what might happen next and to fear the worst. When the crisis eased early in 1999, the United States and other nations began to consider what new kinds of rules were needed.

In the cold war's bipolar world, military clashes threatened to cascade because of the complex system of alliances involved; now, at the opening of the twenty-first century, economic crises that start elsewhere are most liable to spread and affect U.S. interests. A currency crisis that begins in a country as remote from the U.S. as Thailand resonates almost immediately in the financial markets of New York and London as traders, corporations, and financial institutions quickly adjust strategies to exploit or escape from its effects. A 24-hour-a-day-world with tighter and tighter coupling of financial markets through information infrastructure makes economic contagion a reality and a new risk.

---

unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist." Dwight D. Eisenhower, in *Public Papers of the Presidents of the United States, Dwight D. Eisenhower*, vol. 1 (Washington, D.C.: U.S. Govt. Printing Office, 1958–61), 1035-1040.

[3]Lawrence Summers, Nov. 9, 1998.

Economic globalization has even broader implications than reform of financial systems for the formulation of U.S. national security strategy. During the essentially ideological struggle of the cold war, each side wanted the other to be, at a minimum, weak. In today's interdependent, competitive commercial relationships, each party needs the others to be engaged and relatively strong economically so that the free market can function. The stakes in success, it may be argued, are basically shared, and the incentive is to encourage market growth, rather than to isolate and destroy another participant. Strong national or regional economies, even among nations that have been allies but are now competitors or that have long been ideological and strategic adversaries, effectively support U.S. interests in the post-cold war world. U.S. trade and economic policies are critical not only to strengthen other economies as markets for U.S. exports but also as a means to promote a climate of social stability within which trade can flourish. The thread of this argument could be discerned in U.S. explanations of U.S. involvement with NATO in Yugoslavia late in 1998 and early in 1999.

2.2 Advancing Information Technology

A global marketplace can function only with a diverse and confidence-worthy information infrastructure capable of accommodating a huge volume of transactions and communications. Composed of the interlinked technologies of telecommunications, cable, satellites, computer equipment, software, and complex operating protocols, the global information infrastructure constitutes the central nervous system of the global economy. Its existence defines the difference between international economic development prior to the end of the cold war at the dawning cyber era.

In the cyber era, omnipresent, high-velocity information technology enables almost any business to "go global" and reach markets hitherto inaccessible. It allows quick movement of capital by currency traders who begin the moment they enter a market to worry about how to escape should an unfavorable risk climate develop. The only way national economies can grow—especially emerging economies—and markets can flourish is to mine the global investment pool that these traders manage. In this sense, the role traders play is that of market disciplinarian, setting the ground rules for national economic policymaking. As was seen in Russia and Asia in 1998, these traders are not very forgiving of national policies that endanger their returns. The information infrastructure is their tool to administer discipline.[4]

At the individual level, few things better define the spirit of the 1990s than the personal computer (PC). Just ten years ago it existed on the fringes of the economy and popular culture. Although visible and frequently discussed, it had not permeated the everyday lives of most U.S. citizens. Now PCs are almost everywhere, creating many fortunes and becoming a tool for the masses. In 1989, world sales were about 21 million, with 9 million in the U.S.; by 1998, world

[4]Thomas L. Friedman, "Manifesto for a Fast World," *The New York Times Magazine*, Sunday, March 28, 1999, 40.

sales had risen to 93 million, with 36 million in the U.S. In 1990, 15 percent of U.S. households had personal computers—by 1999, the figure was 50 percent. Some forecasts envision a rise in sales of PCs to 41 million in the United States by the end of 1999.[5]

Doubtless, the Internet has been the driving force behind the spread of information technology. Its potential to enable hundreds of millions of people to harness the power of the technologies of the global information network can be fulfilled, however, only if the Internet becomes truly global. With an estimated half of the world's population yet to make even a telephone call, the room for growth is enormous.

Yet in some important nations of the world the free flow of information and the reduction of state control over the means of dissemination are not favored. Just as the Berlin Wall symbolized the hardened international barriers of the cold war, so the Internet, by promoting connection instead of division and fostering the free flow of knowledge, opinion, ideas, and business, may become the symbol of the post-cold war era.[6]

2.3 The Diminution of Government

If economic globalization and advancing technology have the wind of history at their back, then centralized government has that wind in its face. Since the late eighteenth century, a primary role of government in the United States has been as societal risk manager, owing mainly to what were accepted as natural limits to private sector risk management in broad areas of public interest as well as to some notable failures by the private sector to deliver effective risk-management tools.[7] Much government expansion, especially at the federal level since the New Deal can be tied to this role. And nowhere has it been truer than in the realm of national security.

Economic globalization and the proliferation of advanced information technologies have transformed the national security risk field and called into question the efficacy of government leadership in an environment that is essentially commercial. Not just economic trends or technological fads, economic globalization and the proliferation of advanced information technologies represent the bases of the international regime that has replaced the cold war structure. Operating under still evolving rules, logic, and structure, these forces are driven by free market capitalism, rather than an ideological and geopolitical struggle. In the words of Thomas L. Friedman:

---

[5]Robert Samuelson, "Computer Circus," *The Dallas Morning News*, April 3, 1999, 25A. The figures given in the paragraph are all from this source.

[6]Robert D. Hormats, vice chairman, Goldman Sachs Int., "Foreign Policy by Internet," *The Washington Post*, July 29, 1997, A-15.

[7]For an extensive exploration of the role of the U.S. government as societal risk manager, see David A. Moss, *Government, Markets, and Uncertainty: An Historical Approach to Public Risk Management in the United States* (Boston, Mass.: Harvard Business School Division of Research, Working Paper 97-025, October 1996).

> The defining document of the cold war was the Treaty (negotiated by governments), but the defining document of the post-cold war era is the Deal (negotiated by banks and corporations). The defining calculus of the cold war was territory and throw weight; the defining calculus of the post-cold war cyber era is speed—in commerce, travel, communications, and innovation. Einstein's $e=mc^2$ has been replaced by Moore's Law that states the computing power of computer chips will double every 18 months.[8]

Cold war structures were built around nations, in particular, the balance of power between the United States and the Soviet Union. The cyber era puts states in competition not only with one another but also with, on one hand, super financial markets, which can quickly destroy a nation's economy simply by downgrading its bonds, and on, the other hand, super empowered individuals such as Osama bin Laden, who can influence events not because they head a nation but because they can lead loosely defined shadow organizations, in part through wired global communications networks, such as "Jihad Online."[9] In China, in mid-1999, for example, the crackdown on the Falun Gong was prompted by its effective use of cyber space to establish itself in a way that, in the eyes of the government, elevated it to a counterforce to state control, even though the leadership of the Falun Gong existed outside China itself.[10]

Despite the many uncertainties these changes present, one thing is clear: The end of the cold war and the consequent ascendance of technology-driven economic development as the primary global organizing principle have moved the frontier between government and the marketplace—for goods, services, and ideas—away from the model of government as risk manager current in the years following World War II and toward reliance on private initiative. Although this movement has not yet redefined the boundaries among nations, it has redefined the roles of government and business within them.[11] In 1997, Jessica Mathews, president of the Carnegie Endowment Foundation, noted that "The most powerful engine in the relative decline of states and the rise of non-state actors is the computer."[12] Most often discussed in the context of economic policies, the effect of the computer relates to national security strategy as well.

From the end of World War II until the 1980s, the model of the government-business partnership prevalent in the noncommunist world was of strong central management, not only in

---

[8]Friedman, 42-43.

[9]Ibid., 43.

[10]Barbara Crossette, "The Internet Changes Dictatorship's Rules," *The New York Times Week in Review*, Sunday, Aug. 1, 1999, 1.

[11]Daniel Yergin and Joseph Stanislaw, *The Commanding Heights: The Battle Between Government and the Marketplace That Is Remaking the Modern World* (New York: Simon and Schuster, 1999). This source is drawn on here for historical and other information.

[12]Quoted in Geneva Overholser, "Internet Transforming Everything," *The Dallas Morning News*, Aug. 2, 1999, 11A.

national security but also for the economy, and the tasks involved in management were considered of such magnitude that only government could accomplish them. In the United States, in the wake of the depression of the 1930s and the wartime expansion of government that followed it, the notion of central government as protector, economic planner, and final repository of risk made sense; and not until the oil crisis of the late 1970s, after a period of relative peace, prosperity, and generally rising affluence, did this model come into serious public question. The "stagflation" of the 1980s—the lethal combination of inflation and rising unemployment—and the seeming inability of public policies to deal with it revealed the strain on the government-controlled economy. In combination with intransigent social pressures deriving from the civil rights and antiwar movements, these forces provoked public rethinking of government's role in the economy as well as in society in general and led to rightist political victories throughout the industrialized world.

These rightist governments privatized public assets, denationalized basic industries, and reduced government regulation of major sectors of national economies, and not only in the west. Even the Soviet Union and the People's Republic of China took tentative and, in the case of the Soviet Union, sometimes ill-fated steps toward economic liberalization. The idea of government supremacy, which had been nurtured for decades by planners, regulators, and advocates of strong central government, began to lose the trust of the people. The last vestige of trust was in the area of national security, but soon, as the cold war wound down and finally ended that, too, came into question. In the late 1980s and early in the 1990s, rightist governments were succeeded by more moderate "third way" regimes. Still, some of the new administrations were confronted by a deep current of public skepticism of government's ability to manage or even protect national interests.

Internationally, the dissolution of the Soviet empire left the United States the world's only superpower and faced with a dramatically changed national security equation. The specter of nuclear war and the policy of containment were replaced by compartmentalized threats, which were spurred by re-emergent ethnic and regional territorial conflicts, the viciousness of which offered a moral confrontation more than a threat to U.S. security, and by technology-driven economic globalization that take the form of terrorism rather than direct state-to-state action. These include contemporary permutations of past threats of nuclear proliferation and chemical or biological weapons, as well as what is new and emblematic of the cyber era, the potential for an attack on the complex system of systems that enables critical information to flow through the economy, government, and society in general so that they may function on a daily basis. In 1997, a presidential commission found that although the nation's dependence on these systems had grown tremendously between 1985 and 2000, an understanding of the risks presented by such dependence had not.[13]

---

[13]*Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C.: U. S. Gov't Printing Office, Oct. 20, 1997), 5.

The role of government in general, and of the traditional national security establishment in particular, in managing emergent risks is less clear or widely supported now as government supremacy was in national security matters during the cold war. When primary targets were military command-and-control centers, missile silos, ships at sea, and the like, there was no real question of who was in charge or what alternatives for response were available in event of attack. As the twenty-first century opens, the targets are as likely to be privately owned assets and commercial information networks as defense systems. Just as financial markets, for example, now exert enormous influence on governance by insisting on transparency and sound fiscal policies, so such new areas of vulnerability constrain traditional law enforcement, intelligence, and military approaches to national security.

Today, the future course of these forces are about as well understood as the future path of the cold war was in 1946. These are salad days for prophets; opinions on where all this is headed are not lacking. But technology appears particularly inspirational— predictions abound on whether it is taking the world toward utopia or apocalypse—and that the historical landscape is littered with examples of unanticipated consequences of one or another technological innovation seems not to deter the urge to prophesize. Thomas Edison, for example, thought the phonograph would be used to reproduce speech, rather than music; Morse envisioned no commercial use for the telegraph. Technology led in the 1920s to putting hydrogen in zeppelins and in the 1960s to prescribing thalidomide for morning sickness. More recently, in the 1980s, a group of scientists convened at MIT to consider the potential effect on society of the PC. Did they foresee that it revolutionizing publishing, mass communications, scholarly research, financial analysis, the conduct of business, movie-making, even games? They did not. Its greatest impact they concluded would be on shut-ins—those too ill or restricted to reach mainframes.[14]

It was not too surprising, then, that as the twentieth century drew to a close some saw the technology of global connectivity as the way to borderless world peace, while others stockpiled supplies for an anticipated global collapse and a reversion to primitive states to be caused by computer failures with the binary change from 1999 to 2000.

Considerations of strategies for managing the risks of the cyber era ought not become trapped in the belief that either the past or even the present offers a reliable basis for predicting the future. With the end of the cold war, the world is poised on the edge of a knowledge revolution that the future may regard as a milestone in human progress, one that may equal if not dwarf any other in human history. Fundamental rules of life are being rewritten, from genetics to astrophysics, and with that new uncertainties appear.

In *The Age of Spiritual Machines*, Ray Kurzweil has predicted that by 2020 a $1,000 computer will have the same computing capacity as the human brain and in the same time frame

---

[14]Edward Rothstein, “The Future Works, Sometimes,” *The New York Times*, Feb. 23, 1997, 4.

that science will be able to replicate any body part.[15] These predictions may or may not be realized, of course, but not long ago such a forecast would have belonged to the realm of science fiction. Instead, as the twenty-first century begins, to many serious people it seems perfectly plausible.[16]

When change is the norm rather than a deviation and economic connection rather than political division is rising as the world's primary organizing principle, the largely quantitative means of calculating risk used for national security strategy in the more bordered and static era of the cold war—territory, troop size, missile counts, delivery systems, and throw weights—do not easily fit the risk environment now taking shape.

Many of these means originated in another milestone era that marked the boundary between the past and the modern world—the Western Renaissance, a moment of unprecedented philosophical innovation, territorial exploration, and scientific inquiry. The expansion of knowledge and human understanding then challenged the deeply rooted belief that the future was a whim of the gods and that human beings were essentially passive before nature. Tradition and superstition began to lose their hold in the Renaissance on how people approached their lives, leading to the first studious contemplation of the concept of risk.[17]

Of course, in ancient and medieval societies people considered the future, made decisions, and pursued interests, but they did so largely by relying on custom and insight and with no real understanding of calculating risk or of the nature of decisionmaking. Not less rational than prognosticators today, they simply lacked the tools for and comprehension of modern rational decisionmaking.

A capacity to conceive of possible changes in store and of the risks they may present and then to choose wisely from among alternatives to manage those risks lies at the heart of modern society. Yet those who believe that even in the cyber era the best decisions may be based on quantitative methods still contend with those who believe in using more subjective bases to interpret the uncertainties ahead, the principal difference between them being their view on how much the past determines the future.

Most present methods for interpreting the future are owed to early mathematicians and their explorations of ways to define and manage uncertainty. In 1654 in France, Blaise Pascal, the mathematician and philosopher, and Pierre de Fermat, a lawyer and mathematician, while playing

---

[15]Ray Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence* (New York: Viking, 1999).

[16]James Adams, personal communication to the author, Feb. 18, 2000.

[17]For historical and other information, the balance of this chapter draws largely on two sources: Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley, 1998); and Ron S. Dembo and Andrew Freeman, *Seeing Tomorrow: Rewriting the Rules of Risk* (New York: John Wiley, 1998).

with a gaming puzzle, hit upon the theory of probability. For the first time, science—numbers—could be used to make decisions and forecast the future. What began as a gambler's toy grew into a powerful method for organizing, interpreting, and using information.

Other significant discoveries followed, including (in 1705) Jacob Bernoulli's Law of Large Numbers, which drives such modern activities as opinion sampling and the testing of new drugs. The most significant insight of all may have come in 1703, when Gottfried von Leibniz observed to Bernoulli that "nature has established patterns originating in the return of events, but only for the most part."[18] The qualification "but only for the most part" was more profound than Leibniz may have realized, for it provided the principle underlying the notion of risk. Without that qualification, everything would be predictable and no change—or uncertainty—would occur.

Throughout the rest of the eighteenth century, the concepts of normal distribution, standard deviation, and law of averages (de Moivre, 1730), the idea that satisfaction resulting from small increases in wealth is inversely proportionate to the quantity of goods possessed (Bernoulli, 1735), and the theorem that presented a mathematical method for blending new information with old and that thereby enabled intuitive judgments about the future to be developed in an orderly way as actual events unfolded (Bayes, 1764), all were discovered by mathematicians and logicians and, combined, formed the basis for rational behavior for the next two hundred and fifty years. Thus, every major quantitative tool used today in risk management and decisionmaking grew out of developments that occurred 1654 and 1760—with two exceptions: Francis Galton's discovery in 1875 of regression to the mean (or that the driving force is always for a return to some known range of normality) and Nobel Laureate Harry Markowitz's discovery in 1952 of a way to demonstrate mathematically why putting all the eggs in one basket is unacceptably risky.

Most of these quantitative methods assume a stable base from which change emanates progressively or as an anomaly. More subjective methods tend to view change as a largely independent process that is influenced less by the past than by unpredictable human predilections, or, as Winston Churchill said, because "the future [is] just one damn thing after another."[19]

Traditional models of rationality specify how people should make decisions in the face of risk and how the world would be if people behaved as specified, but in the world outside models people do not always follow rules of rationality to address uncertainty or probabilities of risk. This does not mean Macbeth was right—life "is a tale told by an idiot"[20]—but, rather, that the practical limitations of rationality need to be acknowledged. In the words of Nobel Laureate Kenneth Arrow, "our knowledge of the way things work…comes trailing clouds of vagueness.

---

[18]Bernstein, 5.

[19]Cited in Barbara Holland, "You Can't Keep a Good Prophet Down," *Smithsonian* (April 1999), 74.

[20]Shakespeare, *Macbeth*, V, v, ll. 26-27.

Vast ills have followed a belief in certainty…caution is needed because we cannot predict consequences."[21]

As an anonymous observer once noted, the problem with the future is that there are so many of them. In an era of discontinuity, how best to consider what changes are in store and what kinds of risks they may present to the nation? The answer may lie in the behavioral sciences—economics, psychology—more than in the calculable realm of mathematics. More specifically, it might be found in the concepts of reward and regret.

For example, when in the spring of 1999 the U.S. Congress voted overwhelmingly to fund a new missile defense system and the president approved it, neither acted out of an assessment of calculated risk. They acted out of political instinct (and, in the case of congress, perhaps home-district economics) and a sense that the proliferation of nuclear missiles among terrorist organizations or rogue states could pose a terrible threat to the United States and that taking this action now was better than not taking it and regretting that later. Reportedly, the technical efficacy of the new system against the threat did not rank real high among reasons for funding it. Many similar examples can be found, from the swine flu vaccination program of the 1970s to the panic in 1998 in Great Britain about mad cow disease. The potential regret derived from not acting far outweighed calculations of the real probability that the worst would actually occur. Thus the power of regret in the formulation of public policies. Voters can blame politicians who decide policy either for acting or for not acting, and the politicians may—or may not—survive the next election. The tendency in the real world versus the realm of theory often is to act even in the face of insignificant statistical risk.

In considering the blended risk of, say, an attack on the privately owned and operated financial system in order to harm the nation, the conflict between private and public sector perceptions of risk and regret becomes apparent. In the fading, slow world of heavy regulation, government would assume the risk and through various means indemnify the institutions involved from failure. In the fast world of diminished government, business is free to organize as it seems sees fit and to engage in markets it sees as most fertile for its products and services. In doing so, however, whether it realizes it or not, business assumes a new level of responsibility for the public good and adds a new factor of regret to its risk assessments.

As the cold war wound down and as the pursuit of economic reward became, for most nations, the driving force of global policy, emerging new linkages and new forms of competitiveness dramatically altered the national security landscape into one where private assets may become primary targets and conventional business models may prove inadequate to comprehend fully the tension between risk and uncertainty. Heavy reliance on statistical probability and other quantitative decision theories to guide choices that affect such issues as network security are

---

[21]Quoted in Bernstein, 7. Also see Kenneth J. Arrow, "I Know a Hawk from a Handsaw," in *Eminent Economists: Their Life Philosophies*, edited by Michael Szenberg (Cambridge, Eng.: Cambridge University Press, 1993).

liable eventually to cause regret when an exposure assessed as financially insignificant in terms of probability can be exploited by an adversary, bringing embarrassment and public alarm that might translate into lost confidence in the enterprise. As business increasingly separates from central government, it may not need to adopt the high sensitivity to risk of the politician but, instead, to redefine its traditional concepts of risk to include the new elements that come with dependence on an information infrastructure whose ownership and control are greatly different.

But such new linkages are overlays on, not displacements of, existing political, cultural, ethnic, and religious borders. The risk dynamic of the post-cold war era—what Thomas L. Friedman calls "The Lexus and the Olive Tree"[22]—is the conflict between the promise of material reward offered by participation in the new global economy and the powerful psychological hold that territory, history, and culture have on people, a hold evident in many emerging market economies as well as some established ones.

Perhaps the best presentation of the risks of discontinuity and the error of relying fully on the past to project the future comes not from a scientist but from the novelist and essayist G. K. Chesterton. In 1909—though he might have been commenting on the United States's entry into the cyber era—Chesterton wrote:

> The real trouble with this world of ours is not that it is an unreasonable world, or even that it is a reasonable one. The commonest kind of trouble is that it is nearly reasonable, but not quite. Life is not an illogicality; yet it is a trap for logicians. it looks just a little more mathematical and regular than it is; its exactitude is obvious, but its inexactitude is hidden; its wildness lies in wait.[23]

[22]This is the theme of Friedman's *The Lexus and the Olive Tree* (New York: Farrar, Straus, and Giroux, 1999).

[23]Quoted by Bernstein, 331; see also G. K. Chesterton, *Orthodoxy* (New York: Lane Press, 1909).

Chapter Three

Wildness in Wait: One Example

Well, who you gonna believe—me or your own eyes?[1]

The seminal event of the cyber era may have taken place back in 1987. On Wall Street it was a bull market year: U.S. stocks appreciated steeply in the first eight months, despite rising interest rates, and by August the Dow Jones Average reached its (quaint by the standards of the years 2000) peak of 2722. Stocks were valued at precedent-setting levels owing to expanding foreign and domestic investment in common stock mutual funds. The rising values predictably elevated the funds' risk exposure by heavy investment in a rising market, but in the view of fund managers the risk was cushioned by the capability for quick automatic selling to mitigate the effect of a market decline. Justification of the rapid appreciation of stock values was elusive and mostly ignored in the belief that equity markets are independently secure enough to handle the escalation in values and the accompanying increase in the volume of transactions.

From the close of business on Tuesday, October 13, 1987, to the close of business on Monday, October 19th—and without anticipation by any major market player—the Dow fell by almost one-third, or about $1 trillion of value. What was extraordinary was the speed with which prices fell, the unprecedented trading volumes involved, and the consequent threat to the entire U.S. financial system. The threat loomed so great that the next week the president of the United States announced the appointment of a special task force to determine what had happened, and why, and to provide recommendations within sixty days to prevent it from happening again.

In its *Report to the President*, the task force, chaired by Nicholas F. Brady (who the next year was appointed as Secretary of the Treasury), reached some remarkable conclusions. It asserted that what had traditionally been seen as separate markets—those for stocks, stock index futures, and stock options—had evolved into a single, interdependent market facilitated by high-velocity computer-driven telecommunication technologies that tightly linked new financial instruments of various kinds, trading strategies, and clearing and credit mechanisms. This condition became frighteningly clear in October 1987, when suddenly, overwhelmed by contagion-like automated selling by institutional investors, the newly interdependent market segments were unable to maintain linkage, disengaged, and—lacking the equilibrium of connection—cascaded into near free fall.

The regulatory and other structures designed decades earlier for markets assumed to be separate were incapable of responding quickly to such pressure. The automated transaction system of the New York Stock Exchange, used by index arbitrageurs to link the interdependent

---

[1]From *Duck Soup*, Paramount, 1933, film. Spoken by Chicolini, played by Chico Marx, to Mrs. Teasdale, played by Margaret Dumont.

markets, ceased to be useful for that purpose by mid-day October 19. The growing concern that some clearinghouses and major market participants might default severely inhibited the inter-market buying activities of other investors, and the private equity market could not by itself absorb the major selling demands. Only intervention by the Federal Reserve restored confidence and provided the degree of liquidity needed to re-engage the markets and stabilize the situation.[2]

How could this have happened? How could large investors, brokers, and regulators, endowed with talent, sophistication, and experience, have missed the warning signs of impending crisis? Economists may disagree on the causes of the sudden market decline, but one thing is clear: despite their collective wisdom, at the time, major market players proved captive to well-fortified traditional beliefs about risk and opportunity that they were reluctant to question, even though underlying assumptions were daily being challenged right before their eyes. Noted by some, those warning signs were not believed in the sense of being integrated into the way the market was interpreted and the strategies formulated. When the crisis came and its concerted effects appeared, these players saw clearly that no one or coalition of them could have done much to prevent it. The wildness that awaited them was not so much hidden as ignored. Reforms quickly followed.

The stock market break of 1987, however dramatic, was emblematic of an emerging truth of the post-cold war cyber era: many activities once considered separate are now linked by information technologies, thus becoming, if often only subtly, interdependent.

---

[2]*Report of the Presidential Task Force on Market Mechanisms: Submitted to the President of the United States, the Secretary of the Treasury, and the Chairman of the Federal Reserve Board, January 1988* (Washington, D.C.: U. S. Gov't Printing Office, PB88-162680, January 1988).

Chapter Four

Old Questions, New Answers

Formlessness and chaos lead to new forms. And new order.
Closer to, probably, what the real order is.
—Jerry Garcia[1]

Two hikers encounter a tiger. One hiker turns to the other and says, "There's no point in running. That tiger is faster than both of us." "I disagree." replies the other, "the question is not how fast we are relative to the tiger, but whether I'm faster than you."[2]

Asking the right questions is critical to formulating any kind of strategy. For example, no sooner had the Soviet Union formally passed from existence than the question of what to do about Russia presented itself to the United States and its NATO allies. The question seemed to be, how can the United States and its allies help remake Russia in the western image of a democratic, free-enterprise state, and the answers led to the strategy of "shock therapy," which privatized huge portions of formerly state-owned assets in the belief that the necessary market infrastructure would follow because new entrepreneurs would demand it. Instead, of course, the new entrepreneurs, both legitimate and not, simply stripped Russia of resources and exported the money, leaving Russia in a dangerous, destabilizing downward spiral. If a different question had been posed—if instead of endeavoring so quickly to make Russia into a strategic partner—the question had been, "What can Russia accomplish?" a different strategy might have emerged and Russia's position today might be better.

In the case of a strategy for managing new kinds of national security risks that the United States faces in the cyber era, the question might well be not only how should the existing national security apparatus be adapted but, rather, what kind of apparatus is needed. Separate questions, they are likely to yield different answers. The questions posed by the main challenges to the four major institutional players in the new national security apparatus—the military, law enforcement, financiers, and merchants—are, respectively, "who is the enemy?" "who is the criminal?" "what is the risk?" and "where is the market?"

4.1 The Military: The Return of the Warrior

The United States is not the only nation pondering these issues. One of the hottest military publications in China is a book by two professional soldiers in the People's Liberation Army,

---

[1]Carol Brightman, *Sweet Chaos: The Grateful Dead's American Adventure* (New York: Clarkson Potter, 1998), 13.

[2]Quoted in Ron S. Dembo and Andrew Freeman, *Seeing Tomorrow: Rewriting the Rules of Risk* (New York: John Wiley, 1998), 85.

Colonels Qiao Liang and Wang Xiangsui.[3] They proposed a new military strategy, advocating moving away from conventional martial doctrine toward "unrestricted war," which involves multitasking of aggression/defense to include acts of direct terrorism, cyber attacks on critical infrastructures, financial attacks on currencies, political interference, and other methods carried out by military and nonmilitary organizations. Provoked by what they considered U.S. intrusions into relations between China and Taiwan, Ciao and Wang asserted that if a confrontation were to come. "unrestricted warfare" would be the only way a militarily weaker nation like China could confront a superpower like the United States. They believe this strategy would be a viable alternative to seduction by an economically fatal arms race.[4]

This consequence of the United States's role as the sole superpower may have been predictable, but its effects are not calculable using traditional models of national security risk. In a way, the colonels' proposal suggests a reversion of military organization—a reversion from soldier to warrior.

The U.S. military is supremely prepared to defeat soldiers. It has the technology, training, and raw power to shatter conventional enemies, but the newest forms of threat will probably not come only from other soldiers engaged in alternative forms of warfare. They may also come from warriors—individuals of volatile allegiance who are inured to violence and have little or no stake in a particular civil order. Although warriors have been around for eons, the modern soldier, with codes of conduct and national loyalty, particularly in the west, is a product of the maturing of the nation state over the last three hundred or so years. The warrior seemed to fade from the scene as organized armies were formed and professionalized. But now, as empires crumble and only the United States holds superpower status, and as trade and technology challenge the borders and cultural prejudices of many traditional societies, the warrior is back, still brutal but far better armed and far more diverse in tactics.[5] Just look at Somalia and Kosovo for examples of warriors in action and for the difficulty of matching conventional military tactics with the tactics of modern warrior movements. As one observer noted, "The barrage of personal and propagandistic e-mail from both the Serbs and the KLA [Kosovo Liberation Army] in Yugoslavia was reminiscent of Germans dropping stick bombs from zeppelins during World War I—ineffective but heralding the dawn of a new and more dangerous age."[6]

So the soldier's question, "who is the enemy?" cannot be answered with the clarity even of the 1980s. Military adversaries seeking to complicate and disaggregate war as much as possible by enlisting nonmilitary partners and by including terrorism, drug trafficking, environmental

---

[3]See John Pomfret, "China Ponders New Rules of 'Unrestricted War,'" *The Washington Post*, Aug. 8, 1999, A1.

[4]Ibid.

[5]Ralph Peters, "Soldier vs. Warrior: The Modern Mismatch," *The Washington Post*), March 7, 1999, B1.

[6]John Arquilla, senior analyst at the RAND Corp., cited by Linton Weeks in "From the War in Kosovo, A Fusillade of E-Motion," *The Washington Post*, April 10, 1999, C01.

attacks, computer viruses, media assaults, and financial manipulation in their strategies scramble the traditional soldier-to-soldier concept of combat, and warriors with no regard for the “rules of war” fragment the answer even more.

4.2 Law Enforcement: A Race with Technology

The law has not kept pace with technology, nor can it be expected to. The complicated tension between the civil need of nation states for a stable body of law, modified (in democracies) only through deliberative legislatures or process-oriented court interpretation, and the often rapid transforming effects of technology on the economy and societal structures is historical. In the less bordered cyber era, as new technologies based national security risks have emerged, this tension has been complicated even further by outmoded definitions of electronic crime, overlapping investigative authorities, and confused domestic and international legal jurisdictions. Often, in an attempt to clarify some of these issues, law enforcement agencies have responded with programs that conceivably may improve their capabilities to assess and control new risks but, at the same time, challenge traditional concepts of individual privacy and freedom of speech. For example, a proposal by Federal Bureau of Investigation (FBI) in mid-1999 to establish within that organization a capability to monitor international computer networks as a means to detect attacks met great skepticism not only from civil libertarians and privacy advocates but also from U.S. businesses and their foreign partners.[7] Such “big government” solutions, even when well intended and reasonably well safeguarded, face rough going in the market of public opinion.

Thus far domestically, many recent court decisions have come down on the side of individual privacy and free speech, with exceptions relating only to the most extreme cases, such as the ruling prohibiting an abortion rights group from publishing the names of targeted physicians. Even though advancing information technology has altered the way people go about their lives, it has not yet changed the law, because courts and legislatures generally seem reluctant to reshape traditional concepts of rights to accommodate still emerging technologies. Unlike the rise of telecommunications and broadcast television, in which new technologies generated new bodies of law and extensive government regulation, the Internet is being treated much like books or newspapers, with judges emphasizing the primacy of the First Amendment. This trend follows the Supreme Court decision of 1997 striking down the Communications Decency Act as suppressive of free expression.[8]

An indication of the new level of tension in the cyber era between law enforcement and individual rights is the debate over U.S. policy on encryption. Historically, encryption has been almost exclusively the province of governments, used to achieve secure diplomatic and military

---

[7]John Mankiff, “Plan Would Let FBI Monitor Nation’s Computer Networks,” *Dallas Morning News*, July 28, 1999, 1-A.

[8]Joan Biskupic, “Internet Law Favors the First Amendment,” *The Washington Post*, Sept. 12, 1999, A-2.

communication for national security reasons. With the growth of the Internet, and as encryption has become a critical tool—sometimes called the "golden key" of global electronic commerce—the debate that has arisen comes down to this: In the post-cold war cyber era, can national security, police, privacy, and free-market concerns over the use of encrypted communication be reconciled in a way that will meet everyone's interests?[9]

Though legal rulings on government control of encryption remain few, one important appellate court ruling in May of 1999 overturned on a 2-to-1 vote the Clinton administration's restrictions on posting encryption codes on the Internet. Federal judge Nancy G. Edmonds, who wrote the majority opinion, noted that everyday reliance on modern information technologies puts government efforts to regulate encryption in opposition to the First Amendment rights of cryptographers seeking to expand their science, and also to the rights of citizens to receive the bounty of encryption advancement.[10] Although the issue ultimately may be heard by the Supreme Court, in September of 1999 the Clinton administration, perhaps acknowledging the futility of national control over encryption, substantially loosened government controls over U.S. exports of encryption technology, mostly by abandoning its long-held position that encryption systems are weapons and that government must retain its capacity to break any encryption system exported in order to enhance law enforcement and other security agencies' capability to conduct intelligence, investigate terrorists, abate narcotics trade, etc.

On an international level, the first dilemma that the United States, or any state, faces in defending its critical information infrastructure is to distinguish between natural anomalies and criminal or sovereign attacks, which may have originated abroad and been launched through global networks. Investigators attempting to make this distinction may be stymied by a collision between fundamental principles of physics and those of international law, namely, that although electrons may flow through networks that freely cross borders, the authorities of governments do not. According to the principles of sovereignty, every government has exclusive jurisdiction over events within its borders, and, historically, foreign agents have not been permitted to operate in another state's territory without that state's permission. Individual governments try to exert control over data in domestic systems just as they would if these had physical form, and they may consider a situation in which foreigners investigate the criminal misuse of their systems to be a computer crime or, worse, an attack. The widespread, inexpensive availability of the technology necessary for international attacks across computer networks, combined with the anonymity that the technology can provide its users, makes it difficult for investigators to determine whether responsibility for an attack rests with an individual, a group, or a foreign government. Without a

---

[9]Ethan B. Kapstein, *Regulating the Internet: A Report to the President's Commission on Critical Infrastructure Protection* (Minneapolis, Minn.: University of Minnesota, Humphrey Institute of Public Affairs, June 1997), 27.

[10]Biskupic.

credible admission of responsibility, attributing an attack to its actual source may not be possible with confidence.[11]

The law enforcement question, "who is the criminal?" loses much of its focus in cyberspace, where the rules and divisions of the physical world do not readily hold. The gypsy nature of most cyberspace crimes and security breaches suggests that even draconian controls at the national level might not be effective in either preventing them or identifying their perpetrators quickly enough to avoid damage.

4.3 The Financier: Turning Uncertainty into Risk

Perhaps nowhere else have quantitative models designed to convert uncertainty—such as debtor behavior, the occurrence of natural disasters, and even how long someone may live—into measured risk been so widely relied upon as in the world of finance. Financial institutions, after all, are nothing more (or less) than risk traders—buying one risk and selling another. But financial markets have become substantially complex, and to keep pace financial institutions have had to develop increasingly innovative ways of defining and controlling their risk exposure. Huge markets for new financial products, from derivatives to bundled asset-backed securities, have evolved from advanced modeling and computing capabilities as ways to lay off or assume risks of various kinds. Given that some of the biggest, most respected names in finance—among them, Merrill Lynch, Bankers Trust, the Long Term Capital Fund, Britain's National Westminster and Barings Banks, Germany's Metallgesellschaft, and Japan's Daiwa Bank—have in recent years suffered from their judgments about risk, the question naturally arises whether they relied too much on models and not enough on observation. The question gets to a central truth about risk and reward, namely, that they are imprecise, subtle concepts with constantly shifting situational meanings.[12]

The brilliant body of work done over the past couple of centuries in developing mathematical methods for converting uncertainty to calculated risk not only does not embrace this subtlety but, particularly in the calculation of financial risk, seems designed specifically to exclude it, often in favor of finely tailored measurements to equally tailored uncertainties. Nevertheless, mathematical models are indispensable to the management of risk in the high-velocity and immensely complicated global financial markets of the post-cold war era. But the heightened influence of financial institutions in developing rules for the new global economy, mirrored by the reduced role of most governments in the management of national economies, suggests that exclusive reliance on these models will not provide a comprehensive enough

---

[11]Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Old Law for a New World? The Applicability of International Law to Information Warfare*, Institute for International Studies, Center for International Security and Arms Control, Project on Information Technology and National Security, Stanford University, February 1997, 25.

[12]Dembo and Freeman, 21.

approach to addressing the new level of uncertainty present in modern financial markets as these markets become increasingly integrated with and vulnerable to the effects of political volatility emanating from international economic reordering. This volatility is sometimes exacerbated by actions of the financial institutions themselves, as they seek to escape from, or capitalize on, instability within a particular nation or region. In many cases, in the aftermath of large-scale technological and macroeconomic shock, as seen in the 1990s, the complexity and interaction of forces for change create conditions under which it is almost impossible even to delineate potential outcomes, let alone predict them. In such an environment, calculating risk is a decidedly subjective process.

So, although the investor's question, "what is the risk?" has come to embrace greater uncertainties in the new global economy than usually have been considered in financial risk calculus, the substantial absence of organized authority in cyberspace, where financial markets largely function, also raises the stakes that financial institutions have in the security of the global information infrastructure, which are vital to the movement of capital. Without clear international covenants and the governments able to enforce them, this infrastructure, and the Internet in particular, has grown as a largely private-sector, regulated network, which relies for protection on the incentive of the benefits offered to participants. For the international financier, accustomed to exchanging government regulation for risk underwriting, this situation opens a new field of uncertainty requiring broader measures of risk than are found in most mathematical models and more comprehensive risk management strategies than are found among most financial institutions. Essentially, this uncertainty requires an extension of risk calculation from self-interest to the interests of the global financial system as a whole.

4.4 The Merchant: A New Value Chain

Following a period of skepticism among economists and others in the 1990s, the effect of information technology and advanced computing power on U.S. business productivity and competitiveness has grown apparent.

Almost every business is now, at the start of the twenty-first century, an information business, and, with millions of people at home and at work communicating electronically using universal standards, the strategic foundations of enterprises are now being challenged in ways never before experienced. Business and industry definitions, as well as competitive advantages, are up for grabs, because customers increasingly have access to a rich universe of alternatives and suppliers exploit direct access to customers. There is little value in cultivating a close relationship with a major buyer, for example, if it posts its requirements on the Internet and receives bids from any interested supplier.[13]

---

[13]Philip B. Evans and Thomas S. Wurster, "Strategy and the New Economics of Information," *Harvard Business Review* (September-October 1997), 71-82.

Meanwhile, new information capabilities, such as just-in-time inventorying and mass customization, and technology-driven changes in the ways such traditional operating cost elements as economies of scale and the interactions of customers, suppliers, and government affect the bottom line have removed much of the traditional friction of doing business and given birth to more fluid and network-reliant business models. These models depend on outsourcing core operations and are geared toward building competitive power and generating new sources of revenue mainly through mergers, acquisitions, and strategic partnerships.

Information is the glue that holds it all together. The conventional view of a value chain that links a business to its markets is a linear flow of physical activities. But in the new business models a value chain must also include all the information that flows within a company and between a company and its suppliers, its distributors, and its existing or potential customers. Supplier relationships, brand identity, process coordination, and customer loyalty all depend on information, and a failure to appreciate this can be traumatic. Consider the near demise in 1999 of the *Encyclopaedia Britannica*, one of the best known brand names in the world, as customers moved to CD-ROMs while *Britannica*'s management failed to see that their real competitor was the computer, which parents anxious to do the right thing for their children were buying instead of encyclopedias.[14]

Value chains are being recast in almost every sector of the economy because of the new paths through which information now moves. As a result, many businesses are reformulating their strategic assumptions as entire industries undergo fundamental structural change and historical patterns of competition deconstruct. For example, assets such as regional sales and distribution systems, which once provided a competitive advantage as paths to market, can quickly become high-fixed-cost liabilities when even a relatively small percentage of customers migrate to electronic commerce. The value of information has skyrocketed, and the effect is seen not only in the evolution of standards that allows broad reach and connectivity or in the redesign of business structures but also in a true shift of market power between buyers and sellers as increased buyer options and declining costs of changing suppliers require businesses to design new customer-affinity strategies.

Of the four questions addressed here, answers to the merchant's question, "where is the market?" are probably the most revolutionary. The appearance of the new global economy following the end of the cold war, and the tremendous growth of information technologies in the developed world, gradually spreading to the less developed parts of the world as well, have scrambled concepts of business organization and the pursuit of markets that were operable for half a century. As the twenty-first century begins, almost every business competes in two worlds: a physical world of resources and a virtual world of information. Unlike the military, law enforcement, or even financiers, business has had to respond almost immediately to these new

[14]Ibid.

market conditions or risk failure. The result has been one of the most active periods of corporate realignment in history.

The problem is that, although these institutional questions remain valid, the answers are not likely to be found by looking back into the more static, partitioned world of the past and using tools that were successful then. That world now is morphing into one of connection and interdependence among the players. The kinds of national security and other challenges present by this new technology-driven, economically more open, and ideologically more flexible world beg some additional questions, the answers to which may be found in a new model of the government-business relationship. The need for a new model is especially important in the cross-cutting area of intelligence gathering—what kind of information is needed to manage the new risks, how may it be gotten, and how may be shared among stakeholders?

In its consideration of these questions, the President's Commission on Critical Infrastructure Protection (1996–98) assumed as a truism that governments, financial institutions, and businesses, once they possessed reliable information on the threats to and the vulnerabilities of the information networks upon which they relied, would act out of self-interest to make the networks secure. This truism aside, in the post-cold war world, government—in particular, the military, the intelligence community, and general law enforcement—no longer is the only player at the front line of national defense. With economic interests dominating international relations, banks and businesses, as the principal vehicles of economic development, may very well be the targets of those seeking to do the United States serious harm.

The differences in concepts of risk, needs for information, and in the weights assigned to threats by the public and private-sector players present formidable barriers to the creation of any mechanism for sharing information among all of them. The changing dynamics of the government-business partnership, marked by the decline of the national security state and the rise of what may be termed the market state, have only heightened the natural tension between government and business, a tension that will increase if, as seems likely, the present trend toward commercial dominance continues. The compartmentalized responsibilities and distinct delineation of interests characteristic of the government-business partnership model of the cold war simply are ill suited to the more tightly integrated competitive risks of the new global economy. A growing belief among global businesses in the irrelevance of the strategic intelligence governments tend to seek has encouraged their independent gathering of the tactical intelligence they need to successfully compete in world markets. Businesses are driven by their customers, profit, and shareholder value, not by the expressed interests of government,[15] which does not bode the end of the national security state but may foretell a reshaping of traditional national security structures and traditional approaches to intelligence gathering.

[15]James Adams, personal communication to the author, Nov. 17, 1999.

Chapter Five

New Questions, No Answers

It must be considered that there is nothing more difficult to carry out or more doubtful of success, nor dangerous to handle than to initiate a new order of things.

—Machiavelli[1]

Among the institutions faced with the need to adapt structurally in order to cope with the forces of the post-cold war era, government may face the biggest challenge. In one respect, the challenge is reminiscent of that posed in the Progressive Era, at the turn to the twentieth century, when many Americans realized that the government of the nineteenth century related to a sparsely populated and largely agricultural America and was inadequate to the needs of the industrialized and urbanized country taking shape. The questions then had to do with how to strengthen and activate government in order to expand its role as public risk manager, while today most questions have to do with how to deconstruct that role. This is so even in the realm of national security strategy, which was once the undisputed area of government supremacy in which the government-business relationship is that of sole procurer and secure supplier. Today, defense industries, while constituting what may be the last frontier of the state-controlled national security apparatus that emerged from World War II and which was sustained throughout the cold war, also are feeling the effects of the diminution of government and economic globalization.

The strategic conventions since the cold war have been challenged by the demise of the Soviet Union and by the emergence of more fluid, commercially based international alliances, the tremendous leveling effect of technology, new forms of internal instability of nations as they adapt to a new global economic order, and by the growing abandonment of forward basing as a means of military deployment.[2] In the fragility of the cold war, nearly everything was considered under the aegis of national security, and western governments largely controlled banking, transportation, communications, housing, and other areas now, through privatization, more and more being turned over to entrepreneurs and corporations.[3] The decline of the national security state is apparent throughout both the developed and developing worlds, and, even in a nation as protective of its arms industry as France, a socialist-led government has begun to open greater

---

[1]Niccolo Machiavelli, *The Prince*, Introduction by Christian Gauss, translated by Luigi Ricci, revised by E. R. P. Vincent (New York: Oxford University Press "World Classics," New American Library, 1952), 49.

[2]Testimony of former Senators Gary W. Hart (Dem.-Colo.) and Warren B. Rudman (Rep.-N.H.), Co-Chairs of the Commission on National Security in the 21st Century, before the House Armed Services Committee, House of Representatives, Oct. 5, 1999. C-SPAN [Cable-Satellite Public Affairs Network] broadcast.

[3]Jim Hoagland, "Global Riddle: Who Is 'Us,'" Who Is "Them'?" *The Washington Post*, Oct. 24, 1999, B-7.

roles for private enterprise and international cooperation in the manufacture and sales of advanced weapons systems. According to at least one observer, the most successful campaign waged by the Pentagon in 1999 was not in Kosovo but in "twisting the arms" of European leaders to join with U.S. firms in trans-Atlantic mergers rather than pursue a fortress-Europe approach.[4] Thus, even the most secret tools of war are slipping from the grip of nation states and becoming, like any other commodity, subject to the "creative deconstruction" of global capitalism.[5]

Talk of the dissolution of nations is premature, if at all reasonable, but the shifting boundaries between government and private enterprise within and among nations is indeed a reality—one with major implications for managing national security in the cyber era. Faced with the need to protect a critical information infrastructure designed primarily for commercial use but relied on by government as well, both parties must confront several fundamental questions:

- Who will gauge the risk?
- Who will formulate the security strategy?
- Who will choose among alternative responses, should an attack occur?
- Who will assure readiness?
- Who will pay for it all?

These questions are complicated, and the answers are even more complicated. But, given the growth of and increased reliance on information technology, global connectivity, and open markets, not only economically but also for national security, and as a new form of partnership is forged between government and business to accommodate the new reality, both the questions and the answers need to be examined.

5.1 Who Will Gauge the Risk?

The changing dynamics of this government-business relationship suggest the need for a more equal partnership in certain national security matters and make differences in the way each gauges risk more apparent. Although government may have a view of risk that is held fairly uniformly among its many parts, participants in the private sector may hold a variety of views on what constitutes risk and to what degree a risk represents either a threat or an opportunity. This difference is the first, and perhaps most important, problem to examine when considering how government and business may combine in a new way to manage jointly the national security risks in cyberspace.

Government leaders often define risk in the contexts of territorial security, economic security, public welfare, partisan political competition, or the maintenance of the degree of public

---

[4]Ibid.

[5]Ibid.

confidence needed to lead in a democracy. Events, actual and potential, that pose a threat in those areas are very likely to generate government action to mobilize public resources or to coerce the deployment of private resources in order to neutralize a perceived danger. The motives of a government in a specific case may range from the lofty to the crassly political, but risk is almost always interpreted in the public sector against a backdrop of what, in the view of current office holders, are the essential roles and needs of government in order best to serve the nation's interests. A regret-motivated bias toward preemptive action, even when the risk of a security breach or of direct attack remains slight, is quite common in the often risk-averse atmosphere of government.

Business leaders, on the other hand, often hold a narrower view of risk, one tailored more toward the specific interests of the enterprise. Typically, financial interests—new earnings, marketshare, cost reduction, losses in capital—provide the primary context for risk assessment and for the application of most risk management tools. Risk in business is also measured in terms of impediments to the operational capability to deliver a product to market or to the quality of the product. Risks to reputation also are important, affecting as they do customer affinity and public confidence.

Establishing a common ground between these divergent perspectives for gauging risk is complicated by restrictions, by law, regulation, and custom on information flows both between government and business and among businesses. The influence on industry's largely quantitative risk models of infrastructure interdependencies and post cold-war threats to national security is often less clearly definable than it was earlier. As the global business environment grows more deregulated and competitive, most private sector participants regard any new role for government with suspicion and with a reluctance to assume new costs to manage a risk that may extend well beyond the boundaries of an enterprise's interest.

The one common denominator is public confidence. Government and business both derive viability from it, view it as a critical asset, and—most important—will go to great lengths to retain it. Public confidence, however, is greatly influenced by complex dynamics of trust, with the resulting irony that, generally, when people have access to information and democracy is strong, so is distrust of the individuals, industries, and institutions responsible for managing risk.[6] The fragility of trust is indicated by its somewhat contradictory nature: hard to get, easy to lose. The reduced confidence in governments that became evident in the late 1970s, for example, may be linked with government's less than impressive performance in alleviating the economic and social difficulties of the last several decades. Similarly, skepticism of the sincerity of corporate claims of good citizenship runs high, and studies indicate as much distrust of big business as of big government in managing public risk. When it comes to getting and keeping public confidence, events that destroy trust (failure of government programs, cover ups, scandals; corporate failures,

[6]Paul Slovic, "Perceived Risk, Trust, and Democracy," *Risk Analysis* (June 2, 1993), 677.

such as harmful products or safety breaches that endanger the public) are not only more credible in the public eye than more positive events but also have a more lasting effect.[7] A common interest in anticipating and avoiding events that put public confidence at risk may well be the primary motive force for government and major business sectors to rethink their respective compartmentalized perceptions of risk and, then, to undertake a restyling of the traditional government-business relationship in regard to national security in order to determine risk jointly.

5.2 Who Will Make the Strategy?

Without doubt, the ultimate responsibility for the national security of the United States rests with the president as the head of government, political leader, and commander in chief of the armed forces. Although once only the federal government had the vantage point from which to survey the full range of threat conditions that influenced the formulation of national security strategy, as well as the resources to carry out a strategy, in the post-cold war world, where economic crises could pose greater threats than military crises, government alone no longer held that perspective. A strategy that depends predominantly on diplomacy, military power, and law enforcement is no longer sufficient to address today's threat environment.

The rise of unconventional warfare, the confused state of jurisprudence, the reconfiguring of risk, and the high-speed transformation of the global business environment combine not only to alter the conventional menu of probable targets of an attack but to require new forms of partnership to defend those targets. Leaving aside the complex legal issues involved in conducting law enforcement and offensive military actions in cyberspace,[8] the sheer number of privately owned and operated macro-systems on which nations and commerce rely renders government supremacy, or even leadership, improbable in the construction of defenses of either a state or its citizens against an attack meant to disrupt the wide array of services those systems provide. In this complex and mixed environment, traditional government views of managing national security risk will need to be mitigated by a commercial risk calculus, which itself will need to be expanded to value extra-enterprise conditions. A new set of tolerances for all participants will be needed, and new risk management strategies to fit them.

In May of 1998, in a speech at the graduation ceremonies of the U.S. Naval Academy, President Clinton announced the signing of a Presidential Decision Directive—PDD 63 (a result of work done by the President's Commission on Critical Infrastructure Protection in 1996 and 1997)—which attempts to address these new conditions. PDD 63 recommends the creation of an elaborate, government-led, public-private partnership structure that would depend heavily on intrasector information exchange and centralized government decisionmaking on risk and

---

[7]Ibid.

[8]William M. Arkin, "The Cyber Bomb in Yugoslavia," *The Washington Post*, Oct. 25, 1999, [On-line]. URL: http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm

response. Although the commission's report and the resulting PDD focus on new paradigms and new ways to manage risk,[9] both the commission's recommendations and the requirements of the PDD relate almost exclusively to vestigial concepts of defending the shores and apprehending criminals. The creation of the structures proposed in the PDD has been slow to get off the ground. With the exception of the banking and finance sector, whose self interest is evident[10] and where such efforts predated the commission's report, no major industry has yet really responded to the PDD's proposals for greater information sharing between government and business. The report and the PDD made an important contribution by formally recognizing the new character of national security risk, but many of the commission's recommendations and most of the PDD seem to remain too government-centric in their approach to its management to enlist the active participation of most of the business sectors involved.

What may be needed is a broader based, two-pronged strategy that would mix government and business interests in a new way. The first element would be *fortification*, or a series of actions taken by an enterprise, industry, or government agency to install information security technologies, which is a strategy that can be promoted by regulation, threat-information sharing, or direct incentive. The second would be *syndication*, which involves coalescing within and among industry sectors to form financial risk pools similar to those found in the insurance industry to prevent claims from unpredictable natural disasters from falling too heavily on a single insurer.

Fortification would not be a hard sell; nearly every organization today is aware of the value of its information, but the extension of business risk syndication concepts to national security matters puts pressure on traditional government thinking about its role in the formulation of a strategy of national security risk management. Such an extension would leave to industry sectors the task of gauging the risk of disrupted service, valuing its effects, and establishing financial and operational mechanisms by which those effects could be mitigated by some collective action largely independent of government. This approach suggests a role for government primarily as an information provider—telling industry groups about possible threats gathered through intelligence operations of different kinds—rather than information collector, a change that is not compatible with much existing law nor one likely to be received well by the deeply entrenched government national security apparatus that, for many good reasons, is reluctant to loosen its grip on such judgments. Thus, although the facts of contemporary life seem to indicate that neither government nor business is truly in a position to decide independently on the best strategy for

---

[9]*Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C.: U. S. Gov't Printing Office, Oct. 20, 1997).

[10]As a heavily regulated industry and one heavily dependent on public confidence, banking and finance already had a close relationship with government agencies already adapted to many PDD proposals. Resistance to increased information sharing with central law enforcement agencies, however, remains strong.

protecting the clear national interest in a secure and accessible information infrastructure, agreement on what the new alignment of responsibility is remains elusive.

5.3 Who Will Choose the Response to an Attack?

The question of who will decide, and on what grounds, whether a cyber disruption event constitutes an attack on the nation's interests, and, if so, on how to respond may be the most contentious area of all in restyling the government-business national security relationship. When targets are military or government facilities, the simple and clear answer is that the government decides; but when private business assets are the target, and a business risk calculus, rather than pure national interest applies, the answer is more complex. Predetermined boundaries for classifying such events would offer an advantage, but the complexity of global economic conditions, the rapid pace of technological change, and the subtlety of the new brand of threat all make defining such boundaries improbable. Collective decisionmaking, with its attendant imperfections and inefficiencies, may be the sole answer in the event of a cyber crisis.

One model for crisis management in decisionmaking might be the Financial Markets Working Group (FMWG), which was established after the stock market break of 1987 (see **Chapter Two**). The FMWG is a largely ad hoc organization nominally reporting to the president, formally chaired by the Secretary of the Treasury and composed of the chairs of the Federal Reserve, Securities Exchange Commission, and Commodities Futures Trading Board as principals, supported by other bank and financial system regulators as well as by large network of private sector financial leaders. When a market crisis occurs or appears imminent, these parties initiate instant communication to assess the origin and extent of the risk and to formulate action. Their task is to decide whether the markets can themselves handle the situation, or whether government action is needed to defend the larger system from a failure that could cause serious and sustained harm to the nation. Although the structure and operating methods of the FMWG may be instructive, the range of disparity in the interests of the parties and in the clarity of the crisis is liable to be considerably narrower in the financial world than in the arena of national security. Properly constituted, however, such a structure might provide at least a venue for joint decisionmaking when a major cyber crisis occurs—as one most certainly will. sooner or later.

5.4 Who Will Assure Readiness?

A cohesive strategy for cyber national security may require some kind of audit function to assure a state of readiness among its various critical components. If there is to be joint responsibility in this area, then there will also need to be a shared concept of preparedness to facilitate mutual trust and reliance and so that a rapid response may be decided and initiated with confidence. For heavily regulated industries and government agencies, extant oversight and examination processes may be enough—with appropriate focusing—to provide the transparency and stimulus needed to reach readiness. For other players, especially those in highly competitive

areas of business, where the formation of collective risk syndication mechanisms is liable to be difficult to achieve, the disparity of interests and the collision of goals may work against creation of common levels of readiness.

One perhaps controversial way to approach the task of assuring readiness may be to create a new national accounting standard for the security of enterprise information systems, including a readiness standard. Upon audit, a firm that failed to meet this standard might be subject to a contingent liability on its annual financial statements, to the extent that loss of the exposed information would reduce the firm's financial or market position (a possibility that would certainly get the attention of senior management). Establishing a standard level of information security would answer the question of how much information security is enough and result in a heightened state of preparedness.

The development of such a new national standard, however, would probably involve government in a major way, thus providing recalcitrant industries and enterprises with sufficient incentive to strengthen their resistance to a collective effort. When that resistance is combined with the immense technical complexity of developing a workable national accounting standard in a rapidly changing technological environment, the standard—failure to meet which would incur strong penalties—may prove impractical. Still, as evident in the financial services industry, auditable standards can work when they are used to establish a basic level of soundness. The potential for information readiness standard to establish a basic level of network security, whether developed with or without government involvement, may be useful to explore.

5.5 Who Will Pay for It All?

Unlike past national security strategies, the bill for all this cannot be borne by the government and, ultimately, taxpayers. Although government funding is clearly desirable in certain areas—such as education and basic research and development—public financing of the full range of activities necessary to assure the security of information infrastructure is not the best approach, for two reasons: the current and future availability of sufficient public funds for this purpose is, at best, uncertain; and in an era of declining government involvement in the economy, government may not have the political power to act independently to implement the actions needed.

Still, government remains the stakeholder with the greatest accountability for national security, even though that responsibility is shared by public and private sectors and the private sector has a clear self-interest. In the climate of a declining national security state and a less regulated economy, government may need to provide economic incentives for private sector engagement in the new national security role, rather than rely solely on legislative or regulatory requirements. Incentives might take the form of grants, in-kind assistance, guaranteed markets for security technologies, subsidized research, tax credits, accelerated depreciation schedules, tax-exempt bonds, direct loans, or loan guarantees. Distinguishing between the private sector's

fortification and syndication activities for the broad purposes of national security and more limited undertakings for purely enterprise reasons is a formidable task and one liable to be laden with subjective judgment.

Given the nation's experience throughout the 1990s with revising just one established order, namely, financial regulatory reform, there is no strong reason for optimism that the difficult questions discussed in this chapter can or will be answered quickly. Nevertheless, the process of redefining roles and creating a coherent strategy for cyber national security will need to begin, despite the predictable contentiousness it may generate. Nothing yet suggests that the cold war, the pre-cyber era model of national security, is likely to return. Instead, there is much to suggest the contrary—that a new model, based on shared and decentralized responsibility, is called for, not just in the future but now.

Chapter Six

Conclusion

Not everything that is faced can be changed.
But nothing can be changed until it is faced.
—James Baldwin[1]

Reordering the responsibilities, direction, and relative power of major institutions is a massive undertaking, usually accomplished only as a result of revolution, catastrophe, or some other form of fundamental societal dislocation. Accomplishing it peacefully is not impossible, however given three key elements: agreement on the definition of the problem, agreement on the appropriate solution, and agreement on a structure capable of delivering the solution.[2] Although each element may inherently be a source of contention, in democracies accessible political processes exist for their effective resolution. In the case of adapting the relative national security roles of government and business to the realities of the post-cold war cyber era, reaching agreement and forming a winning coalition among key stakeholders remains at a very early stage.

6.1 Agreement on the Definition of the Problem

At a fundamental level, there seems to be wide agreement in all sectors that the forces of economic globalization, advanced information technology, and diminished government that have emerged and gathered momentum since the ending of the cold war have brought into question the effectiveness of the structures and regimes that governed nations and constituted the international economic system since the end of World War II. Among major nations, and most political factions within them, the serious argument is over how, not whether to, cope with the profound changes in process and the uncertainties they present. This shared recognition of the inevitability of basic structural change represents a dramatic departure from the intense ideological struggles of the cold war, when change was often viewed from an adversarial perspective and considered stoppable only through the application of military power and a variety of economic restraints.

6.2 Agreement on the Appropriate Solution

Recognizing the inevitability of basic change and agreeing on how to solve its attendant problems are vastly different positions. There is little unity among major stakeholders on the

---

[1]Many electronic sources attribute this statement to James Baldwin, but none can provide a citation. A similar statement occurs in Baldwin's *The Fire Next Time* (New York: Dial Press, 1963): "To defend oneself against a fear is simply to insure that one will, one day, be conquered by it; fears must be faced."

[2]Ethan B. Kapstein, *Regulating the Internet: A Report to the President's Commission on Critical Infrastructure Project* (Minneapolis, Minn.: University of Minnesota, Humphrey Institute of Public Affairs, June 1997), 11.

specific nature, magnitude, and seriousness of problems associated with such change. Complicating this situation is that most if not all nations are on the cusp of the process, speculating on what may take place in the long term. Thomas Friedman has commented that the situation is so new it does not even yet have a name. Instead, it is defined by what it is not, "the post-cold war era."[3] There is good reason to believe that the true effects of these changes may simply not be discernable enough for governments and private businesses to be able to formulate a viable long-range strategy for dealing with them, and, instead, a more incremental approach may be warranted.

6.3 Agreement on a Structure Able to Deliver the Solution

The absence of agreement among key stakeholders on specific problems and solutions makes true structural realignment unlikely. This discord promises to be the greatest source of contention. So long as there is great dissent over the relative roles and responsibilities of participants in this new era, there will also be great inertia about changing extant structures. However, experimentation with cooperative mechanisms for dealing with new risks is feasible and may continue for an indeterminate period of problem and solution definition. As the recent agreement on financial system regulatory reform indicated, government leaders are often left no real option but to adjust to the more rapidly moving private sector when its many participants undertake whatever changes are necessary to compete in the new economy. Reluctant as military and law enforcement stakeholders may be to accept what seems the new reality of reduced government control, evolving conditions may well force acceptance on them in this new arena of national security.

6.4 What's Next

The dawning of the cyber era and the emergence of the new global economy imply neither the demise of all national security risks present since the end of World War II nor the obsolescence of all the national security strategies for managing them. Neither does it imply the uselessness of government in promoting the benefits of economic globalization, while also creating safety nets to protect large numbers of people from less beneficial aspects of markets. But, for the United States, it does imply added risks and, to manage them, a substantial change in the way the national security apparatus operates and how government interacts with the private sector.

During the 1990s, the Clinton administration and Congress convened numerous commissions, special panels, and study groups to consider the nature of post-cold war national security risks and to discuss changes that may be required in the roles of military and civilian national security agencies to manage those risks. Among the achievements of these groups may

---

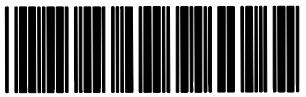
[3]Thomas L. Friedman, "Manifesto for a Fast World," *The New York Times Magazine*, Sunday, March 28, 1999, 43.

be their success in raising awareness within and outside government of the new, yet to be well understood kinds of national security threats found in cyber space, where so much business, government, and general communications activity is now taking place. As mentioned in section **5.2**, the Clinton administration responded to these analyses with PDD 63, a proposal for a government-business partnership designed to protect against cyber attacks on those public and privately owned infrastructures critical to national security and which depend for their daily operation almost totally on linked and, in most cases, global information networks. Flawed though PDD 63 may be by over reliance on government decisionmaking, it at least offers a modest new strategy for coping with this new form of threat. Harder work lies ahead.

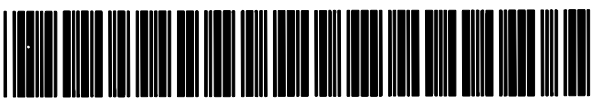
One of the serious national security issues liable to face the president of the United States taking office in January 2001 may be restructuring the U.S. national security apparatus in order to match its capabilities better with the threats of the twenty-first century. This promises to be a huge undertaking, fraught with serious political and economic risks. It may, however, be impossible for the new administration to avoid this task if the president is to carry out the highest responsibility of that office—the protection of the nation from attack.

Acronyms

CD-ROM	compact disk read-only memory
FBI	Federal Bureau of Investigation
FMWG	Financial Markets Working Group
KLA	Kosovo Liberation Army
PC	personal computer
PDD	Presidential Decision Directive



PPDALY



ISBN 1-879716-62-3