THE INFORMATION REVOLUTION AND NATIONAL SECURITY

Edited by

Thomas E. Copeland

August 2000

CONTENTS

iii

TABLES

FOREWORD

The current era has seen more rapid and extensive change than any time in human history. The profusion of information and the explosion of information technology is the driver, reshaping all aspects of social, political, cultural, and economic life. The effects of the information revolution are particularly profound in the realm of national security strategy. They are creating new opportunities for those who master them. The U.S. military, for instance, is exploring ways to seize information superiority during conflicts and thus gain decisive advantages over its opponents. But the information revolution also creates new security threats and vulnerabilities. No nation has made more effective use of the information revolution than the United States, but none is more dependent on information technology. To protect American security, then, military leaders and defense policymakers must understand the information revolution.

The essays in this volume are intended to contribute to such an understanding. They grew from a December 1999 conference co-sponsored by the U.S. Army War College Strategic Studies Institute and the University of Pittsburgh Matthew B. Ridgway Center for International Security Studies. The conference brought together some of the foremost members of the academic strategic studies community with representatives of the U.S. Government and U.S. military. As could be expected when examining a topic as complex as the relationship between the information revolution and national security, the presentations and discussions were far-ranging, covering such issues as the global implications of the information revolution, the need for a national information security strategy, and the role of information in U.S. military operations. While many more questions than answers emerged, the conference did suggest some vital tasks that military leaders and defense policymakers must undertake.

The Strategic Studies Institute is pleased to offer the essays as part of the vital national debate over the changing nature of security in the information age.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

BIOGRAPHICAL SKETCH OF THE EDITOR

THOMAS E. COPELAND is a Doctoral Research Fellow at the Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh. His previous publications include papers on U.S. technology transfer policy and the effect of insubordination on civil-military relations, and he has researched and written on terrorism, transnational organized crime, and the misuse of historical analogy in American foreign policy. Mr. Copeland has taught classes in international relations and public administration at Geneva College and the University of Pittsburgh. His professional experience includes service with the Office of the Chief of Naval Research, the Washington Post Company, and the Institute of World Politics. He is currently a research consultant to the Federal Government with LEXIS-NEXIS, Inc.

INTRODUCTION

At the beginning of the 21st century, Americans are content with their lot in life. Unemployment is at a 30-year low, incomes are rising, and inflation is minimal. The world seems to be free of major conflict, and—just in case it is needed—the U.S. military is the most advanced and capable in the world. These are the good old days.

However, the apparent calm hides a number of crises—the future of democratic capitalism in transition states in Europe, Asia, and Africa; ongoing internal and external debates over the proper role of America in the world; differing approaches to guaranteeing the stability of world ecosystems; the radicalization of many religious and ethno-nationalist causes; and the declining sovereignty and legitimacy of the nation-state as it struggles to respond to economic, social, and political challenges brought on by the information revolution. The Chinese symbols for "crisis" mean both danger and opportunity. This might also be true of revolutions, including the information revolution.

The information revolution is a phenomenon that defies simple characterization. Its origins lie in the not-so-distant past—the British codebreakers at Bletchley Park during World War II created "Colossus," the world's first working computer. That crude device is now outperformed by a hand-held calculator. Yet the origins of the information revolution really go further back to the inventions of the radio, the telephone, and even the telegraph. In many ways, information has been making the world a smaller place since the invention of the printing press.

But the information revolution, as it is commonly understood today, is heralded as the greatest global transition since the Industrial Revolution. It is transforming the world's most advanced nations from industrial societies to information-based societies. Citizens, firms, and governments in information societies rely

increasingly on high-speed and high-quality information to conduct their daily functions and operations. Pieces of data have become the building blocks of many modes of human interaction and activity.

The revolution is perhaps best illustrated by its results. The speed and volume of computing power have increased exponentially while costs have been dramatically reduced, bringing personal computers to half of all American homes. The revolution has created the Internet, which from its origins as a secure, nuclear-proof communications system for the military has become a true global information system, home to more than 40 million web sites with more than 800 million pages of information, accessed by more than 165 million users. The information revolution is moving beyond computer networks; even small countries like Finland have gone wireless—more than 80 telecom service providers service the two-thirds of all Finns who own mobile phones.

Opportunity.

The information revolution seems to hold a lot of promise. The U.S. economy saw tremendous growth in the 1990s, thanks to information technologies. Indeed, expectations of future economic growth fueled by the information revolution have driven the New York and NASDAQ stock exchanges to record levels. The promise of economic growth and development applies elsewhere as well; technological advances are allowing the least developed countries to leapfrog ahead in time, cost, and technology, from having no telephones to acquiring wireless telecommunications. Improved person-to-person contact and understanding—thanks to new communications technologies resulting in the creation of a "global village"—seem to offer hope that the use of military force may become far less necessary in the future.

Advances in technology and communications are also revolutionizing other areas of human interaction such as

politics and medicine. Election candidates now put significant time and money into building web sites intended to get their message out to voters, who are able to check the candidates' records, read news stories, participate in polls, make campaign donations, and register to vote, all while on-line. The state of Oregon is the first to consider allowing citizens to vote over the Internet. These same computer users are also able to access the latest research reports and advice on medical issues, network with others suffering from similar diseases or conditions, and even set up appointments on-line. New information technologies are being used for distributed medicine, allowing doctors in urban hospitals and research centers to work with medical professionals in remote areas to diagnose and treat patients. Changes in politics and medicine are matched by developments in education, entertainment, travel, and trade.

Danger.

At the same time, there is a dark side to the information revolution. The gap between the information "haves" and the information "have-nots" is getting larger; perhaps only 20 percent of the world is being influenced by globalization and the information revolution. While the United States is the world's superpower in information technology, driven primarily by the corporate sector, our dependence upon information systems creates enormous vulnerabilities. Even though President Truman warned many years ago that the critical infrastructure of the United States was vulnerable, it has taken the country a long time to begin to realize its weaknesses in the face of new threats. Those new threats are becoming more potent; advances in telecommunications enable opportunists and individuals with malign intentions—terrorists, political extremists, and criminal groups—to organize themselves effectively and to conduct new kinds of activities counter to U.S. interests.

The U.S. Army War College's Strategic Studies Institute and the Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh in December 1999 sponsored a conference on the information revolution and its impact on national security. The goal was to bring together the corporate, academic, and government communities to share lessons learned from their respective efforts to conceptualize and deal with the new threats and opportunities presented by the information revolution. Discussions at the conference suggested a number of important implications.

Technological Threats Need to Be Carefully Assessed.

The technological threats most often discussed in public—cyber-terrorists, hackers, and asymmetrical attacks—are not yet as significant as some of the dominant policy debates suggest. We have seen very little evidence of cyber-terror attacks. Although the information revolution has created vulnerabilities and expanded the scope for criminal activity, most hackers are juveniles who thus far have done little damage against relatively unimportant targets, using fairly simple tactics like denial-of-service. As a type of asymmetrical threat, terrorism in the past has benefited from technological advances like the jetliner and television. But while terrorists certainly make use of some of the latest technologies, they still rely primarily on tried-and-true tactics and weapons. Terrorists face serious challenges in acquiring the technological tools, expertise, and access needed to successfully attack critical information systems. Thus the information revolution has not yet brought new kinds of terrorist threats, but it has increased the power available to traditional terror groups and other opportunists.

Technological Opportunities Abound.

At the same time, technological solutions are being pursued to exploit opportunities made possible by the information revolution. Access to open sources through new information technologies (such as the Internet and commercial satellites) levels the playing field in intelligence collection between public and private entities. Today's intelligence consumer has many new choices, even as public institutions like the vaunted National Security Agency find themselves falling behind the latest technological developments. The Information Dominance Center at the U.S. Army Land Information Warfare Center (LIWC) takes advantage of new software programs, wireless technology, and video teleconferencing to train for and coordinate information operations in the complex physical and informational environment—such as peacekeeping—in which today's Army often operates. Private sector companies are producing new software programs that bring together databases with structured augmentation processes to create a system of virtual collaboration among intelligence analysts that is open and logical. And technological advances such as data mining and automated learning and discovery are being used by the Computer Emergency Response Team (CERT) at Carnegie Mellon University to create useful intelligence from information it has collected on nearly 23,000 computer security incidents.

Organizational Adaptation is Problematic.

The U.S. military and most other traditional institutions, including firms and governments, are ill-prepared to meet new organizational challenges posed by nonhierarchical, amorphous, networked opponents. It was argued that at the international level we see a lack of agreement among nation-states on how they should regulate things like the Internet and e-commerce, the growing empowerment of (and outright challenges from) nontraditional actors, and the inadequacy of traditional

intergovernmental forums for dealing with many global issues. Further difficulties arise at lower levels.

Rigid bureaucratic hierarchies make it extremely difficult for national governments to prevent or respond to many new kinds of transnational threats. Both strategic and temporary alliances among criminal organizations are hard to track, as are emerging terrorist organizations that are small or include only one individual. Hacker attacks, often carried out through a network of proxies or "zombie" computers, are not typical investigative subjects for law enforcement and intelligence agencies. This is not to suggest that the U.S. Government is neglecting to respond to these threats or to consider changes to organizational structures. It is probably farther ahead than any other government in understanding and responding to new threats, but it is still ill-prepared and inadequately organized to address these problems.

The U.S. military has adapted unevenly to the information revolution. It has been relatively successful in applying technology to the battlefield and in tackling new roles and missions, but it has not addressed the disadvantages of its hierarchical and centralized system when facing flexible, networked opponents in the new information environment. This failure must be corrected.

Opportunities Exist to Make Organizational Change.

The undisputed predominance that the U.S. military enjoys over military forces anywhere in the world, and the relative lack of serious national security threats facing the country at the moment, have created a unique environment wherein the military should be free to make organizational changes. Some traditional roles and missions will still need to be fulfilled in the future through traditional structures, but the military must adapt itself more fully to a decentralized, nonhierarchical system. The kind of networked, flexible organization that is called for is not a

radical idea—40 years ago Morris Janowitz suggested in *The Professional Soldier* that technology had changed warfare to such a degree that coordination, cooperation, and teamwork are more fundamental to operational success than are authoritarian leadership and structure. The military has pushed decisionmaking further and further down the chain of command, and is experimenting with new technologies that link soldiers and commanders in real time. However, the military's willingness to make needed organizational changes—required by amorphous and networked opponents of the future—will continue to be constrained by institutional inertia, service rivalries, and conservative thinking.

The business community has been somewhat quicker than the military to respond to the organizational adaptation imperative, particularly in regards to competitive intelligence. A handful of best-practice companies are carefully establishing unique organizational networks and practices that enable them to coordinate strategic and tactical competitive intelligence in ways that significantly enhance their successful adaptation to changes in the global market. Businesses are finding new ways to organize themselves to carry out risk assessment and management and to provide critical and timely services. There is much for the military to learn from the business community about flexible organization, and the private sector can learn a great deal from the military about things like the redundancy of critical systems.

New Concepts Are Needed.

Dr. John Arquilla of the Naval Postgraduate School proposed that much of the normal discussion of information strategy is located only at the technological and organizational levels, and therefore there is a need for more new thinking at the level of ideational tenets. Members of the academic, think tank, business, and military communities who participated in this conference provided

some unique and important contributions to the conceptualization of the information revolution and its impact on national security. Participants offered new and more complex characterizations of the nature of the information revolution, new definitions and understandings of theoretical and operational elements of information operations and warfare, and components of a national information security strategy. They also urged deeper consideration of the implications of information for the security dilemma, deterrence and coercion, perception and misperception, alliances, and conflict resolution.

Conclusion.

If indeed current technological threats are not as significant as they appear in the public debate, one might question whether dramatic organizational changes and ground-breaking new concepts are really necessary. However, it is clear that technology is changing and improving so rapidly that the dangers and opportunities created, exacerbated, or illuminated by the information revolution will only grow in importance. We hope that the following summaries of presentations and papers at the conference will be an important contribution to the debate over the information revolution and national security.

SESSION 1:
OPENING ADDRESS

"The Information Revolution:
Both Powerful and Neutral"

James N. Rosenau
University Professor of International Relations
The George Washington University

Much of my presentation may prove to be controversial. So let me start with an observation that I believe is incontrovertible, namely, that the information revolution, by providing technologies that have continued to greatly accelerate the collapse of time and space, has added substantially to the complexities that mark our time. Perhaps most notably, the revolution has rendered what once was remote close-at-hand; it has transformed the linear into the nonlinear, the sequential into the simultaneous; and in so doing, it has pervaded world affairs with what I like to call "distant proximities."

This label for the consequences of the information revolution is useful because it reeks of complexity, of nuance, and the need to guard against simplistic conclusions. For there can be no mistaking distant proximities for simple interrelationships, readily discernible and easily understood. Distant proximities encompass the tensions between core and periphery, between national and transnational systems, between communitarianism and cosmopolitanism, between cultures and subcultures, between states and markets, between decentralization and centralization, between universalism and particularism, between pace and space, between the global and the local—to note only the more conspicuous links between opposites that have been accelerated by the information revolution. And each of these tensions is marked by numerous variants; they take different forms in

different parts of the world, in different countries, in different markets, in different communities, in different professions, and in different cyberspaces, with the result that there is enormous diversity in the way people experience the simultaneity of the distant proximities that the information revolution has intruded upon their lives.

Put differently, distance is not measured only in miles across land and sea; it can also involve less tangible, more abstract conceptions in which distance is assessed across organizational hierarchies, event sequences, social strata, market relationships, migration patterns, and a host of other nonterritorial spaces. Thus to a large extent, distant proximities are subjective appraisals, what people feel or think is remote and what they think or feel is close-at-hand. There is no self-evident line that divides the distant from the proximate, no established criteria for differentiating between the more-remote or close-at-hand environments. In other words, nearness and farness connote scale as well as place. They are a context, a "habitat of meaning," [1] a mind set that may often correspond with spatial distance even as there are other scalar contexts which can make the close-at-hand feel very remote and the faraway seem immediately present.

The Neutrality of the Revolution.

In short, clearly we need to be sensitive to nuance if we are to begin to grasp the meaning and potentials of the information revolution. I have tried to highlight this need in the title of my presentation, in characterizing the information revolution as powerful but neutral. Surely, some would argue, anything that is powerful cannot also be neutral, that the word "revolution" suggests power, that power suggests purpose, and that, by their very nature, purposes are laden with values. Thus, such a line of reasoning would conclude, to speak of the information revolution as powerful but neutral is not to trace nuance; it is be profoundly erroneous!

No, I shall contend, it is nuance and not error if one treats the revolution in terms of the technologies that facilitate the rapid spread of information and the simultaneity of distant proximities rather than in terms of the information itself. Information is anything but neutral. It can be skewed and designed to distort; it reflects, to repeat, subject appraisals. This is not the case, however, with information technologies. They are essentially neutral because they do not in themselves tilt in the direction of any particular values—neither toward good or bad, nor left or right, nor open or closed systems. They are neutral, in the sense that their tilt is provided by people. People and their collectivities infuse values into information. For better or worse, individuals and organizations introduce information into political arenas and thereby render it good or bad. The neutrality of information technologies enables the democrat as well as the authoritarian to use information in whatever way he or she sees fit.

There is, in other words, some utility in starting with the premise that the technologies that generate and circulate information are neutral. It enables us to avoid deterministic modes of thought in which people are seen as being deprived of choice by the dictates of information technologies. Put more positively, the neutrality premise compels us to focus on human agency and how it does or does not make use of information technologies.

This is not to imply, of course, that consequences do not follow from the power of information technologies and the degree to which information technologies are available. Indeed, a prime reason why consequences follow is that the technologies have facilitated human choice. Through the Internet people can now make choices in a vast global market, in the political realm, in the types of entertainment they enjoy; and there are endless other ways in which the Internet is disaggregating the power of choice down to the individual level. Clearly, then, the availability of information technologies facilitates the exercise of human agency. Yet, to posit choices as facilitated by information

availability is not to refer to the impact of values. Information technologies are about the contexts within which decisional alternatives are considered. They set the range within which ends and means are framed, alternatives pondered, and choices made.

If we view this matter in this way, it is misleading to analyze information technologies in causal terms. That is, it is misleading if one confines the meaning of causation, as I do, to human agency. So viewed, causality accounts for the choices that are made, and why information is interpreted in one way rather than another. But information technologies are not human agents. They are simply equipment, inanimate hardware, gadgetry. Yet, as such, they are both powerful and neutral.

By treating information technologies as neutral, we cast them as background conditions and not as immediate stimuli to action—as second-order dynamics that influence, contextualize, facilitate, permit, or inhibit courses of action, but not as first-order dynamics that change, transform, foster, impose, or shape courses of action. The distinction between the two types of dynamics is important; it differentiates between the operation of structures and those of agents. Put more forcefully, the distinction prevents the analyst from mistaking second-order for first-order dynamics, for treating information technologies as an unseen hand that somehow gets people, groups, or communities to pursue goals and undertake actions without awareness of why they do what they do and, accordingly, without taking responsibility for their conduct.

A good illustration of the dangers of positing information technologies as first-order causal dynamics is evident in the adaptation of vertical business organizations in the 1980s to the horizontal flexibility required by the globalization of national economies. When diverse enterprises first seized upon the new technologies, they treated them as labor-saving devices and as means to control labor rather than as mechanisms for organizational adaptation. The

result was an aggravation of their vertical bureaucratic rigidities. It was only after they made the necessary organizational changes in order to keep abreast of their operational environments that the information technologies "extraordinarily enhanced" the success of their enterprises.[2] For all practical purposes, in other words, the restructuring of businesses away from hierarchical and toward network forms of organization preceded the considerable impact of information technologies, even as the latter then facilitated eye-catching growth on the part of the former.

In the same way, the notion of information as neutral does not ignore the convertibility of information into knowledge and, thus, into power. More accurately, information technologies facilitate the exercise of what has been called "soft power," a concept that differentiates information from the conventional dimensions of material power such as oil production, troops in uniform, military hardware, and agricultural production.[3] As clearly demonstrated during the Gulf War and the Kosovo conflict, military capabilities today highly depend on advanced information technologies; the targeting of missiles, the distribution of ideas through short-wave broadcasts, and the dropping of leaflets over cities exemplify the application of information to modern security strategies. Yet, despite the innumerable ways in which soft power can be used, it is nonetheless the case that the information technologies on which it is based are neutral. To repeat, what counts is how officials and governments generate and employ the technologies, and how publics interpret the information and knowledge that comes their way.

Needless to say, as conditions with which humans must cope, information technologies are crucial dimensions of the political scene. As they change, so do the contexts in which choices are made. As new technologies are developed, so is the range of plausible choices altered. Among other things, for example, technological innovations pose the question of how the range of choice is expanded by the availability of

information for those who are, so to speak, informationally rich and how it is narrowed for those who are informationally poor—and, indeed, how the discrepancies between the rich and the poor configure the context within which the two perceive each other and interact.

These contextual factors have been mostly neglected by political scientists who study world affairs, a neglect I seek to highlight here by addressing four main ways in which information technologies contribute to the context within which world affairs unfold. More specifically, I undertake to explore (1) how the technologies have made possible an alteration of the skills of individuals; (2) how they may be affecting the circumstances whereby the gap between the informationally rich and poor is undergoing transformation; (3) how they may be changing the conditions under which individuals and groups interact; and, (4) how they may be contributing to the evolution of new global structures.

The Skill Revolution.

While the world's present population may not be more skillful than earlier generations, there are good reasons to presume that the skills of today's person-in-the-street are different than was the case for his or her predecessor. The latter may have been more skillful in building fireplaces or cathedrals, but today's citizenries are more skillful in linking themselves to world affairs, in tracing distant events through complex sequences back into their homes and pocketbooks. These changes seem so extensive as to warrant labeling them as a "skill revolution," as a transformation that has three basic dimensions—an analytic dimension, an emotional dimension, and an imaginative dimension—all of which have been greatly facilitated by the recent advent of technologies that bring ideas, information, and pictures into the lives of people in ways that had not previously been possible. Global television, the Internet, the fax machine, fiber optic cable,

e-mail, the computer, and, most recently, a mobile phone that links one's e-mail and computer, have all enabled people to alter their skills in such a way as to adapt more effectively to the demands of an ever more complex world. [4]

Some have argued that people tend to adapt to the information age by turning away from the realm of ideas and politics. However, quite the opposite proved to be the case in a systematic survey of Americans who make extensive use of at least four of five information technologies and were classified as Connected or Superconnected to the digital world:[5]

> Despite the national lament that technology undermines literacy, Connected Americans are… more likely to spend time reading books than any other segment of the population broken down in this survey. Seventy percent of the Connected say they spend 1 to 10 hours reading a book during a typical week; another 16 percent read for 11 to 20 hours a week. Far from being distracted by the technology, Digital Citizens appear startlingly close to the Jeffersonian ideal—they are informed, outspoken, participatory, passionate about freedom, proud of their culture, and committed to the free nation in which it has evolved.[6]

Furthermore, the dynamics of change fueling the skill revolution are likely to accelerate as increasingly e-mail and computer-literate generations of children and adolescents move into adulthood. For example, it is portentous, or at least noteworthy, that a 1999 survey of young people between the ages of 13 and 17 in the United States revealed that 63 percent used a computer at home (compared to 45 percent in 1994) and 42 percent had e-mail addresses. [7] These findings suggest that the ranks of Superconnected and the Connected are likely to swell with the passage of time and the advent of new generations, thus adding to the ways in which the skill revolution is a powerful source of change in world affairs.

While the acceleration rate of the skill revolution elsewhere in the world may not match or exceed the rate in

the United States, it is important to stress that the changing skills of people everywhere matter. As indicated in the ensuing analysis, the newly acquired analytic, emotional, and imaginative skills have enabled individuals to join and participate in organizations appropriate to their interests and thereby to know when, where, and how to engage in collective action. In addition, as will be seen, the enhanced public affairs oriented skills of people have contributed to a major transformation of the global structures that govern world affairs.

Bridging the Information Gap.

There is little question that the benefits of the information revolution have been enjoyed by only a small proportion of the world's population, and that the gap between those who are rich and poor with respect to their access to information is huge. For example, while North America and Western Europe had, respectively, 43.5 and 28.3 percent of the world information technology market in 1995, the comparable figures for Latin America on the one hand and Eastern Europe, the Middle East, and Africa on the other were 2.0 and 2.6 percent. Put even more starkly, while the number of personal computers per 1,000 people in low-income and lower-middle-income economies in 1995 was 1.6 and 10.0, the comparable figures for those in newly industrialized economies (NIEs) and high-income economies were 114.8 and 199.3. Or consider Internet users per 1,000 people in 1996: for the former two types of economies the number was 0.01 and 0.7, respectively, whereas the number in the latter two types of economies was 12.9 and 111.0.[8]

Notwithstanding the importance of these huge gaps between the informationally rich and poor—gaps which provide the rich with advantages and opportunities not available to the poor—such data tell only part of the story. Most notably, they do not depict the trend line that readily allows for the assertion that not only are the informa-

tionally rich getting richer, but the informationally poor are also getting richer. The gap remains huge, but it is nonetheless the case that in a variety of ways the information revolution is also unfolding in the developing world and that, along several dimensions, the gap is narrowing and likely to continue to narrow in the years ahead. This shrinking of the gap stems from several sources. One is the enormous decline in the costs of information technologies, a decline that is brilliantly suggested by the fact that, for diverse reasons, "computing power per dollar invested has risen by a factor of 10,000 over the past 20 years" and that the "cost of voice transmission circuits has fallen by a factor of 10,000 over those same 20 years."[9] Another source of the narrowing gap involves the capacity of developing countries to "leapfrog the industrial countries by going straight from underdeveloped networks to fully digitized networks, bypassing the traditional analog technology that still forms the backbone of the system in most industrial countries."[10] Likewise, while most of the developing world has yet to be wired, its peoples can get a cellular phone and do not have to wait for the installation of fixed lines. It is noteworthy, for instance, that the

> number of cellular phones per fixed line is already as high in some low- and middle-income economies as in some industrialized countries; some developing countries with low density in both traditional telephone service and cellular phones have recently invested in cellular technology at a very fast rate . . . .The Philippines, a country with low telephone density (only 2.5 main lines per 100 people), has a higher ratio of mobile phone subscribers to main lines than Japan, the United Kingdom, the United States, or several other industrial countries with densities of more than 50 main lines per 100 people.[11]

Put differently, not long ago it was conventional to regret that development in Africa lagged because the continent was not wired. But now this lag is less portentous because communications in and to Africa are on the verge of becoming wireless. In other words,

> The wireless revolution is ending the dictatorship of place in . . . profound way[s] . . . . In the past, one of the biggest disadvantages of being born in the poor world was that you were isolated from modern communications—and hence locked into the local economy. But mobile phones are great levelers, spreading the latest tools of communication to areas were traditional phone companies could not reach. The phone ladies of Bangladesh are going around with mobile phones that would turn heads in Hollywood restaurants, and enabling their customers to plug themselves into the global economy.[12]

Of course, the rise in the trend line in developing countries is especially noticeable among their elite and educated populations. Once the Internet was introduced into Kuwait in 1992, for example, scientists, scholars, and students came on-line in increasing numbers. Within 6 years their ranks had increased to some 45,000, and many of these are younger people who hang out in any of seven Internet cafes in Kuwait City, where they escape the heat and at the same time use the Internet for chatting, dating, or otherwise reinforcing their local culture.[13] The information revolution has also reached the small villages of the Middle East: in the case of Al Karaka, Egypt, there was electricity but only one telephone in the 1970s; however, less than two decades later all its houses had electricity, and "there are also 20 telephones and more than 55 television sets. . . ."[14]

Nor are authoritarian countries able to hold back the information revolution. China, for example, has some 1.2 million Internet accounts, many of which are shared by several users, and it would appear that the number of accounts and users grows continually.[15] Likewise, Iran has an estimated 30,000 people with Internet accounts even as it also seeks to control the flow of information to and among them.[16] Whether such controls can ever be adequately established is, however, problematic.

In sum, while there are billions of persons who do not have access to the Internet, their numbers are dwindling as more and more people and organizations everywhere are

coming on-line. Put differently, and to recast a common-place metaphor, to focus on those who lack access may be to see the glass as 19/20 empty, but the trend line is in the direction of it being increasingly more than 1/20 full.

Interactive Contexts.

Perhaps the single most important consequence of the newer information technologies—and probably the consequence that justifies a continuing reference to the "information revolution"—concerns their impact on the modes through which individuals and organizations interact. Until the advent of the most recent technologies, and especially the Internet, the vast majority of these interactions were hierarchical in nature, both within organizations and across organizations engaged in similar pursuits. The former hierarchies tended to be formally established, with ranks and positions that allowed for top-down flows of authority and policy directives, whereas the across-organization hierarchies were also marked by top-down arrangements but were more in the nature of, so to speak, pecking orders—informal but widely shared rankings of prestige, influence, and power. Both the formal and informal hierarchies, however, have been supplemented by the horizontal networks that the newer technologies permit. As a consequence of the capacities for networking facilitated by the newer information technologies, the present era is marked by a veritable explosion of organizations and associations, an explosion so vast that fully tracing and documenting it is virtually impossible. At every level of community in every part of the world, new organizations are continuously being formed that are preponderantly sustained by network rather than hierarchical structures.[17]

Note that hierarchies are being supplemented and not replaced by networks. To stress that the network has become a central form of human organization is not to imply that hierarchies are headed for extinction. There will

always be a need for hierarchy, for authority to be arrayed in such a way that decisional conflicts can be resolved and policies adopted by higher authorities when consensual agreements prove unachievable in any type of organization. The present period of dynamic transformations is likely to be one in which many hierarchies are flattened, perhaps even disrupted, but such a pattern is not the equivalent of anticipating the demise of hierarchical structures. [18]

This is not to imply that horizontal networks are new forms of organization. The networks that flow from horizontal communication have long been features of human endeavor. Such interactions have always been possible, say, by steamship and letters during most of the 19th century and by wireless and telephone during the first half of the 20th century. But these earlier technologies were available only to elites. Others could not afford them. What is new today, however, is that horizontal exchanges are not only rendered virtually simultaneous by the information revolution, but their cost has been reduced to nearly nothing. As a result, horizontal networking is no longer confined to the wealthy and the powerful; instead, it is now available to any ordinary folk who have access to the Internet. Stated in terms of the new technologies,

> the growth of a vast new information infrastructure including not only the Internet, but also cable, cellular, and satellite systems, etc., [has shifted] the balance . . . from one-to-many broadcast media (e.g., traditional radio and television) to many-to-many interactive media. A huge increase in global interconnectivity is resulting from the ease of entry and access in many nations, and the growing interest of so many actors in using the new infrastructure for all manner of interactions. [19]

The networking potential that flows from the easy availability of information technologies is perhaps especially conspicuous in the United States. For not only has Internet usage in the United States more than doubled in the last 4 years, [20] but 9 percent of those in the aforementioned survey of the usage of diverse information

20

technologies were classified as either "Connected" or "Superconnected" to the course of events.[21] That this high-usage stratum of the public is capable of extensive networking can be readily deduced from a central finding of the survey:

> The Internet, it turns out, is not a breeding ground for disconnection, fragmentation, paranoia, and apathy. Digital Citizens [the Connected and the Superconnected] are not alienated, either from other people or from civic institutions. Nor are they ignorant of our system's inner workings, or indifferent to the social and political issues our society must confront. Instead, the online world encompasses many of the most informed and participatory citizens we have ever had or are likely to have.[22]

Clearly, then, the significance of virtually free access to the Internet by ever greater numbers of people can hardly be underestimated. Already it has facilitated the formation and sustenance of networks among like-minded people who in earlier, pre-Internet times could never have converged. The result has been the aforementioned organizational explosion, a vast proliferation of associations—from environmental to human rights activists, from small groups of protesters to large social movements, from specialized interest associations to elite advocacy networks, from business alliances to interagency governmental committees, and so on across all the realms of human activity wherein mutuality of interests exists. This web-like explosion of organizations has occurred in territorial space as well as cyberspace, but the opening up of the latter has served as a major stimulus to the associational proliferation in the former. Indeed, the trend toward network forms of organization,

> is so strong that, projected into the future, it augurs major transformations in how societies are organized—if not societies as a whole, then at least parts of their governments, economies, and especially their civil societies.[23]

A stunning measure of the shift from hierarchical to network organizations facilitated by the new information technologies can be seen in innovations adopted by the U.S. Marine Corps. In a recent exercise called URBAN WARRIOR, a unit of Marines comprised of all ranks from generals to privates launched an "invasion"of the California coast, with the lower ranked personnel that "hit the beaches" all carrying hand-held computers that linked them to all the others in the unit and collectively provided all concerned with a picture of how the "battle" was unfolding. In effect, they operated as a network in which rank and hierarchy were irrelevant, an arrangement that the Marine Corps plans to apply on a larger scale in the future. [24]

While the large extent to which the Internet underlies the trend toward networking in government, business, and military organizations cannot be overstated, its relevance to the world of voluntary associations and nongovernmental organizations (NGOs) is even more profound. In effect, it has facilitated a step-level change in what is called "civil society," that domain of the private sector where people have not had the resources to widen their contacts and solidify their collaborative efforts that have long been available to governments, corporations, and armies. Now it is possible to inform, coordinate, and mobilize like-minded individuals in all parts of the world who have common goals to which they are willing to devote time and energy. Equally important, NGOs and the advocacy networks they sustain are proliferating. In 1979, for example, only one independent environmental organization was active in Indonesia, whereas by 1999 the number of such organizations had risen to more than 2,000 linked to an environmental network based in Jakarta. Likewise, registered nonprofit organizations in the Philippines grew from 18,000 to 58,000 between 1989 and 1996; in Slovakia the figure went from a handful in the 1980s to more than 10,000 today; and in the United States, 70 percent of the nonprofit organizations—not counting religious groups and private foundations—filing tax returns with the Internal

Revenue Service are less than 30 years old, and a third are less than 15 years old.[25]

Clearly, then, the proliferation of advocacy networks is altering the landscape of world affairs and having substantial consequences for the course of events. Whether or not a global civil society will ever evolve, it is certainly the case that transnational networks of private citizens have become pervasive and central actors on the global stage.[26] It is not an exaggeration, in other words, to note that the global stage is becoming ever more dense as a huge variety of NGOs acquire the new technologies and thereby extend their reach and coherence. Indeed, as I will elaborate below, is a density that has altered the structures through which world politics are conducted. In sum,

> our exploration of emergent social structures across domains of human activity and experience leads to an overarching conclusion: as a historical trend, dominant functions and processes in the information age are increasingly organized around networks. Networks constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in processes of production experience, power, and culture. While the networking form of social organization has existed in other times and spaces, the new information technology paradigm provides the material basis for its pervasive expansion throughout the entire social structure.[27]

New Global Structures.

With people in both developed and developing countries becoming more skillful in relating to public affairs, and with organizations proliferating at an eye-catching and accelerating rate, it is hardly surprising that information technologies have contributed to transformations in historical global structures. Stated most succinctly, as the global arena has become ever more dense with actors and networks, the traditional world of states has been supplemented by a second world comprised of a wide variety of nongovernmental, transnational, and subnational actors,

from the multinational corporation to the ethnic minority, from the professional society to the knowledge community, from the advocacy network to the humanitarian organization, from the drug cartel to the terrorist group, from the local government to the regional association, and so on, across a vast range of collective endeavors. Despite its diversity and cross-purposes, this "multi-centric" world is seen as having a modicum of coherence such that it coexists with the state-centric world. In effect, global structures have undergone a bifurcation in which the two worlds are conceived as sometimes cooperating and often conflicting but at all times interacting.

Needless to say, this interaction between the worlds has been greatly facilitated by the information technologies, thus collapsing time, deterritorializing space, and rendering traditional boundaries increasingly obsolete. Indeed, the more the technologies advance, the more they facilitate the opening up of both governments and nongovernmental organizations to the influence of their members, to bottom-up and horizontal processes that have greatly complicated the tasks of governance on a global scale.[28] For national governments these changes—and the vast proliferation of interconnections they have fostered—have confounded the traditional practices of diplomacy and the long-standing premises of national security, thereby necessitating a rethinking of how to pursue goals in relation to the demands of both other states and the innumerable collectivities in the multi-centric world.[29] For the latter the increased connectivity has provided opportunities as well as challenges as they seek to network and build coalitions with like-minded actors and contest the coalitions that stand in the way of their goals.

In short, the bifurcation of global structures has led to a vast decentralization of authority in which global governance becomes less state-centric and more the sum of crazy-quilt patterns among unalike, dispersed, overlapping, and contradictory collectivities seeking to

maintain their coherence and advance their goals. More than that, the interconnection of these patterns

> is likely to deepen and become the defining characteristic of the 21st century. The information revolution is what makes this possible; it provides the capability and opportunity to circuitize the globe in ways and to degrees that have never been seen before. This is likely to be a messy, complicated process, rife with ambivalent, contradictory, and paradoxical effects.[30]

The information revolution may be neutral in the sense that it permits the application of diverse and competing values, but clearly it underlies extensive consequences in every realm of global affairs. And since there is no end in sight to the development of new information technologies, clearly the full ramifications of their impact are yet to be experienced as people and their collectivities seek to keep abreast of the complexities of the dynamic transformations that are altering the human condition.

DISCUSSION

Discussion focused on three subjects: the idea that technology is neutral; the relationship between the two worlds of global politics (state-centric vs. multi-centric); and the implications of information quality for interpretation and learning.

Dr. Rosenau: There are consequences of technology, they are just second order—and not necessarily all good. As to its neutrality, we should differentiate between human consequences as against the gadgetry and technology that lead to those consequences.

In Seattle at the meeting of the World Trade Organization, we saw the two worlds of world politics converging in the streets. My notion of the 21st century is that in the political world we will continue to see the disaggregation of authority, which will move upwards to supranational organizations like the European Union,

sidewards to social movements, and downward to subnational groups. A lot of the shifts in authority will be to the detriment of the nation-state. I would never say that states are on their way out or off the stage, but they are not as competent as they used to be. They cannot control the flow of information, money, pollution, crime, drugs, or people across their boundaries. It seems that the world is going to get messier.

Regarding the quality of information, with my students I say that their task is to develop knowledge, to be self-conscious and aware of the context frames they use when looking at the world. The information revolution makes people more possessive of working knowledge. Let me give an example. Scientists took a sample of chess players and nonchess players, and asked each group to recreate a chess board after a chart was flashed for 5 seconds. They divided the chess players into two groups, one which saw pieces in an ordered pattern, and the other which saw a random alignment of pieces. Those facing the game-like scenario had no problem reconstructing it; those faced with a random board had no idea what to do. The notion of the skill revolution (as part of the information revolution) is that while all of the information sometimes gets misinterpreted or ignored, the net consequence of the flow is greater imagination and capacity for judgment, so that people enlarge their working knowledge. Some would say that the revolution is not happening, that government continues unabated; but the information revolution, despite all its faults and the problem of being inundated with information, has led to dramatic changes and increases in peoples' skills.

SESSION 1 - ENDNOTES

1. Ulf Hannerz, *Transnational Connections: Culture, People, Places,* London: Routledge, 1966, pp. 22-23.

2. Manuel Castells, *The Information Age: The Rise of the Network Society*, Vol. I, Oxford: Blackwell Publishers, 1996, p. 169.

3. See, for example, Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs*, Vol. 75, March/April 1996, pp. 20-36; Richard Rosencrance, "The Rise of the Virtual State," *Foreign Affairs*, Vol. 75, Fall 1996, pp. 45-61; Ryan Henry and C. Edward Peartree, eds., *The Information Revolution and International Security*, Washington, DC: CSIS Press, 1998; and Martin C. Libicki, "Information War, Information Peace," *Journal of International Affairs*, Vol. 51, Spring 1998, pp. 411-428.

4. An extensive discussion of the skill revolution can be found in James N. Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity*, Princeton: Princeton University Press, 1990, Chap. 13; James N. Rosenau, *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*, Cambridge: Cambridge University Press, 1997, Chaps. 14-15; and James N. Rosenau, "The Skill Revolution and Restless Publics in Globalized Space," in Michel Giraud, ed., *Individualism and World Politics*, New York: St. Martin's Press, 1999, pp. 44-68. Newly generated empirical materials that affirm the hypothesis that skills in the realm of public affairs have advanced in recent decades are provided in James N. Rosenau and W. Michael Fagen, "Increasingly Skillful Citizens: A New Dynamism in World Politics?" *International Studies Quarterly*, Vol. 41, December 1997, pp. 655-686.

5. The Superconnected were those in the survey of 1,444 randomly selected Americans who exchange e-mail at least three days a week and use a laptop, a cell phone, a beeper, and a home computer, whereas the Connected were those who exchange e-mail three days a week and use three of the four other technologies. Jon Katz, "The Digital Citizen," *Wired*, December 1997, p. 71.

6. Katz, p. 72.

7. Carey Goldberg and Marjorie Connelly, "Fear and Violence Have Declined Among Teen-Agers, Poll Shows," *New York Times*, October 20, 1999, p. A1.

8. World Development Report, *Knowledge for Development, 1998/99*, New York: Oxford University Press for the World Bank, 1999, p. 63.

9. *Ibid.*, p. 57.

10. *Ibid.*

11. *Ibid.*

12. "A Survey of Telecommunications: The World in Your Pocket," *The Economist*, Vol. 353, October 9, 1999, p. 36.

13. Deborah L. Wheeler, "Global Culture or Culture Clash: New Information Technologies in the Islamic World—A View from Kuwait," *Communications Research*, Vol. 25, August 1998, pp. 359-376.

14. William E. Schmidt, "The Villages of Egypt Relish the Fruits of Peace," *New York Times*, September 24, 1993, p. A4.

15. Erik Eckholm, "A Trial Will Test China's Grip on the Internet," *New York Times*, November 16, 1998, p. A8.

16. Neil MacFarquhar, "With Mixed Feelings, Iran Tiptoes to the Internet," *New York Times*, October 8, 1996, p. A4.

17. Lester M. Salamon, "The Global Associational Revolution: The Rise of the Third Sector on the World Scene," *Foreign Affairs*, July/August 1994, pp. 109-122.

18. For an analysis that stresses the limits of networks and the necessity of hierarchies, see Francis Fukuyama, "Social Networks and Digital Networks," a paper presented at the Workshop on the Future of the Internet, Palo Alto, May 6, 1996.

19. David Ronfeldt and John Arquilla, "What If There Is a Revolution in Diplomatic Affairs?" paper presented at the Annual Meeting of the International Studies Association, Washington, DC, February 17, 1999, p. 4.

20. Rajiv Chandrasekaran, "Politics Finding a Home on the 'Net,'" *The Washington Post*, November 22, 1996, p. A4.

21. Katz, p. 71.

22. *Ibid.*

23. David Ronfeldt, "Tribes, Institutions, Markets, Networks: A Framework About Societal Evolution," Santa Monica, CA: RAND, 1996, p. 1. For a skeptical view of the potential of networks, and especially the Internet, see Deborah C. Sawyer, "The Pied Piper Goes Electronic," *The Futurist*, February 1999, pp. 42-46.

24. Joel Garreau, "Point Men for a Revolution: Can the Marines Survive a Shift from Hierarchies to Networks?" *The Washington Post*, March 6, 1999, p. 1.

25. David Bornstein, "A Force Now in the World, Citizens Flex Social Muscle," *New York Times*, July 10, 1999, p. B7.

26. See, for example, Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics*, Ithaca: Cornell University Press, 1998.

27. Castells, p. 469.

28. Michael Peter Smith and Luis Eduardo Guarnizo, eds., *Transnationalism from Below*, New Brunsick, NJ: Transaction Publishers, 1998.

29. See Richard H. Solomon, Walter B. Wriston, and George P. Schultz, Keynote Addresses from the Virtual Diplomacy Conference, Washington, DC: U.S. Institute of Peace, 1997; also, by same authors, *Reinventing Diplomacy in the Information Age*, Washington, DC: Center for Strategic & International Affairs, 1998.

30. Ronfeldt and Arquilla, pp. 19-20.

SESSION 2:
INFORMATION AND DECISIONMAKING

The second session assessed the impact of the information revolution on intelligence and decisionmaking, looking at issues related to "data overload" or "information smog," as well as the abundance of open sources that challenge traditional government monopolies of intelligence. In addition, it considered how information technology might be used to enhance intelligence analysis.

"Exploiting Open Source Information— Abundance, Value, and Intelligence Community Credibility"

Dr. Davis Bobrow
University of Pittsburgh

We begin with two intelligence community equations. First, the quality of an intelligence product is equal to collection x exploitation/processing x analysis. Second, intelligent policy is equal to the quality of the intelligence product x awareness of U.S. behavior and options x policy user/consumer discipline. What this means is that one could have a great intelligence product, zero uncertainty, perfect timing, and still have a disaster. If one understands the idea of "value at the margins," it is not obviously or necessarily the case that upgrading the first term of either equation (collection and quality product, respectively) offers the most leverage from an increment of improvement. We leave it up to the reader to decide which of the six yields the fastest improvement for the contemporary United States.

Our premise is that the information revolution makes less credible the notion that official intelligence communities have a monopoly (if they ever did) on any of the elements of a quality intelligence product. Therefore, they

31

should understand that they are in an extraordinarily competitive environment, with a complex group of American and foreign processors, collectors, analysts, and consumers. Whether or not this is accepted in the intelligence community, anyone interested in being informed will understand that they have a menu of choice far greater than they have ever had before.

The Problem Context.

Even an oversimplified version of the global information environment will reveal millions of people producing "stuff," some of which may be considered "information." There are now many more producers and sources, a real proliferation of suppliers. The problem is sifting through all the available information to find the important nuggets. Take government providers and others, add commercial overhead imagery and some 8,000 online commercial databases, etc., and one finds simply a "supply glut" of information.

In the post-Cold War period, there is a demand boom for intelligence products. There are more issues, more government consumers, more cross-sectoral customers (public, private, and nonprofit), more coalitions, and more outside actors, all stimulated by the notion that in the new information environment, information carries a premium for effective behavior.

At the same time, the intelligence community faces a resource problem, and the ratios are getting worse. There are more requirements and more potential sources; one might call this "more hay to the needle." But there is less manpower available—there are fewer searchers for the needles. The number of CIA analysts basically has been flat since the mid-1970s; in fact, there have been radical workforce reductions across U.S. intelligence agencies associated with the Department of Defense over the last decade and a half. What this means is fewer specialists and more generalists who issue-hop, depending on policy

priorities. In the context of information overload, there is an increasing tendency to follow the maxim of Sandy Berger: "I worry about today's problems today and tomorrow's problems tomorrow." This means that intelligence, no matter how good, will be of little help because it will come too late.

Open Source Generalities.

In this context, we turn to considering open sources. Experts for many years have suggested that exotic sources are less important than open sources. George Kennan stated that "the need by our government for secret intelligence about affairs elsewhere in the world has been vastly overrated." He also noted:

> I would say that something upward of 95 percent of what we need to know could be very well obtained by the careful and competent study of perfectly legitimate sources of information open and available to us in the rich library and archival holdings of this country. Much of the remainder, if it could not be found here (and there is very little that could not) could easily be non-secretively elicited from similar sources abroad.

Allen Dulles, another man who knew about secrecy, said:

> Because of its glamour and mystery, overemphasis is generally placed on what is called secret intelligence, namely the intelligence that is obtained by secret means and secret agents . . . . In time of peace the bulk of intelligence can be obtained through overt channels, through our diplomatic and consular missions, and our military, naval, and air attaches in the normal and proper course of their work. It can also be obtained through the world press, the radio, and through the many thousands of Americans, business and professional men, and American residents of foreign countries, who are naturally and normally brought in touch with what is going on in those countries.

Both of these experts stressed open source information well before the information revolution. The obvious questions are: What has happened to prove they are wrong, or what

33

has happened to make us realize they are right? The obvious answers are "not much" and "a great deal."

The Central Intelligence Agency (CIA) Directorate of Intelligence review listed the contribution of open sources at 35 percent—much higher than either human intelligence or signals intelligence. The community's open source program office found that over 80 percent of the information gaps production managers had identified could have been filled by open sources. So the range is probably somewhere between 35 and 80 percent. Open sources also have the advantage of the "third party rule," which is that one can disseminate information to people who do not have a lot of clearances. If one believes in the multi-actor world as outlined by James Rosenau, the need for dissemination is crucial for information to realize its full potential value.

The Aspin-Brown Commission, which began early in the Clinton Administration, talked about creating an open source gateway to the intelligence community, in effect screening intelligence requirements to sort out information that had to be produced from secret vs. outside sources. In 1997, despite all these reasons, about 1 percent of U.S. intelligence community funding went to open sources. The ambitious Aspin-Brown recommendations have never been implemented, and perhaps the community is even sliding backwards. Recently, another wave of reports following alleged intelligence failures triggered the post-mortems calling for more use of outside experts and outside information to control for internal bias.

Why the disparity between the alleged value of open sources and funding? There are several charges often made against open sources.

• First, open sources and unclassified analysts, if used too much, let the enemy know about sources and methods. But we should fall back on Edward Teller's rule that if everything is open, it is hard for others to find the needle in our haystack.

• Second, there is a lack of analytic discipline in open sources. However, most American collection agencies and foreign counterparts go around pitching their latest "hot take" which has never been subjected to collective discipline or competitive analysis.

• Third, it is easier to provide misinformation inserted into open sources. But this is not true if one is aware of how easy it is, and where no one has a vested interest in defending the purity of the source or collection technology.

• Fourth, nonintelligence community analysts are more gullible and take a more benign view of human nature. However, classic historians do not seem to have that flaw, and most students of American politics are somewhat cynical.

• Fifth, it is argued that we need "hard facts" for military operations, so-called "expeditionary facts." But in the past, American military endeavors have often been hindered by the lack of open source information which could have provided missing facts.

An Ambiguous Case: The Chinese Embassy in Belgrade.

The U.S. cruise missile attack in March 1999 that damaged the Chinese embassy in Belgrade has been criticized as an intelligence failure which could have been prevented through more reliance on open sources. We decided to check this out, but found that obvious open sources—both on the Internet and even traditional tourist guides like *Fodor's*—provide no address for the Chinese embassy. But a little more digging reveals two official Serb government web sites which have listings of where the embassy is. So if there is an address, one only needs a map to get expeditionary facts. We went to Hillman Library here at the University of Pittsburgh to find a map which indeed shows exactly where the current Chinese embassy is in Belgrade.

Does that make the case for open sources? Unfortunately, it is not that easy. An official U.S. Government map (made public by a disgruntled public employee) shows the embassy clearly. So maybe we did know exactly where the embassy was. Later articles indicated that NATO officers involved in operations knew where it was, and that it was taken off the "no-hit" list because the Chinese were assisting the Serbs with military intelligence.

Looking at almost any individual case to argue about the value of open sources and uncleared analysts, it is easy to find ambiguity. Yet there is often valuable open source information even on expeditionary facts. In the case of the Chinese embassy in Belgrade, however, there is no reason to conclude that the policy choice—bombing—would have been different even if open sources had been consulted.

Given the current information environment, we should remember that the open source debate has been going on for 50 years. The Intelligence community faces challenges and opportunities that are more than mere budgetary problems, yet there is a chronic resistance to open sources and open analysts. It is past time to move beyond the unrewarding anecdotal debate between optimists and pessimists, and run a systematic set of tests to see who does better at producing one or another type of intelligence product.

"Crisis Avoidance and Mitigation: The Genoa Approach"

Scott Fisher
PSR/Meridian

One of the things we face in the intelligence world after the information revolution is delivering products in time. In the conflict between depth of analysis and length of time, what usually ends up suffering is depth of analysis. We need products in less time than before, and we only handle what is happening today.

The information revolution has made situation management much more difficult. The goal should be to develop a mitigating strategy before the crisis requires intervention, so that the use of military force is an option of choice, not a necessity. But there are often problems in getting decisionmakers' attention, and there is usually a disconnect between them and analysts. The Genoa approach—a mixture of information technology and collaborative software—tries to bring the parties back together to increase both depth and speed of analysis.

There are three key concepts in the Genoa approach: transparency, persistence of information, and a cohesive environment. With transparency, whatever the intelligence analysts produce can be seen by decisionmakers, who can take the product and recreate or get inside the process that created it. Persistence is also important. We need a corporate memory not just to save information, but to be able to manipulate it later, that is, to be able to query against databases of past experience. The cohesive environment of Genoa is designed to make sure that all of the tools work together to provide transparency and persistence.

Genoa utilizes a powerful, web-based environment that facilitates out-of-the-box thinking. The idea is to avoid using the standard train of thought. To use a historical example, although the United States considered Pearl Harbor as a possible site of conflict, we determined that we would fight Japan in the Philippines first, and we were obviously wrong. The goal is to expand the possibilities of imaginative thinking, to look at more and different arguments, and to arrive at more clear and concise policy options, enabled by the technology being developed for Genoa.

Genoa takes a three-pronged approach to time. We utilize corporate memory in the form of databases to develop current crisis paths, which are in turn leveraged to develop scenario-based planning about the future. The notion of corporate memory may be controversial because it allows

one to go back later and analyze who made the most successful analysis. However, it is crucial to preserve information to use in the future. The idea of crisis paths is that instead of considering only the most likely scenario, Genoa allows analysts and policymakers to consider other plausible but high-impact and high-uncertainty options.

A key step in this process is the involvement of policymakers. For example, a policymaker may have found something that focuses his attention, like a newspaper article about Aum Shinrikyo. With this system, the analyst develops various scenarios, and the policymaker can consider a number of options. But the policymaker must be involved for the process to be valid.

The logic behind crisis paths is structured argumentation. Genoa provides a set of templates to use, which can handle either a top-down hypothesis (take a model and collect intelligence to test it) or a bottom-up, data-driven model (the information is present, but its applicability must be determined). An analyst can build a transparent argument for why something is a threat, using a structured hierarchy of questions that can be edited to suit the demands of the particular case. The system thus makes a transparent and direct connection between the evidence and the rationale for the argument, enabling analysts and policymakers to argue not about conclusions but about the details, the intelligence data.

The next step is collaboration between analysts. Genoa creates what are called thematic argument groups (TAGs), places for virtual collaboration. Little time is required to set up a TAG, and any member of a TAG can participate in the discussion through the software tools. The goal is to make it preferable to collaborate virtually rather than over the phone. In this environment, there is a push and pull of information.

In the search for information, the question of signals versus noise is important. However, Genoa offers the ability to search for more focused information, using thematic

navigation and semantic regions to find subdocument level stories. Any analyst or decisionmaker can take the new information and go back and modify the argument, lessening the danger of rigid argumentation.

The final step is summarization and publication of information, which can take place through typical printed publication or computer-based visualization and data storage.

In sum, the Genoa approach provides transparency in analysis and persistence of information in a cohesive environment which aides decisionmakers and analysts in handling the speed and volume of information in the new global information environment.

"Intelligence Analysis and Information Overload"

Lisa Krizan
Defense Intelligence Agency

Being a parent has really colored my outlook on life. It reduces life to the basics, like eating, sleeping, working, and playing. This way of thinking spills over into work life. After beginning with some comments about intelligence sharing between national intelligence and business intelligence, I will share some thoughts on dealing with information overload by getting back to basics in terms of intelligence requirements and analysis.

Intelligence Sharing in a New Light.

Although "information sharing" traditionally has been a government-to-government transaction, the environment is now receptive to government-private sector interaction. There has been a widespread trend toward incorporating government intelligence methodology into commerce and education. As economic competition accelerates around the world, private businesses are initiating their own "business

intelligence" (BI) or "competitive intelligence" services to advise their decisionmakers. Educators in business and academia are following suit, inserting BI concepts into professional training and college curricula.

Whereas businesses in the past have concentrated on knowing the market and making the best product, they are shifting their focus to include knowing, and staying ahead of, competitors. This emphasis on competitiveness requires the sophisticated production and use of carefully analyzed information tailored to specific users; in other words, intelligence. But the use of intelligence as a strategic planning tool, common in government, is a skill that few companies have perfected.[1]

Although BI practitioners refer to the national security model of intelligence, they do not seek to conduct secret intelligence operations, which are limited by law to government authorities. Large corporations are creating their own intelligence units, and a few are successful at performing analysis in support of strategic decisionmaking. The majority of businesses having some familiarity with BI are not able to conduct rigorous research and analysis for value-added reporting, so they are hiring BI contractors, "out-sourcing" this function, or establishing their own intelligence units. The implication of this trend is that BI professionals should be skilled in both intelligence and in a business discipline of value to the company.[2]

Demand in the private sector for intelligence skills can be met through the application of validated intelligence practices of the intelligence community. Conversely, the business perspective on intelligence can be highly useful to government intelligence professionals. As a BI practitioner explains, every activity in the intelligence process must be related to a requirement, otherwise it is irrelevant.[3] Government personnel would benefit from this practical reminder in every training course and every work center. In the private sector, straying from this principle means wasting money and losing a competitive edge. The

consequences of inefficient national intelligence can be costly on an even larger scale, particularly in an environment of information proliferation.

Whereas government practitioners are the acknowledged subject-matter experts in intelligence methodology, the private sector offers a wealth of expertise in particular areas such as business management, technology, the global marketplace, and skills training. Each has valuable knowledge to share with the other, and experience gaps to fill. On the basis of these unique needs and capabilities, the pubic and private sectors can forge a new partnership in understanding their common responsibilities.

Defining the Intelligence Problem.

Customer demands or "needs," particularly if they are complex and time-sensitive, require interpretation or analysis by the intelligence service before being expressed as intelligence requirements that drive the production process.[4] This dialogue between intelligence producer and customer may begin with a simple set of questions (Who, What, When, Where, Why, and How), and, if appropriate, may then progress to a more sophisticated analysis of the intelligence problem being addressed. The Taxonomy of Problem Types shown in Table 1 illustrates the factors that customers and producers may take into account in articulating the nature of the intelligence problem and selecting a strategy for resolving it.

This model enables decisionmakers and analysts to assess their needs and capabilities in relation to a particular intelligence scenario. This ability to establish a baseline and set in motion a collection and production strategy is crucial to conducting a successful intelligence effort. Employing a structured approach as outlined above can help producers and customers avoid inefficiencies of time and effort—particularly in a situation of information overload—and take the first step toward generating clear

41

intelligence requirements by defining both the intelligence problem and the components requisite for its solution.

Characteristics	Problem Types				
	Simplistic	Deterministic	Moderately Random	Severely Random	Indeterminate
What is the question?	Obtain information	How much? How Many?	Identify and rank all outcomes	Identify outcomes in unbounded situation	Predict future events/ situations
Role of facts	Highest	High	Moderate	Low	Lowest
Role of judgment	Lowest	Low	Moderate	High	Highest
Analytical task	Find information	Find/create formula	Generate all outcomes	Define potential outcomes	Define futures factors
Analytical method	Search sources	Match data to formula	Decision theory; utility analysis	Role playing and gaming	Analyze models and scenarios
Analytical instrument	Matching	Mathematical formula	Influence diagram utility, probability	Subjective evaluation of outcomes	Use of experts
Analytic output	Fact	Specific value or number	Weighted alternative outcomes	Plausible outcomes	Elaboration on expected future
Probability of error	Lowest	Very low	Dependent on data quality	High to very high	Highest
Follow-up task	None	None	Monitor for change	Repeated testing to determine true state	Exhaustive learning

Table 1. Taxonomy of Problem Types.

Evaluating and Selecting Evidence.

To prepare collected information for further use, one must evaluate its relevance and value to the specific problem at hand. When the sources and volume of information are proliferating, intelligence analysts face an enormous challenge in determining the source and applicability of collected information to the intelligence issue. Several aspects to consider in evaluating the relevance of information sources are reliability, proximity, appropriateness, plausibility, and support.

Reliability of a source is determined through an evaluation of its past performance; if the source proved accurate in the past, then a reasonable estimate of its likely accuracy in a given case can be made. However, if the source is completely untested, then evaluation of the information must be done solely on its own merits, independent of its origin.[5] *Proximity* refers to the source's closeness to the information. The direct observer or participant in an event

may gather and present evidence directly, but in the absence of such firsthand information, the analyst must rely on sources with varying degrees of proximity to the situation. *Appropriateness* of the source rests upon whether the source speaks from a position of authority on the specific issue in question. *Plausibility*, or expectability, is the degree to which, based on prior knowledge, the analyst would expect the information to be true. Finally, *support* is the degree of confirmation for the information from other sources or pieces of information.

All these factors of source and content contribute to an initial assessment of the value of a particular piece of information to the intelligence production process. Those pieces that are judged to be reliable and useful may then undergo further scrutiny in light of customer needs, while items of questionable value may be rejected or set aside for further processing and comparison with other information.

Conclusion.

The intention here has not been to be overly simplistic, but to focus on how, in a situation of information overload, focusing on basics may be beneficial. In particular, the use of sophisticated models of intelligence problem definition, and careful selection and evaluation of evidence, may help the analyst sift through the growing mountains of information to find the real gems.

Discussion.

The panelists were asked to comment on two related issues: the political nature of intelligence gathering and processing, and the notion of a market analogy for intelligence consumers and producers.

The Political Nature of the Intelligence Process.

Dr. Krizan: The intelligence community, in order to maintain continuity amidst political changes, must array

its assets against problem sets and use established procedures designed to be responsive to the customer. When the customer changes or its needs change, the intelligence community may be organized enough but not flexible enough to respond quickly to those changes.

Dr. Bobrow: The problem of politics and hierarchy will not go away, but the way to remedy it without creating excessive autonomy among government intelligence agencies is through the market. The intelligence market needs intensive competition and low barriers to entry, multiple sellers and buyers, high transparency, and mobility. The open source world makes it more likely that we will face that situation. For example, large firms have some influence on American foreign policy in terms of shaping the agenda, issues, options, and so on; those firms do not rely just on the official intelligence community, in fact they often try to shape what the community digests. So create the market, and let's go with it rather than resist it. Otherwise the problem will not go away. The problem is compounded by the fact that the customer often is in the community—not outside it. The Genoa and Krizan approaches are not inherently aimed at a hierarchical system; it would be better if everyone had the technologies such as Genoa in order to conduct better intelligence analysis. That is the only way we can get close to removing the inherent distortions in the market.

Dr. Fisher: The Genoa approach faces a tough political battle—people do not want persistence and transparency in the intelligence community because it will become clear who is doing the best analysis. Clearly we understand there are hurdles to overcome, but we are just trying to develop the technology, and hope the politics will follow.

The Intelligence Customer and the Market Analogy.

Dr. Bobrow: We are skirting between the horns of a dilemma—of the analyst being too close or too far from the intelligence customer. Let me suggest three things. First, in

the market analogy, the consumers are not just the government, but responsible agents such as the public interest, the nation, an ethnic group, and so on. The more transparent the market, the more consumers are held accountable for having gone out to get the "taste good" answer rather than a more informative one. Second, will we create a utopian, perfect market? Not entirely, but in this new information environment there is a better chance of coming closer to it. Third, people already go shopping for the answer that will suit, and there are tremendous incentives to put forward "good" answers. To change these human tendencies, we would have to change the subsequent costs and benefits, handled by getting multiple suppliers and consumers and a greater chance of later evaluation.

With a market there is a better chance of the analyst not being far out from everyone. Public agents may be interested in having a different "take" about the future or the present, so there is a possibility of greater diversity. Supply diversity is happening anyway, despite foot-dragging by the intelligence community. Take the example of the business world, where firms looking at potential investment sites assess the target from lots of angles. Obviously the U.S. Government is taking different angles on the same subject, environmentalists would take a third angle, and so on. But the notion that a closed community can reform itself enough to level the playing field is utopian. It can try, but those activities will erode.

SESSION 2 - ENDNOTES

1. Richard D'Aveni, "Hypercompetition," briefing to SCIP Conference, Alexandria, VA, March 28, 1996.

2. Jan Herring, "Strides in Institutionalizing BI in Businesses," briefing to SCIP Conference, Alexandria, VA, March 28, 1996.

3. David Harkleroad, "Actionable Competitive Intelligence," briefing to SCIP Conference, Alexandria, VA, March 28, 1996.

4. Douglas H. Dearth, "National Intelligence: Profession and Process," in Douglas H. Dearth and R. Thomas Goodden, eds., *Strategic Intelligence: Theory and Application*, Washington, DC: Joint Military Intelligence Training Center, 1995, p. 18.

5. Adapted from Gary Harris, "Evaluating Intelligence Evidence," in Ronald D. Garst, ed., *A Handbook of Intelligence Analysis*, Washington, DC: Defense Intelligence College, 1989, pp. 34-35.

SESSION 3:
INFORMATION AND INSTITUTIONAL ADAPTATION

The goal of the third session was to consider what lessons the private sector and the armed forces might learn from one another in responding to the challenges and opportunities of the information revolution.

"Lessons from Business Intelligence: Achieving Strategic and Tactical Coordination in Organizations"

Dr. Cynthia Miree
Oakland University
and
Dr. John E. Prescott
Joseph M. Katz Graduate School of Business
University of Pittsburgh

The issues and instruments of the military and national security intelligence communities are similar to those in business intelligence. There are four things that we believe are important to compare and contrast between these communities. First, there is cost—business organizations have more budgetary constraints and limitations than does intelligence. Second are outcomes. Failures of military or national security intelligence have far more significant repercussions than do failures of business intelligence. Third, there are ethical issues. Business intelligence is much more concerned about ethics, and many investigations have been toned down or stopped altogether for ethical reasons. Fourth is the sustainability of the competitive intelligence department itself. Whereas in the national security community one may worry about getting the decision-maker's attention, on the business side you have to be worried about whether the boss will shut down

the whole operation. So what do business organizations do to mitigate or avoid some of these problems in competitive intelligence?

This report is based on our study of competitive intelligence by Best-Practice Companies (BPCs). The study was sponsored by 17 corporations, and we did case studies of five BPCs. Most companies that engage in competitive intelligence have either a strategic focus or a tactical focus, but not both. The overall purpose of this study was to examine how the competitive intelligence function could assist the sales organization in being more effective, and the specific research goal was to determine how BPCs coordinate the strategic and tactical intelligence process in the sales function.

We looked at the sales function because it has an interesting hierarchy of sales representatives out in the field passing information back to the high-level managers, who are making strategic decisions about product lines and marketing, the whole process being mediated by mid-level managers. It is interesting to note that this hierarchy actually bears a resemblance to the organization of intelligence agencies.

There were four main areas of focus in our study: (1) organizational structure—how the competitive intelligence departments are actually structured; (2) what kind of competitive intelligence knowledge they are creating in their sales and marketing functions; (3) how they coordinate strategic and tactical competitive intelligence; and (4) how they measure the results of the competitive intelligence against the demands of their "consumers."

Our first key finding was that companies that both (1) establish coordination of strategic and tactical intelligence as a priority, and (2) are able to articulate the formal and informal processes that are used to achieve coordination, are more likely to achieve coordination than those who do not establish coordination as a priority and are not able to articulate their formal and informal coordination processes.

48

Our second key finding was that in most BPCs, the coordination of strategic and tactical intelligence in the sales function is facilitated through the sophisticated use of coordinating mechanisms we have labeled the TAP-IN process: Teams and Technology, competitive intelligence human resource Allocation, the role of competitive intelligence in the strategic Planning process, the Interaction between competitive intelligence and top management, and the use of human Networks.

There are several fundamental issues in TAP-IN:

• Consistency across TAP-IN mechanisms;

• Hierarchy of importance for TAP-IN mechanisms;

• Level of sophistication for each TAP-IN mechanism;

• Effect of hierarchy on presence and use of TAP-IN mechanisms.

The first mechanism of TAP-IN is Teams and Technology. Within BPCs, organizational processes are enabled and managed by teams and the use of information technology. The competitive intelligence groups are represented on most important strategic and tactical teams within the organization. Either technology is used to bring individuals together geographically, or used as depositories for information. BPCs tend to use technology for one or the other, but not both equally—usually a 80/20 split.

Second is the Allocation mechanism. Competitive intelligence human resources are explicitly designated for assignment to strategic and tactical activities through job design. That is, human resources are carefully allocated to where they are most needed. One example we studied was the MetLife company, where one competitive intelligence expert is strategic and the other two are tactical, making sure their sales representatives can win bids.

Planning is the third TAP-IN mechanism. Competitive intelligence input is embedded in the strategic planning process. We looked at several organizational examples of

this. At Boehringer, strategic planners solicit competitive intelligence inputs from business intelligence and from their sales force, while at MetLife they use a competitive intelligence database and competitive landscapes in strategic planning. At Dow Chemical, competitive intelligence input is represented both directly and indirectly in the strategic planning process and Dow's value-based planning process, which evaluates the contribution of strategies to stock market value.

Interaction, in the form of dialogue, is the primary and preferred method of communication in BPCs; they are much less interested in putting out certain types of intelligence products. For example, Amoco is trying to implement common mental models across decisionmaking and competitive intelligence. At their strategic planning meetings, they do not bring in competitive intelligence products the first day, but debate issues and what they mean in a face-to-face forum. Both MetLife and Boehringer emphasize frequent face-to-face conversations with internal customers, particularly strategic internal customers.

The fifth TAP-IN mechanism is Networking. In BPCs the establishment and use of internal and external networks are expected and reinforced. The companies that do competitive intelligence best are able to coordinate their internal and external human intelligence networks. Some companies, like Boehringer, evaluate and select competitive intelligence personnel based on an employee's networking skills and the possession of viable internal and external networks. Dow is establishing and leveraging networks over time to enable speedy access to information in a global company.

In conclusion, Best-Practice Companies, which do not have the budgetary or human resources of the government intelligence community, are creating unique organizational methods and forms to bring together strategic and tactical intelligence in cost-effective ways—the TAP-IN process—

that improve the companies' competitiveness and capabilities in the rapidly changing and information-rich global market.

"Multilateral Institutions in the Global Information Economy"

Dr. William Drake
Director
Project on the Information Revolution
and World Politics
Carnegie Endowment for International Peace

I would like to begin with some comments on the information revolution (IR) and the new interest in its impact on international relations. I will add some comments on multilateral institutions and the global information economy, and talk about some of the reasons why they have had a particularly difficult time adapting to the IR. I think that this has importance and relevance beyond the realm of communications and information policy, because the nature of the global information infrastructure and how it is managed impact the kind of IR we have on a worldwide scale. Changes in the governance of information and communication at the multilateral level have had a major impact on the structure of the global economy and the worldwide shift toward the IR. I will conclude with several points on the IR and how it impacts international cooperation and global governance.

The IR and World Politics.

There has been a striking lack of interest by political scientists in the IR and its impact on national security, although this is finally beginning to change. James Rosenau is one of the few who have actually studied this, and in Washington, DC, there are some folks in the think tanks who are beginning to study these issues.

There are a number of significant impediments to good analysis of the IR's impact on world politics. First, creative thinkers on the IR are widely scattered across the disciplines. There is interesting work being done in business, communication studies, sociology, and some, though much less, in political science. But most of these thinkers are not conscious of the international relations consequences of the IR.

What is striking about this void in political science is that almost every day in the nation's leading newspapers there are front page articles about the Internet or some aspect of globalization or the IR, and yet somehow when you read the political science journals you do not see much mention of this phenomenon. This is partly due to political science's concern with creating certain kinds of theoretical constructs and with maintaining the methodological discipline of the field. Problems which do not lend themselves to the traditional methodologies are not well received, even though much of the globalization and communication phenomenon can be measured quite easily. Political scientists dismiss the IR as a change in the "exogenous variables" that impact in some unspecified way people's political preferences, but which as a whole have not changed the nature of world politics.

Second, there is a kind of "two cultures" problem—there is no shared language or vocabulary between technical and national security experts. Among those seriously studying the issue there is a growing recognition of the important connections between these two fields. This tribalism is mirrored in government circles. People in national security like those in the Department of Defense and the intelligence community are thinking about the IR, but the State Department is far behind—the culture of information management and dissemination in State is not good for understanding the IR.

Third, there are a lot of interesting questions about international politics which are not being asked. There are

systematic questions about the impact of the IR on the interstate system, on the global distribution of power and wealth, on the vertical levels of sovereignty, on individual state units, and on democratization and globalization. One largely unexplored area is the foreign policy decision-making implications of a hypermedia environment—the government can't control how issues are framed, who generates information, etc. We really need a broad interdisciplinary debate on these kinds of questions.

Conceptualizing the IR.

Contrary to the conventional wisdom, the IR is not fundamentally or primarily about technology—it is about human agency. Technology does not drive anything independently, or else similar technologies would have meant similar socio-political outcomes in states with similar technologies, but that is not what we have seen. Technology provides us with sets of tools, it facilitates certain types of transactions, and it changes some of the trade-offs between different paths of activity, but it does not ultimately do anything by itself.

If you look at the history of the IR, I think it is much more important to focus on the actors and the dynamics of control over the information environment. Over the past 50 years we have seen in the economic sphere an effort to privatize information in a way that changes who is able to make decisions on economics. This is the beginning of some fundamental transformations that we are just beginning to see more clearly.

The IR really evolved through three main stages. The first phase was from 1837 to 1963, and was marked by the telegraph and radio. In that era, large suppliers (communications monopolies) exercised great control over how information sources were constructed and configured. Systems tended to be large and centralized. The second phase began in 1964 with the success of the IBM 360 computer for commercial customers, and ended in 1990.

53

This period saw the shift in authority and influence from suppliers to large corporate users (such as banks and automobile manufacturers) who demanded specialized communications systems and services. The third phase began in 1991 and might be called the "distributed" era, initiated with the privatization of the Internet backbone. Technological tools in the hands of governments and corporations are now diffused at low cost through many players in economic and other spheres. This is a qualitatively important shift that people have not grasped. Nongovernment organizations (NGOs), organized crime, and terrorists have an unprecedented ability to create and disseminate information on a worldwide scale that challenges the state. In this new realm of world politics, a lot of the old rules do not seem to apply any more.

The IR and Multilateral Institutions.

In terms of global communication, we have witnessed an evolution in how governments adapt multilateral institutions. In the first period there were cartelized, intergovernmental, state-controlled systems which essentially excluded the private sector from authoritative decisionmaking. The markets for communication technologies were largely regulated by governments for their own purposes. In the second phase, there came a demand for liberalization to include nongovernmental actors, open up markets to competition, and allow specialization for businesses in goods and services. This produced a fundamental bifurcation between the status-quo interests of government and monopolies, on one hand, and the open-market interests of a newly emerging coalition, on the other. This, in turn, caused a significant shift out of the stable, consensual, bureaucratic approach in global communications, which had ruled for a 100 years, to a conflictual, trade-driven and highly-politicized environment.

In the third phase—the present—governments are struggling to adapt existing multilateral institutions and regimes to the information economy, while creating new regimes for the Internet, e-commerce, and so on. But they are facing enormous difficulties in this because there is no agreement on how to manage these fundamental issues on a global scale. The point is that with the distributed IR, the ability of governments to adapt to the new rules of the game is deteriorating. There is a decoupling between traditional forms of governmental authority at the international level and what's actually happening in technology, markets, and social practices today. Traditional regimes are losing their ability to control or shape what people do with information technologies on a global scale, and we are moving into a chaotic, heterogeneous, difficult-to-forecast environment.

Conclusions.

There are other challenges for global governance posed by the IR. First, the United States is becoming the driving force in international politics, but it has less to do with state power than with the power of the private sector, technology, and civil society. The American private sector is driving a lot of global activities. There is always a tension between systemic interests and particularistic interests in the United States, and we tend to advance particular (private) ones of powerful organizations under the guise of systemic (public) interests, and others often do not buy in.

Second, the IR has created a growing empowerment of nontraditional actors and issues, such as human rights, landmines, the environment, and women. NGOs are becoming real players in international politics, using information technology to give them far greater influence than they otherwise might have; small organizations without deep pockets are now able to be much more aggressive and influential than traditional theories of international relations would have predicted. The pressure for transparency in multilateral and international

organizations, for opening up to these kinds of actors, is going to be a permanent feature of international politics in the future.

Third, in many cases, the traditional forms of intergovernmentalism will be inadequate to deal with future issues on a global scale. We need new efforts to build cooperative bridges such as global public policy networks to share activity and authority with nongovernmental entities.

The IR, not by itself but in conjunction with other political, social, and technological factors, is going to make global governance more difficult. Intergovernmental frameworks will not be able to adapt, the result being turbulence in world politics.

"Lessons from the Military Experience: The U.S. Military and the IR: The Pitfalls of Uneven Adaptation"

Dr. Steven Metz
Strategic Studies Institute
U.S. Army War College

Like any large, complex organization, the U.S. military has been buffeted by the Information Revolution (IR) and found adaptation difficult. In many ways, what has happened to the U.S. military in responding to the IR is similar to what has happened to business, to governments, and to nongovernmental organizations. But there are crucial differences about military adaptation that we need to keep in mind. If business gets it wrong in terms of understanding and adapting to the IR, some investors lose money, managers lose their jobs, and the business fails. If government gets it wrong, political appointees change, a new party gets elected, and so on. But if the military is wrong, people die, national interests suffer, and perhaps even nations will crumble. These high stakes in understanding and adapting to the IR make attempts to

study the effect of the IR on the military all the more important.

Looking at how the military during the past 10 years has adapted to the IR, we find that the success of the military has been somewhat uneven. When it comes to taking new technologies and applying them to traditional military functions, the U.S. military has been quite successful. When it comes to mastering new roles and missions that emerge out of the IR, the military has been moderately successful. But when it comes to understanding the IR and the need to adapt or adopt new organizational structures, the military still has a long way to go.

We should begin with the least painful change—the ways in which the military services have taken new technology and applied it to their traditional missions. In trying to understand the IR, the services and the Department of Defense (DoD) have largely focused on conventional warfighting. This is what they spend the most time thinking about, so it makes sense that this is where they have been most successful. On a conceptual level, the IR has forced the military to think futuristically. There is probably no other large organization on earth which has put more resources and brainpower into thinking about the future than the U.S. military. This began several years ago in all of the services and is seen in concepts such as the Army After Next. The Joint Forces Command, the Marine Warfighting Lab, and other facilities are conducting experiments, wargames, seminars, and conferences to look at how the IR impacts warfighting. The official thinking is that the IR allows the U.S. military to do the same job it has always done, but to do it better.

The future battlefield is the second area where the military sees the IR having an important influence. The mainstream position (taken from Major General Robert H. Scales, Jr., the former Commandant of the U.S. Army War College) is that the future battlefield will be characterized by high speed, adaptability, and agility, and that more

accurate and timely information will lead to speed and precision of operations. The conceptual template for this is found in Joint Vision 2010, which is designed to create a military with "full spectrum dominance"—the idea that the U.S. military will be better than any conceivable enemy in any conceivable type of conflict.

This dominance begins with information superiority. The military's goal is to create a near-perfect, seamless link between information collected on the battlefield, the decisionmaker using it, and the action taken to implement the decisions. Military commanders in the past have always been looking through the fog of war, and if one considers Napoleon at Waterloo or any other battlefield commander in history, it is interesting to consider whether, with better information, they might have made better decisions. Through better technology and new concepts, the military wants to see through the fog of war. The goal is to provide a commander with a perfect picture of the battlefield and thereby enable him to make nearly perfect decisions. An important and unanswered question, however, is whether information superiority and full-spectrum dominance are actually feasible.

The military has had moderate success in adapting new roles and missions to the imperatives of the IR. There are two new areas which are particularly worthy of comment. First is the broad category of information operations.The military has been trying to adapt its institutions somewhat toward the goal of attaining information superiority. One thing the military has done is to give joint responsibility for information operations to U.S. Space Command, and all the services are involved in information operations. The argument that we need a fourth service to handle information operations will likely intensify in the future. Within information operations there are three important missions:

• Information-in-warfare, which addresses the role of information in conventional activities, such as intelligence,

surveillance, and reconnaissance. The military has always done these things, the new technology just enhances its capabilities.

• Offensive info war, which includes physical attack against the enemy's information assets, electronic war like jamming, psychological operations, information attacks (cyberwar), and military deception. This is one of the most controversial elements of information operations because of the range of legal, political, and ethical questions associated with it. There were several stories in the media on the use of information warfare in Kosovo, but there were conflicting claims about the extensive use of offensive information warfare and claims that such operations were considered but were not used. Because of the interconnectedness of global information systems, there is a significant problem of control over the effects of cyber-warfare. Both current and future information technologies do not match well with the legal, ethical, and political frameworks we currently use to govern armed conflict.

• Defensive information warfare, which includes operational security, counterpsychological operations, electronic protection, information assurance, and counterdeception.

The second new mission is critical information protection, where we face new vulnerabilities as well as empowerment. There is a great deal of concern over how the United States can protect its critical information infrastructure. The military certainly has a role in this, but it is not well-defined so far, particularly regarding the use of military capabilities to protect commercial information. It is clear that the reserve components will be important, but this mission is rife with potential problems. It raises some serious issues of civil-military relations, including distinctions between the two sectors and the functions that are appropriate for the military.

Organizational adaptation is the area where the military has been least successful. The good news is that the

IR facilitates internal communication, training and leadership development, and planning. There are discussions now of creating virtual staffs; instead of needing all of the planners to be in one place at one time, you can have them linked electronically and hopefully include the best possible information and analysis. New training efforts include advanced simulations, distributed learning, and so on. In those areas the military has adapted well.

The bad news is that the IR challenges hierarchies and bureaucratic organizations—it erodes old notions of centralized control that are the bedrock of military organization and function. It is plain that flat networks have serious advantages in adaptability and flexibility over rigid hierarchies in dealing with the new information environment. The U.S. military has not really dealt with this problem, or tried to think about how it might react in the future to nonstate, networked enemies. Take, for example, the struggle against drug trafficking organizations, which are highly flexible and adaptable networks, and the way in which the U.S. Government (including law enforcement) is trying to respond with bureaucratic and hierarchical means. The military admits the need for hybrid organizations—part hierarchical and part networked—but it has not yet fleshed out the concept.

Let me conclude with a couple of observations. First, today the U.S. military is far ahead of every other state military in the world in understanding and integrating the IR. Other state militaries are way behind in all facets of technology, organization, tactics, and strategy. Second, the Air Force and Marine Corps have done the best job of understanding the IR and adapting to it. Why is the Air Force so adaptable and quick to understand the opportunities of the IR? In part because the Air Force's guiding concept of strategic bombing is about defeating the enemy but not necessarily its military forces in the field. Strategic information warfare could be considered a modification of the same idea, allowing you to attack an enemy's infrastructure directly without having to defeat his

military. The Marines' advantage is that smaller organizations are often more adaptable, and recent leadership has placed a premium on innovation and creativity. Third, nontraditional, flexible enemies which are networked will be the military's biggest challenges in the future, not traditional enemies.

Finally, the IR is simply the first phase in the larger, historic Revolution in Military Affairs (RMA). The next stage will likely be marked by the merger of information technology with things like robotics, biotechnology, and extreme miniaturization. Most revolutions have three phases: a moderate step, a radical step, and consolidation. We are right in the middle of the moderate phase, taking new technologies and grafting them onto old ideas. But eventually the radical phase will emerge.

So while the U.S. military is likely to succeed against any other traditional state military in terms of adapting to new technologies, the future may belong to non-state actors. We may be in the middle of a historic RMA, where the IR was simply the spark. If so, everything we know about the nature of war may be changing. Right now the U.S. military has elaborate programs to look at that possibility, but the implications of it still remain to be seen.

Comments

Dr. Paul Hammond
University of Pittsburgh

One of the questions of relevance in integrating such a panel is bringing together a panel's presentations, and I would like to share some thoughts I have on the issue of institutional adaptation.

First, the military has often been way ahead of the business world, in part because of the scale of their work and the enormous amounts of money spent on information-related problems. There is an important

historical point here. In 1961, Secretary of Defense Robert McNamara hired a man to do a "program" budget for the Department of Defense (DoD). The critical thing for the budget was that it separated the accounting system required by Congress from the information system that DoD used. He didn't follow Congress's guidelines on how money was to be spent; he got rid of input-oriented rules to focus on better output-oriented programs. The program budget model included new analytical techniques that allowed the consideration of budget alternatives, yet this also required a great deal more information. This was a giant step towards management-oriented information systems, which were not just systems safe for a steel company to see how production was going, but could tell you how the company was doing from the view of the top. This innovation did not require gee-whiz information technology, but it was an important beginning.

Dr. Prescott spoke of information-oriented people, salted throughout an organization, networking internally and externally. This is a profound step beyond McNamara's approach, which was still directed toward internal DoD information. In the business world you also look outside. The missing step between the DoD model and Dr. Prescott's Best-Practice Companies is that during the 1960s and 70s, businesses had in-house research and development (R&D) organizations. When they came up with innovations for products and processes, the source usually was outside of the firm. Networking was the rationale for doing the R&D even if it benefited others; networking enabled companies to find the innovations they wanted. What we see now is a more extensive networking system with costs that are not tied primarily to R&D itself.

Second, there is a question of how to get an advantage in zero-sum games. There are two kinds of problems from information distortion and manipulation in information systems. First, we should consider reliability. In the 1950s, the U.S. Air Force spent a lot of money on building command and control systems, and they learned then that garbage in

equals garbage out. Unless these systems had benefits to the information providers, the providers gave them garbage. Low-level information sources knew more than the top levels did, and the system did not run well. How do you get reliable information? One possibility would be a library system in which providers benefit from the information, so they have an incentive to do better. We probably do not have this kind of system today. The second problem of information distortion can be seen in adaptations to information technology. Surely we should expect to see new ways for distorting information, manipulating people, and so on, where people will take advantage of information systems. One of the goals of our information systems should be to ensure accurate information, whether it is at the input stage, the analysis stage, or final usage.

Discussion.

The panelists were asked to reflect on several issues: public perceptions and opportunities for asymmetrical attacks through media relations; reliable information versus perfect information; the appropriate public relations role for the military; and the proactive or reactive tendencies of business and the military.

Public Perceptions.

Dr. Metz: The defining feature of war in the information age is that the political-perceptual element is as important as what actually happens—what you make your own people think and other audiences, not just the enemy. Maybe the model for future symmetric warfare is not Iran-Iraq, but India-Pakistan proxy-conflict with air strikes, posturing, and perceptions management. The United States in the future is going to face enemies like Somalia, who really understand our psyche and can be more effective in fighting us. Saddam did it badly, and Milosevic, though it looked early on like he understood, also failed. Future enemies will understand us better, and their future leaders are students

in our colleges today who will have a savvy understanding of the United States.

Dr. Drake: We now refer to "audiences" when discussing war, and we lose sight of metrics for measuring assumptions. Now we are thinking about wars that involve global audiences needing satisfaction, not just for national security reasons but for politics. We struggle with the problem of issue management, trying to find ways to frame issues in real time, but it usually takes a long time to respond. Thanks to CNN, others get to shape the response first, and the United States responds belatedly. We need to anticipate better.

Dr. Metz: This presents a broad-based challenge to the political utility of force. The military's focus on precision and consideration of nonlethal technologies are designed to maintain the political utility of force.

Dr. Prescott: Businesses have been dealing with this on a smaller scale but more frequently than the military, and the military needs to get over its arrogance of not learning from the business community.

Dr. Hammond: Such arrogance may have been justified at one point, but now the "off-the-shelf" that the military should consider is not technology but organizational practices as outlined by Dr. Prescott.

Reliable Information or Perfect Information?

Dr. Metz: The answer is both. The offense/defense question has now shifted to a tension over hiding versus finding. The military says we should plan for that mission, building redundant sensors, utilizing data fusion, etc. So the military thinks it will be able to get perfect information, but I do not think it is going to be possible. Better finding will lead to better hiding technology.

Dr. Prescott: In the business world, competitive intelligence and competitive intelligence organization are

dynamic capabilities which allow firms to learn, to reconfigure themselves, to combine with other functions. Competitive intelligence gives decision-makers a better way of using imperfect information.

A More Active Public Relations Role for the Military?

Dr. Hammond: The military has good reason for not being out in front—it needs to preserve its nonpartisanship. While we think the military wants, and is trying, to get its message across, the costs of trying to be the spokesman make leaders reticent about getting out in front. However, in the future that boundary may have to be shifted.

Who Is More Proactive: Business or the Military?

Dr. Prescott: The business community is not ahead of government intelligence agencies in terms of discipline, but it is better in innovation and lack of departmentalization. Business managers will not put up with compartmentalization, and the speed and quality of decisionmaking are better in business than in the military.

Dr. Metz: The costs of failing in business are much less than the military's costs of failing, so it is easier for business to be flexible and adaptable.

SESSION 4:
SIGNALING AND PERCEPTION
IN THE INFORMATION AGE

Dr. Robert Jervis
Adlai E. Stevenson Professor
of International Politics
Columbia University

Dr. Williams invited me to speak about signaling and perception in the Information Age, and I would like to make some remarks that I hope will contribute to today's discussion. In his introduction, Dr. Williams made reference to several of my books, including my first, *The Logic of Images*. If you are familiar with it, you know that it is about how actors, mostly states but including anyone, try to project desired images of themselves to get others to do what they want them to do. Those images can be true, or they can be deceptive. Then I did a later book, *Perception and Misperception*, showing that in theory these two are very much interrelated. They are two sides of the same coin, because when I am perceiving, I am trying to make certain inferences about the sort of actor you are, your intentions, your character; and when I am giving off behavior to try to project images, I am trying to influence you. When I am perceiving, I want to understand your projection strategy; and when I am projecting, I want to know how you are perceiving. So the two should fit together. However, my two books do not fit together at all either in substance or in style. The one on images is quite inductive and partly utilizes rational choice theory (before it became a theory), and the perception book is much more social-psychological.

Now what makes this more than a personal anecdote is that as the two subject areas have developed, they have really maintained a zone of separation. One other note on the academic literature. In the last 15 years there has been a lot of work done in economics based on signaling models,

and they are almost entirely deductive and descriptive, and quite often useless, because they are totally unempirical and unpsychological, and unfortunately do not get to the heart of the matter.

These two areas need to be brought together better, keeping in mind several things we tend to lose sight of. First, actors almost always want to project desired images of themselves. An important book in this regard is Erving Goffman's *Presentation of Self in Everyday Life* (1959), a sociological classic. Second, the possibility of deception is always present. Anyone who has been a university administrator is familiar with how much deception there is in the world. Now if we look at the U.S. Government, from what we do know from declassified sources, there are a fair number of deception operations. But if we ask how alert is the United States and the intelligence community to deception by others, particularly in peace time, I think the answer is remarkably slight. Part of the problem is that it is very hard to deal with deception, when you are really just trying to get a sense of what is going on in the world, and there is so much noise in the system, so much overload, so much ambiguity. For intelligence analysts and policy-makers, when you try to layer deception schemes on top of that, it may be that the only things you have to latch onto may be totally misleading. It tends to erode your ability to act. Third, which I will come back to, different people have different theories through which they interpret the world, different mindsets. This tends to be lost sight of when people send messages.

Let me give you one example based on the infamous date of December 7, 1941. As World War II buffs know, about 24 hours before the Japanese attack on Pearl Harbor, Washington sent a message to Pearl Harbor saying they should be alert for a Japanese attack, even though Washington was confident the attack was coming in the Philippines. The people in Pearl Harbor received the message, they understood it, and they thought there was a very high chance of going to war, too. So they put the base on

full alert for sabotage, which meant among other things putting all the airplanes together in the middle of the tarmac. What went wrong was that from the perspective of Pearl Harbor personnel, the pressing day-to-day danger was Japanese sabotage. There was a large Japanese community there, the Americans knew they were under surveillance by the Japanese, and, if there was going to be a war, the obvious thing for the Japanese to do was to commit sabotage. Washington was concerned with more global issues like the Philippines, and sabotage was small potatoes to them. But note what is really important at the second level. Pearl Harbor did not know what was the pressing information that caused Washington to be so worried, and the people in Washington could not put themselves in the place of the military leaders at Pearl Harbor who, in doing their duty, had to be worried about things like sabotage. This is the story of a great deal of signaling and perception, certainly in the realm of international politics, and in other realms as well.

For the moment, I will use the term "signals" generally, although there are distinctions among different types of signals. The meaning of signals always comes in the eyes and head of the perceiver. That is obvious, but it tends to be lost sight of. It also means that people think differently, perceive differently, and will have many interpretations of various actions that are familiar, but also ones that are strange. Let me give an example that is too good for me to have made up. Several years ago, before Monica Lewinsky, there was the Paula Jones suit, which President Clinton underplayed for a while. But then he hired Robert Bennett as his lawyer. Two things happened as a result. One was that the case suddenly got much more publicity in the *Washington Post*. According to a *Washington Post* editor, the question was: if Paula Jones had no case, how come Clinton needed to get a hired-gun like Bennett? I do not think Clinton quite realized that was the message he was sending. The other thing that happened, and it was seemingly quite unrelated, was that the U.S. dollar was

greatly strengthened in the currency markets. According to a currency trader, "Clinton's hiring Bennett was really a boon for the dollar." Why? "We were starting to lose faith in him, and that helped turn things around."

What this is telling us, and this may be an extreme case (although the Pearl Harbor case may not be extreme), is that signalers have two problems. One, which I will return to, is knowing what is in the other person's head. Two, any message conveys meaning at two different levels. First there is the message that is being conveyed, and the second is the fact that the sender feels that he or she needs to send a message. Let me give another example. In most restaurant restrooms, there is a little sign over the wash basin saying "employees must wash their hands after using the toilet." What message does this send? To the customer, it appears that the restaurant is hiring people too dumb to know that this is what they are supposed to do, so the restaurant put the sign up to tell them. This is probably not the message they want to convey. Similarly, in some situations when a currency is weakened, or a bank is giving off some disturbing signs, lenders or investors may come out with a statement that they have "confidence" in the solidity of the bank. Or, when university presidents get in trouble, sometimes the board of trustees will issue a statement that they have great confidence in the leadership of the president. On one hand, you might believe them, but on the other wonder why they need to say that.

How would we feel if the American and French presidents issued a statement that there were no differences between their countries that could not be resolved by peaceful means? Universities have recently instituted teaching awards, not to impress students, who know better, but to impress the trustees and donors with how seriously they take teaching. If the university does take teaching seriously, it should not have to have the awards.

There are a great many messages which have this problem. But there is even a second layer, because once you

issue a "reassuring" message, it becomes somewhat expected. Returning to the example of the university president, if it is expected that, when they get in trouble, the board will make a statement of confidence even if they do not have it, then if the board later decides that the statements are meaningless or counterproductive and declines to make them, then the interpretation is that the president really is in trouble. So there are a great many difficulties arising from the fact that signals exist on those two levels.

Let me turn to the crucial problem first of how the impact of signals by definition depends on how they are perceived, and secondarily that this is often unrealized. Many think the best movie for international politics is *Rashomon* (1950), and I absolutely agree. It is the story of four people involved in a crime who all see it very differently. Recently there have been a number of conferences between Americans and former Soviets, between Americans and Vietnamese, going back over Cold War incidents and bringing together the different sides. Leaving aside the numerous problems with these, they reveal the tremendous differences in what the sides believed and how they interpreted the others' motives. It really confirms a great deal of *Rashomon*. Take, as an example, how foreign diplomats have a meeting and then go away and write up separate memos about the same meeting. Forty or fifty years later sometimes it is possible to get the documents from both sides to compare them, and they are often just wildly different. They tend to report more about what they said than what the other side said. They tend to allege hesitancies on the other side, and frame it all in terms of the objectives they were trying to meet. Sometimes you want to ask if this is even the same meeting because the differences are so great.

Ernest May, a great historian, has done an interesting book on the Spanish-American War. He notes that President McKinley's speech to Congress was meant to convey a very strong message to Spain; there are several paragraphs that are obviously the gist, and the rest is just

packaging. May went to the archives in Madrid and got the cable from the Spanish ambassador, essentially a copy of the speech, marked up by the Spanish foreign minister. There were extensive markings in the paragraphs that McKinley had meant as throw-away lines, there was nothing in the margins next to the sections he had meant as important.

We find this phenomenon in domestic politics as well. Historian Richard Immerman and political scientist Fred Greenstein, both experts on Eisenhower, had the marvelous idea of going back to look at the conversation that Kennedy and Eisenhower had the day before the inaugural. Kennedy had been briefed by Eisenhower a couple of days before that, Eisenhower had touched on Southeast Asia, and Kennedy was disturbed enough about it to ask Eisenhower for a second briefing just on Southeast Asia. The way in which this meeting comes down to us in the Schlesinger and Sorensen books is that Eisenhower says it would be unfortunate if we had to send ground troops into Asia (although really more Laos than Vietnam), but if the choice is having to lose Laos or Vietnam or sending ground troops, then we have to send ground troops. There was no tape recorder in the Oval Office, at least not one running that day, but Immerman and Greenstein found four memos of the conversation: Clark Clifford's, McNamara's, Eisenhower's, and yet a fourth. None of them say what is in the Schlesinger and Sorensen books, not surprisingly. They all say something quite different, they contradict each other on many points, they focus on what the person taking notes is most concerned with, and the final twist is that because Immerman and Greenstein know Eisenhower well, they think they can reconstruct what he actually said. But that is after studying him for 10 years, something no one in the room could, and they all came away with very different impressions.

The second order problem is that people rarely realize this. Putting it most simply, empathy is extremely difficult. To understand the other person's mindset, the theories they

have, the way they see the world, is difficult, especially when they view you—as an individual, a corporate actor, or a country—very differently from how you view yourself. So a couple of other examples. One of the biggest surprises we have found since the opening up of archives of Soviet documents is that they talked in private the way they talked in public. They actually addressed each other as "comrade." At the top of the page they would actually say, "Workers of the world unite!" The same sloganeering we discounted really was the way they talked to a certain extent. They talked about us as imperialists, not just telling that to the Third World. They meant it. It is not surprising, although disturbing, that in the many now-declassified National Intelligence Estimates which were written in an attempt to understand the Soviet Union, it was very rare for analysts to be tasked by policymakers to write a memo as if they were Soviet intelligence officers writing to their bosses about what the United States was doing and why it was doing it. They did not want to do that. It is difficult, and no one wants to do it—certainly no analyst wants to do it on his or her own.

As a result, actors tend to think that their signals get through. They sometimes worry they will be discounted as deceptive, or their objectives rejected as being false, but they usually think that at least on the first level the other side understands what it is they are trying to say. Often this simply is not true. The British ambassador to the Ottoman Empire, in one of the perennial crises of the late 19th and early 20th centuries, attempted to give the Ottomans an ultimatum. To show them he was serious and would do no more bargaining, he got in his sailboat and sailed out into the Bosporus in plain view of Turkish spies, and was confident that this would be noticed. They did notice it, but their reaction was that he could not be serious—the ambassador was off sailing again, and nothing serious would happen.

Another example from one of the Vietnamese-American conferences. President Lyndon Johnson launched a peace

offensive in December 1965, with a bombing pause over North Vietnam, dispatching emissaries to over 100 countries, and so on. Johnson probably was serious, he was looking for a way out now, this was not just for public relations. But the North Vietnamese totally discounted it, and, in fact, they thought if he were serious, he would not do it this way—he would not send out so many emissaries, he would not be so public, so demonstrative. They did not know Johnson; this was how he always behaved, he believed in overdoing things. The Vietnamese thought that maybe there was a time the Americans would talk peace, but this clearly was not it. On the other side, the North Vietnamese had a four-point peace program, one point of which was quite ambiguous (regarding the role of the National Liberation Forces). They thought we completely understood what they were trying to say, and it was discussed in several secret meetings at the end of which the Vietnamese thought we understood clearly. We may have discounted some of it as deception, but we did not understand what they were trying to say at all. This happens a great deal.

Let me talk about some implications and some conclusions. First, this is a problem not only between but within governments. As anyone who has been in Washington knows, the only thing worse than negotiating with the enemy is negotiating with the folks in the building across the street. This reflects not only different interests, but people have different tasks and see the world very differently. In the Kennedy Administration, in trying to determine policy toward Vietnam, a team of State Department and Department of Defense experts was sent out into the field. When they came back to the National Security Council (NSC) with wildly different reports, Kennedy supposedly leaned back in his seat and asked if they had visited the same country. Of course they had not, they had visited their own minds—they were simply closed-minded the way we all are. They had certain beliefs and views, and they were going to interpret what they saw in that light.

Second, attempts at deception work best, and I suspect will only work, if you are trying to convince the other side of what they already believe. You have to plan to do what they do not expect you to do; you cannot change their minds. Deception can only work well when you have a lot of information. Remember the Ultra decrypts and the Double Cross system in World War II, which worked brilliantly together, but only because the Allies were reading Hitler's mail.

Third, there are lots of cases where the other side will read messages you have not sent. For example, at one meeting between Scowcroft, Schultz, and Gorbachev, Gorbachev was getting really upset, and the Americans could not figure out why he was so irritated. When they asked him what was wrong, he said that a Reagan speech of the week before had been really troublesome. Scowcroft and Scultz had no idea what speech he was referring to, but after the meeting they found out Reagan had given a speech to some small Republican group, and the public had not really paid attention. It was written by a fundraiser, and it served its purpose. But Gorbachev read it, and no one had expected that.

Fourth, different countries have different histories, and this is important because of the tendency to draw historical analogies based on historical experiences. States often do not understand how important that is to the other side. The North Vietnamese have indicated, and I think this is probably true, that they were very influenced by Geneva 1954, where they felt they were betrayed not only by the Americans but by their friends. By way of historical analogy, therefore, they vowed they would not repeat a whole series of errors they associated with Geneva '54. Almost no one in the Kennedy and Johnson Administrations knew what Geneva 1954 was, let alone that it perhaps might influence the Vietnamese later.

Finally, what is most self-evident to you is apt to be the most troublesome, because you assume it is self-evident to the other side and it rarely is.

My conclusions are implicit in what I have already said. First, *Rashomon* is the rule, not the exception. You have to plan on it, you cannot always defeat it. You have to act on the assumption that it is difficult to get your message through, and that many of the inferences you make about the other side are quite wrong and are different from those the other side holds. Second, people rarely understand this, partly because it is harder to act when you try to deal with this. Third, and related to that, actors often think their messages have been received and understood when they have not been. Therefore, when the other side does not react as expected, you assume the message has been rejected. This may be true, but often the message simply has not gotten through. Fourth, actors tend to think that others understand the images they have of others and the images they are drawing from the other side's behaviors, and that often is not true. And finally, in the face of all this, people still have to act, and there is a difficult balance to be maintained between being open to new information and realizing a degree of ambiguity, confusion, and deception—and setting a strong course in the world.

A final anecdote on this. Richard Neustadt's book *Presidential Power* (1960) points out the importance of how the President gets his information. Dean Acheson came up to Neustadt and told him, "You're always trying to tell the President that he should get all this information that conflicts with each other; my job is to make sure the President makes up his mind and does something." It is a real tension between coming to grips with the difficulties I have laid out and setting a course in the world.

But if I were to advocate a prescription, I do think that without slighting the need for acting in the face of uncertainty, that most important decisions in business and government should not be made without competing papers

explaining what information is likely to be conveyed by this decision to the other side and how the other side is likely to view what we are doing, what its interpretations will be. In other words, without extremely strong efforts to put oneself in the other side's shoes, to exercise some empathy. I think there are very few decisions that are taken on that basis. Doing so might not be easy or solve all the problems, but it might be a step in the right direction.

Discussion.

Dr. Jervis was asked to comment on several issues: American signals regarding democratization; signaling and perception in the Information Age; and simplicity and subtlety in signaling.

American Signals Regarding Democratization.

We can be sure that the message of democratization is received differently in different countries that have different histories, mindsets, and ideologies. It probably is taken well in some areas by newly democratizing countries, the message being that we think those efforts are important. It also might be taken by them as a sign of hypocrisy if we are not putting our money where our mouth is, particularly if they look at our foreign aid budget. It would be interesting to find out what these countries actually think about the message of democratization in light of other U.S. policies. In other countries it is certainly taken as a sense of American hubris—"they're trying to force us into their mold"—that we think we have discovered the latest panacea, because it is a little suspicious that during the Cold War, although we did as much for democracy as any country, the record is not great. Kennedy faced three possibilities in the Dominican Republic, one that it would become a democracy, two a totalitarian state, and three a communist state; until we could guarantee the elimination of the third option, we would have to settle for the second. So

the message of democratization probably does not convey all that we would like it to.

Signaling and Perception in the Information Age.

The discussions during this conference about the explosion of information and information overload suggest that we need to spend more time thinking about institutional and personal screening mechanisms. One of the psychological screening mechanisms would be to become more theory-driven, maybe not in terms of formal theories but in terms of beliefs and expectations. It may well be that the greater volume of information leads to an increased role for what people believe in the first place.

Second, there are many more sources of information out there now. The role of private messengers through history is very interesting. There were priests involved in private diplomacy between the United States and Japan in 1941, and although they did not exactly bring on the American entry into the war, they muddied the diplomatic waters. There are a lot of examples where private actors trying to do good by bringing together two countries often end up doing a great deal of harm. Today there are many more opportunities for private diplomacy, with more access to information.

Third is the problem of knowing the other side's decision cycle and timing. One reason the United States was so surprised in Vietnam was that we were interpreting messages and intercepts found in South Vietnam as if they reflected very recent decisions made in Hanoi. But with all the problems of command and control on Hanoi's side, there was actually a multi-month lag time, so what we were picking up often reflected decisions made 6 months prior. So sometimes you see the other side reacting to you when it really has not, because it has not had time to get your response or message and digest it. Information overload may make the problem worse, though not necessarily. And when you're working in real-time, the press will be on your

back, it is hard to keep a secret, and it is hard to get the time you need to think before replying. You all know how regular mail goes out at the end of the day, offering you an opportunity to take something back on further reflection— e-mail doesn't allow you to do this. E-mail should have a built-in 15-minute delay so you can call it back.

Simplicity and Subtlety in Signaling.

It may indeed be true that it helps to have a reputation for having difficulty responding quickly, rather than having a reputation for being ready and able with clear lines of command and control. A response should be thoughtful. In negotiations deadlines are useful, but there are situations where time is more important and needs to be slowed down. Regarding subtlety, when you look at the historical record, it is evident that when people have tried subtle messages, very few of them have gotten through. On the other hand, some nonverbal signals do get picked up by trained diplomats. Also, when you do not get a response, you cannot assume your message has been heard and rejected. The difficulty often in bargaining is that you want to send something subtle because you do not want to appear weak, so you are caught in that trap. But I think the chances of subtle signals getting through are not great. If you do not get a response, do not assume anything, and do what you can to make things clear.

SESSION 5:
THE INFORMATION REVOLUTION
AND THREATS TO SECURITY

The aim of this session was to assess how some of the threats to U.S. national security might be exacerbated by various aspects of the Information Revolution, looking specifically at asymmetrical warfare, cyber-threats, and different kinds of viruses.

"Metaphors and Modern War:
Biological, Computer, and Cognitive Viruses"

Edmund M. Glabus
Aegis Research Corporation

My plan is to be controversial and creative in thinking about asymmetric warfare. What I am proposing is not a doctrine, not an operational concept, but more of an innovative but tentative idea, using a metaphor to tease out questions for further inquiry. The first thing people think of when considering war is tanks coming over the hill, but this is not the first thing to think of in information warfare. An effective way to think about other things is to use a metaphor which conveys quickly what you are trying to communicate. The metaphor I will be using is that of the virus.

Let me begin with some of the common definitions of a virus: (1) *archaic*: venom; (2a): the causative agent of an infectious disease; (2b): any of a large group of infectious agents; (2c): a disease caused by a virus; (3): something that poisons the mind or soul. Now a layman's definition of a virus would be any agent that takes external copying equipment and uses it to make copies of itself. There are three types of viruses I would like to talk about:

• **Biological**: any of a large group of submicroscopic infective agents . . . that cause various important diseases in man, animals, or plants [Webster's].

• **Computer**: a computer program that can infect other computer programs by modifying them to include a (possibly evolved) copy of itself [Cohen].

• **Cognitive**: an agent that infects people with a meme, a unit of information in a mind whose existence influences events such that more copies of itself get created in other minds [Dawkins/Brodie].

The virus metaphor is a heuristic, sort of a cheat sheet, and is no substitute for good scholarly research—but in a soundbite world, you need to attract attention and communicate quickly. Table 2 illustrates the three virus domains and the similarity of terms used within them.

Biological	Computer	Cognitive
Gene	Machine instruction	Meme
Cell	Computer (paper)	Mind
DAN	Machine language	Representation
Virus	Computer virus	Cognitive virus
Gene pool	All software	Meme pool
Spores/germs	Electronic messages	Broadcast/ Publications
Species	Operating system	Cultural institutions
Genus/higher	Machine architecture	Culture
Organism	Program	Behavior
Genetic evolution	Artificial life	Cultural evolution
Genetic susceptibility	"Back door"/ security hole	"Hot button" or psychological door

Table 2. The Three Virus Domains.

A quick note on memetic viruses. There have been seven articles in the last 180 days with "memetic" in the title. These viruses are inherently good at replicating them-

selves, from deception campaigns to urban legends that will not die, especially on the Internet.

Let me turn to a discussion of viruses in asymmetrical warfare. Of course the goal of asymmetry is that the adversary force wants to avoid U.S. strengths and exploit U.S. weaknesses. This is possible through the use of different virus domains.

First, biological viruses such as anthrax are quite powerful. Iraq declared that it had 2,245 gallons of anthrax, enough to kill billions of people. To put that in perspective, the average swimming pool has 25,000 gallons of water in it—lots more than the relatively small amount of anthrax, when only a small amount of it is needed to be fatal. It is very hard to find anthrax even in the production phase; it is easy to evade intelligence. In asymmetric warfare the enemy may try to step aside of U.S. strengths—to avoid our best-trained military fighters—by using a virus. We are much better trained in other things than we are in biological warfighting. A biological attack can hinder U.S. reliance on speed and agility in combat, and exploit America's perceived unwillingness to suffer many casualties. A powerful technique of virus use is a second strike against emergency responders, which makes it difficult to mobilize, assess, and respond to the first incident; the second one makes possible significant death and disruption.

Second, opponents may use computer viruses in asymmetric warfare. How does the virus metaphor apply to information warfare? The virus allows one to leapfrog across geography—it is easier to inject a computer virus across oceans than other kinds of viruses. The enemy's use of such a virus may negate the moral high ground for the United States that we claim with non-lethal warfare. Both France and Russia sound positive about non-lethal warfare. The user of viruses is able to claim some moral ground in certain forums by arguing that it is non-lethal. It is difficult to coordinate responses to information warfare attacks, especially from viruses, and this may allow an enemy to

exploit the U.S. reliance on information superiority and just-in-time logistics.

Third, an enemy may also use cognitive (memetic) viruses. The use of memetic viruses offsets the physical use of force, moving off the high-tech battlefield and into the human realm. It also flies under the radar of U.S. warning systems, although the United States is rejuvenating its efforts to deal with propaganda and to coordinate responses to it. Memetic viruses inject ambiguity and complexity into conflict, and complicate American policymakers' efforts to achieve political consensus.

So should viruses be considered a sort of unconventional weapon of mass destruction? Maybe so for anthrax, because it can cause such widespread destruction. The answer for computer viruses is no. Although they may produce mass disruption, they are temporary events that can be mitigated once we learn how to combat individual viruses. On the cognitive side, viruses are perhaps weapons of mass deception but not destruction.

Let me conclude by pointing out some common strains and issues among these three virus domains. All three types can be used by states, groups, or individuals, from both internal and external sources, and remote delivery means are available. All require heavy civil involvement—from local and state to the federal level—and raise jurisdictional questions. Most defensive assets for all three are in the Reserve and National Guard. The viruses are cheap to develop and produce, and can become antidote-resistant. It is difficult to train for combating viruses, and hard to conduct combat assessment. And in general, Americans find the use of all three to be repugnant.

The virus metaphor is powerful, and it is relevant to all different facets of warfare. It is important to have creative thinking in all these areas, and I hope that the virus metaphor moves us in that direction.

"Terrorism as an Asymmetrical Threat"

Dr. Stephen Sloan
University of Oklahoma

It is important to begin by emphasizing ambiguity. The problem is that it is difficult in warfare to determine clearly who the enemy is, where the battlefield is, and what strategy is needed to achieve what goals. Many years ago, Admiral Watkins aptly said that warfare would take place in an ambiguous environment. This has special relevance to the changing roles and missions of the military. An article in *Foreign Affairs* several years ago was titled "The U.S. Military as International Social Worker," and we see iterations of military operations other than war (MOOTW), and so on.

Clearly, the end of the Cold War broke the outward coherence of the international system; there was a balance of nuclear terror, and deterrence worked, although with the Cuban missile crisis it was a close thing. The end of the Cold War released forces that were always there—ethnic, national, etc. Today, beyond the arbitrary dimensions of the nation-state are forces geared to using violence in different forms. There are changes in the international system, including an expansion of the technological universe and what Lucian Pye referred to as "diffusion of world culture." There are incredible transnational movements, the Pepsi generation, the Internet. Visit Nepal, and you will see sacred cows walking the street in front of Internet stores.

The response to the technological universe has been a reassertion of primordial loyalties, and although we are seeing perhaps a withering away of those loyalties, we also see self-determination alive and well. There is a reassertion of community not just overseas but also in the United States, people identifying themselves with their own core and periphery.

The United States now certainly feels the difficulty of addressing asymmetric warfare. It is the classic question of martial arts, converting the strength of one's opponent into weakness. The United States has liabilities of national power. And this is still within an environment of ambiguity—there is no longer an agreed-upon definition of what constitutes national security. It used to be traditional military forces and issues, but now it includes environmental challenges and a wide variety of other things. It is clearly difficult to identify what is a national security interest in this changing security environment.

Terrorism is, of course, nothing new in terms of the information revolution. In my earlier studies I have emphasized the role of technology and nonterritorial terrorism—not confined to particular areas. But long before Internet, there were two profound revolutions changing terror. First, the impact of jet aircraft—they became global targets of opportunity, and threw out the window any conceptualization of terrorism as insurgency. You could deal with insurgency, but not when the conflict took place far away from the disputed territory. Second, the impact of communication—the 1972 Munich incident was the breakpoint, although Aum Shinrikyo crossed the Rubicon into mass terrorism more recently. Before the Internet, the CNNdrome provided the public with images but not context. Recall from Vietnam the images of a man shooting a Viet Cong sympathizer; now we see images of an American soldier dragged through the streets of Mogadishu. Things are not in context any longer.

This ties in with perception issues as addressed by Dr. Jervis. We are now dealing with virtual insurgency and virtual terrorism. The military talks about force multipliers, but psychologically one can create threats or magnify them, leaving an increasing impact on the population. These situations have legs—the rumor that TWA Flight 800 was downed by a missile was spread after Pierre Salinger pulled the rumor off the Internet.

86

The situation is complicated by several issues. In regard to the impact of information warfare, a serious organizational debate will continue—organizational doctrine is near and dear to the military heart because that is where the money goes. The classic works on the infrastructure of terrorism suggested a centrifugal model, where the leader was not the center of the organization. This enabled the group to bond and carry out actions quickly without depending on a larger organization. This was also a disadvantage, however, because the compartmentalization required by security concerns kept them from engaging in concerted campaigns—they needed command and control. But through the impact of the Internet and tactics like "netwar" (see John Arquilla and David Ronfeldt), these groups can now use measures short of traditional war, attacking with network forms attuned to the information age. Disparate, small groups are now able to network their groups and activities.

The problem we experience technologically is the fact that we rely on ladder hierarchies which are not well-suited for dealing with centrifugal organizations now that they can coordinate their actions across the Internet. But increasingly we are seeing not just Internet use, but free-floating terrorist cells of two or three people, totally independent of society. They float within environments of anger and hatred, but are free, and they are a profound future threat. There were tremendous security efforts for the Atlanta Olympics, but one lone terrorist—a "bubba cell"—pulled off an attack. These cells are difficult to penetrate.

The greater danger, though, is the cell transitioning to netwar, because our response is still hierarchical. The "lead agency" approach still puts State or the FBI in charge, but increasingly we face seamless terrorism where one cannot differentiate between overseas and domestic groups. New roles and missions are being created beyond the military. The FBI is going overseas, and its assets are increasing globally. The military is also deeply involved in counter-

terrorism regarding weapons of mass destruction (WMD), although always emphasizing it as a part of homeland defense.

Serious issues about civil-military relations are being tested. We need to get the National Guard more involved; there will be new requirements for domestic intelligence collection. Related questions of civil liberties, clipper chips, and concerns about the National Security Agency will arise. I am particularly concerned with the bureaucratic responses to these issues. Despite an apparent appreciation of the words, in national preparedness we are seeing a bureaucratic cockfight, and we are throwing money down the tubes.

Ultimately, we face a major problem, but not just on WMD. The fact is with a biological attack we are dealing with crisis management—sorting out the bodies. The key issue is preemption and how we engage in it. We can no longer afford to be reactive, we need to have information cells to do offensive and defensive information warfare. No matter how good the Federal Emergency Management Agency and the National Guard are, we will only be doing triage after an attack comes.

So let me suggest four things we need to do: demystify, deglamorize, delegitimize, and deter asymmetric warfare. We have not done well so far. We can see the bodies, but we never deal with the context in which a tragedy takes place. Sun Tzu was correct that we live in "infested times."

"The Cyberterrorist Threat"

Lieutenant Colonel (Select) Gregory J. Rattray
U.S. Air Force

While working on my Ph.D., I have spent the past 18 months working in the Pentagon on information warfare (part of the 5 years I have been involved in infowar), and I see it as a huge challenge. Organizational responsibilities

flow from how you define the threat, and we face a problem of broad definitions and descriptions of infowar. But despite national-level attention we do not have structured responses. As an aside, I wonder why, if asymmetries are such a threat, we have not seen more cyber-terrorism happening. We have not suffered much yet from digital disruption. We have been saying this is a problem, but nobody has used it to come after us.

So who are we talking about? Cyber-terrorists are non-state actors with an objective—not states, not individuals or criminals. They are not engaged in public diplomacy, or cyber-espionage, or the use of web sites to release information. Boundary setting efforts are difficult. Many things we do would be appropriate to deal with all levels of threat.

What is cyber-terrorism? It is the destruction or disruption of information and systems. The idea of mass disruption in particular is getting lots of play in public. It might be possible to cause train wrecks with underlying switching technology, but one would need lots of data. Crashing the stock market is the classic case of what you would do to disrupt the United States, and we do see stock markets disrupted by information problems. It would be difficult for us to recover from would-be data corruption of stock market databases, such as the disruption of clearing and settlement of trades, which would raise questions about every trade and create long-term complications. There are also some gray areas like attacks on the media, disrupting CNN, and attacking computer portals; these kinds of attacks highlight the capability of the terrorists. What means are used depend on the objectives of the group.

There are several possible motives for cyber-terrorists.

• political coercion—These terrorists want careful orchestration of actions, and do not wish to alienate the public;

• religion/millennial/anarchists—Disruption is the goal. Terrorist groups may be networked with the goal of a long-term jihad against West, having no specific political goals but also not intended to be a short-term effort; they may plan for long-term disruption and perhaps even the use of extreme WMD; and,

• hackers—Hackers themselves could be co-opted by groups trying to do any of these; however, there are operational security problems with using hackers, and some difficulty of orchestration with hackers actually willing to commit violence.

There also is a range of means available for committing cyber-terrorism. These may include digital attacks like malicious code; denial of service through information overload (we see this most right now); targeted intrusion—hackers breaking in, mostly exploratory so far; corrupted code—the Y2K remediation effort has created an enormous opportunity to create new code insertions into U.S. software, and a lot of the code is from India, Israel, and China; and radio-frequency weapons—things like jammers to disrupt transmission of data will become more important as Internet goes infrared and wireless. However, I would question the traditional wisdom on whether terrorists have the tools, expertise, and access needed to conduct these attacks. Web tools are like hand grenades rather than bullets—they cause problems in networks but cannot be targeted that well. They are not atomic bombs, either—they are not that powerful. The bullet would need a concerted effort and strong tools, and require more expertise than they are likely to obtain easily. However, insiders make it much easier for them to get the access and expertise they need.

The assumption is that cyber-terrorists are most likely to target our critical infrastructure, and most energy and money are spent on critical infrastructure protection. Luckily what sprung from the Oklahoma City and Tokyo incidents were some new mitigative efforts that also looked at cyber threats. We have been focused on critical physical

nodes without looking out for internal interconnections, such as timing and synching computers; these are not a major part of our efforts now. Terrorists are also likely to go after high visibility organizations like corporations, the media, or DOD; attacks against web pages are clearly coming from groups that want to get their name out, get notoriety for their actions. We also need to watch out for hoaxes, and there credibility is the key. Until this year, when we got more real viruses, we had lots of virus hoaxes and spent a lot of time and energy on them. We are doing a better job at recognizing the problem, and PDD-63, the plan for national critical infrastructure protection, calls for a web of organizations and information sharing centers to address various types of threats.

One other note on the possibilities of cyber-terrorism. Terrorists may run two types of campaigns: single incidents with a dramatic impact, forcing us to focus on planning; or protracted guerrilla campaigns which are more difficult to deal with, allowing hit-and-run tactics and posing a significant long-term threat. The policy and investment responses to these types of campaigns may differ significantly.

So what have we actually seen of cyber-terrorism? There has been plenty of theoretical stuff, but we have not seen much evidence. Information systems have been a target for centuries. Cavalry units cut telegraph wires during the Civil War; and there is a long history of infrastructure attacks by Luddites, the IRA, and others. We have seen cases of hackers as terrorists, using the denial of service as a political act, but terrorists as hackers have not been demonstrated to be a threat. An example of hackers as terrorists may be the Zapatistas; related special groups announced and launched an attack on DoD web sites; the military's response actually forced a crash of the attackers' computers.

There are challenges for us in defending against these attacks, and there are challenges for cyber-terrorists. Our

challenges include systems and infrastructures, where we need to get producers to build better systems; tactical warning and attack, which means we need better sensors and network maps; and the fact that response requires cooperation and coordination, which are difficult in practice.

Challenges for cyber-terrorists include problems of developing expertise—the culture of existing groups is not technologically adaptive or adoptive; there are limits to the use of hackers for hire; targeting is more than hacking; and mass disruption may engender resistance in infrastructures and publics over time.

Let me conclude with a couple of observations. We need to avoid hype and try to understand the underlying forces which are making cyber-terrorism a threat. The means to counter it are available, but employing them is tough. The United States is being proactive but we need to do more, and that includes making some difficult policy choices—there is no silver bullet, so we must discern the risks to guide our efforts.

Comments
"An Electronic Pearl Harbor? Not Likely."

David Isenberg
Arms Control Implementation Division
Dyn Meridian

I have some prepared remarks that I would like to share, and then some specific comments about the presentations we have just heard.

Let me begin by summarizing the conventional wisdom, to wit: Some day soon, society as we know it is going to collapse. Why? Because our computer networks will be attacked by hostile states or terrorist groups, and, as a result, the nation's critical infrastructure will go down. The power grids, telephone lines, air traffic control, and

financial networks will collapse; panic will engulf the nation, anarchy will reign in the streets, and life will be one continuous Y2K scenario. Life, as we know it, will cease to exist.

It does not take much effort to see warnings of this. One cannot go a day without reading accounts of the perilous cyber-threats confronting the nation. Consider some of the recent headlines: "Telecom Links Provide Cyber-Attack Route,"[1] "Pakistani Hackers Tap Lackland,"[2] "U.S. Scurries to Erect Cyber-Defenses,"[3] "Cyberwarfare Breaks The Rules of Military Engagement,"[4] "In Theory, Reality, U.S. Open to Cyber-Attack,"[5] and "China Plots Winning Role in Cyberspace,"[6] to name a few.

Preparing for an eventual cyber attack has been a growing threat industry for years now. The Pentagon and numerous other cabinet agencies have been setting up offices to deal with this latest addition to the pantheon of weapons of mass destruction. Think tanks have been cranking out thick tomes,[7] academic journals regularly run articles on the subject,[8] and the defense industry has been holding conferences[9] to solemnly announce the emergence of our newest threat.

There is just one thing wrong. As Gertrude Stein once famously said of Oakland, "There is no there there." Similar to the way the media has gone overboard the past couple of years regarding the prospect of an attack against the United States with biological weapons, the imminence of information warfare attacks has been, in the words of Mark Twain, greatly exaggerated.

In fact, it is nothing short of amazing when you consider that there still is no definition of "information warfare" that is accepted government-wide. Nevertheless we are spending billions of dollars a year on various information operations.[10] This is not to say, of course, that fears of information warfare attacks are totally off base. Certainly, we have seen many deliberate disruptions of web sites, e-mail servers, and introductions of various viruses over the

years. But most of these have been merely garden variety bothersome incidents, not the work of a rogue state or implacably hostile terrorist group.

The problem is that we have been so inundated by lazy, inaccurate, misleading reporting about the subject—which is usually characterized by the phrase "Electronic Pearl Harbor," that we take as a given that which has yet to be shown a true threat. In fact, the reporting is so bad that there are web sites out there devoted to debunking the myths that have grown up about the threats posed by computer viruses.[11] Of course, these sites are in the minority. The vast majority of the sites dealing with the issue, like the media at large, hype and exaggerate the threat.[12]

Consequently, we may do more injury to ourselves than any enemy has done, by simply overreacting. Many press stories are recycled versions of ones that circulated previously, and were wrong in the first place. For example, there was an article in September 1999 about how the U.S. Government is growing increasingly worried that foreign infiltrators are building secret trap doors into government and corporate networks with the help of foreign-born programmers doing Y2K-related work.[13] Anonymous CIA analysts were quoted about being worried over the threat. The only problem, according to George Smith, editor of the *Crypt Newsletter*,[14] is that the same story was first circulated back in the late 1980s and has been periodically recycled since.[15]

Another classic myth which keeps being brought back to life and has assumed the status of the Holy Grail is the Gulf War Virus. For example, in November 1998 the Center for Strategic and International Studies (CSIS) released a report on the danger of hackers and terror from the Internet entitled "Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo." The CSIS study passed on a number of myths, including:

> The United States has readied a powerful arsenal of cyber-weapons . . . planting logic bombs in foreign computer networks to paralyze a would-be opponent's air defense system. . . .

While interesting reading, it is yet another in a long line of appearances by the equivalent of the Internet's Piltdown Man: the Gulf War virus hoax. This was originally an April Fool's story in which the National Security Agency (NSA) was claimed to have developed a computer virus to attack Iraq's air defense computers during the Gulf War; the way in which the CSIS report presents this myth indicates it was taken from sources known to be contaminated by it. [16]

To paraphrase Pogo, we have met the enemy and it is mostly our media. The overwhelming tenor of the coverage has always been toward accentuation of the sensational parts of it. So when people do "intelligence analysis" on this and go to their Lexis-Nexus database, they find hundreds of cites of the same scare stories and minor variations on them going back over the decade. The bad analysis comes when this is used as "proof" that an "electronic Pearl Harbor" can be implemented by any teenager or group of malcontents with Net connections.

In fact, most, if not all, of these articles have a dreadful sameness about them. Again and again the same media organizations recycle the same quotes and clichés, uncomprehending or indifferent to the fact that they are not actually producing anything that is real news. Other characteristics of "electronic Pearl Harbor" stories are:

1. Obsession with hypotheses upon what might happen, not what has happened.

2. Rafts of generally insignificant computer security incidents accumulated as anecdotal evidence and delivered in an out-of-context or exaggerated manner, insinuating that something awful is about to happen—today, tomorrow, a year from now, always in the not easily glimpsed future.

3. Abuse of anonymous sourcing and slavish devotion to secrecy. Emergency Planning Handbook (EPH) stories usually contain a number of "anonymous" sources—from the Pentagon, the White House, Congressional staff, computer security firms, intelligence agencies, think tanks or unspecified consulting firms. Frequently the anonymous will allude to even more secret and terrible things which cannot be mentioned in print or the Republic will crumble.

4. Paranoid gossip, the equivalent of which is offered up as still further proof the nation is in electronic danger. Russia, China, France, India, Israel—almost any country — can be portrayed as taking electronic aim at the American way of life. Programmers of foreign descent are tarred as potential cyber-saboteurs in a kind of modern techno-McCarthyism. Teenagers are transformed into electronic bogeymen with more power at their fingertips than the Strategic Command. The allegations tend to be delivered by anonymous sources or "experts" not required to provide substantive examples. I am not convinced at all that being an expert on terrorism makes anyone an expert in the virtual world, so one goal might be to keep the talks focused on what is real, rather than what might be real. By attempting to restrict any discussion to reality—not media reality—you can put them on the defensive.

Keep in mind there have been no examples of terrorism in the virtual world with any measurable impact at all in the real world. Computer viruses, for example, are not viewed as the work of terrorists by anyone in computer security. While we know viruses exist and a certain amount of money is spent each year in attempts to control them, there are no metrics that exist to measure or even quantify their effects or numbers with any precision. Even the anti-virus industry does not have any accounting standard that provides such information outside of raw numbers of actual individual viruses created, which in itself is a completely meaningless figure with regard to the real world. The empirical evidence that exists shows only that computer viruses never constitute much more than "annoyances" in networked

computing. Conversely, you cannot use that information to infer that they could mean anything special in the hands of potential terrorists.

Let me quote from James Dunnigan, a military affairs writer:

> What gets lost in all the fanfare and desperation over information war is that most of the damage to information systems is, and always has been, caused by human error. The flubs are either by the users, or by the programmers, hardware designers, and the 'integrators' (who put the hardware and software together). Often it is impossible to tell if a system failure is a result of some bad programming or sloppy chip design or the consequence of someone's information war attack . . . . Information war makes good copy—nothing like a frightening lead story to spice up a slow news day. But information war is nothing more than the same old use of deception against an enemy that has been with us since the first recorded battle, 3,200 years ago.[17]

In short, there is no smoking gun that proves any claims the administration or the Pentagon has made about the potential for information warfare against the nation. But there is a substantial body of empirical evidence which suggests the welfare of the United States is not as tightly coupled to networked computers as the futurists suggest, or, rather, that computer security problems, while real, are part of the noise of a technological society that everyone works through on a day-to-day basis.

For example, consider the Melissa virus. There was no impact on the stock market, no impact on the economy. And so it has been with computer viruses in general. Although they are often bandied about as part of the info-war Pearl Harbor scenario, there are no convincing studies that show computer viruses, despite widespread existence on corporate, government, and military computers over the entire decade, have much of an impact on anything. More likely, you can factor them in with the types of human errors, accidental erasure of files, and network accidents

caused by incompetent administration that everyone struggles with.

So how do we go from an unquantifiable grit in the economic machine to a software bomb that brings down everything? No one has a compelling answer for that other than science fiction scenarios and what-ifs, which are a dime-a-dozen. It is like saying the common cold virus could mutate into something that causes cancer next year. No one would take the cold virus scenario seriously, but many seem to believe the software possibility.

Where were the cyber-warriors during the conflict over Kosovo? There was no impact, other than a minor media one when alleged Yugo-hackers (who could also have been American teenagers) tried to mess with NATO's web page. There was no impact, other than a media reaction, to "Chinese hackers" messing with the U.S. Information Agency (USIA) web page, or whomever they messed with—and again we could be talking about American teenagers.

Anyway, there are no studies that explain how the defacing of web sites equates to a potential for looting the electronic treasury and turning off the water or power. The only thing that can be said is that it appears that web site break-ins are common. But this cannot be explained by simply *detecting* more such attempts. In many cases, it is merely a reflection of better monitoring and awareness—that is, the Pentagon is seeing what, in all likelihood, was always there. And there is some self-fulfillment, too—the more it gets into the mainstream press, the more net idiots are inspired to get a piece of the action. This is a well-known hacker phenomenon.

There are precious little detailed technical descriptions that demonstrate how an electronic Pearl Harbor would be attempted. You simply cannot find any. You can find a lot of technical description of security holes in software and hardware. But this is not the same thing. Because you can overwrite the stack of various pieces of Internet software

with malicious commands does not equate to turning off the power on the eastern seaboard. It only equates to gaining some access on one vulnerable machine. Does that machine control everything of value in the United States? Probably not. However, there is a lot of nebulous description, which in reality can be done by anyone with a 15-minute education on the topic.

The hyperbole surrounding the vulnerability of our information systems has degraded useful education on the topic and created an environment where it is actually harder to get practical work done. There has also been an explosion in snake-oil salesmen seeking to line their pockets by catering to the fears of the not so well-informed. It mirrors what has happened with Y2K. Every major statement by an administration or Pentagon official on this subject is always followed by press releases on the business and PR newswires issued by fly-by-night consulting and computer security firms trying to coat-tail on the publicity. As a result, it has become very difficult for someone not highly trained in the area of computer security to differentiate the con men from the legitimate. Yet, this is what management in government and corporate America must do everyday. One might conclude that the hysterical tone the government uses has actually harmed national security by opening a portal through which con men, idiots, and the simply greedy gain access to systems they might normally get nowhere near.

Furthermore, there are a number of very good reasons why the national security preoccupation with an electronic doomsday has actually been a hindrance to the establishment of good computer security measures. First, it creates the impression computer security is an endeavor designed to protect from catastrophic events that come in one lump. Nothing could be further from the truth. Computer security is a day-to-day affair. Information technology professionals in a working environment have to deal with aspects of it as a daily part of their jobs. The constant implication that security is only of interest as it

relates to theoretical catastrophes interferes with education on it. Good computer security practices come from the grass-roots up. Fundamental education on basic issues—even as simple as being able to get trusted anti-virus software or password management—is more important than the creation of yet more super agencies and analysts to mull over or handle the threat. Put even more bluntly, computer security is everybody's business. It does not do well in secret or in a hierarchical world.

Second, the overemphasis on theoretical threats has resulted in a true rube's approach to the subject. Anybody can come up with the suggestion to create a new agency, a "cyber-corps," an "electronic FEMA," an arm of the military—to be a central coordinator for computer defense, but this completely ignores how successful computer security practices evolve. For example, the anti-virus industry is a model of distributed computer security. It is a true global network. There is no central overseer of anti-virus effort. To be sure, the industry is aggressive and often conducts business in a predatory manner, but in spite of itself it must be distributive in nature. There simply is no other way to combat computer viruses. No one can do it all. No central location could possibly muster enough resources and react fast enough to emerging infections.

Another example of the necessarily distributive nature of net policing is the Internet reaction to spam. The emergence of spam as a growing nuisance really does get to the heart of computer security issues. Simply, spammers make unauthorized use of the computing resources of others. In response to this, an informal international group of administrators who hate spam emerged to construct protocols and procedures for dealing with the worst offenders. Again, this is a distributed process—not a centralized, pyramidal, bureaucratic effort. The Internet itself, in other words, tends to work against those attempting to damage it. This also has very important implications for those contemplating the use of it as a platform for information warfare operations.

The continued entertainment of the idea that another safeguard of the infrastructure is just another super agency away is unwise and misinformed. The Department of Defense (DoD) has a serious brain drain in computer security workers, partly because of this approach. Many communication security workers started working for DoD but lit out for greener pastures because (1) DoD simply will not pay them what they are worth in the private sector, and (2) they are stuck in a hierarchical, centralized scheme in which they have to consult with many distant superiors to perform basic functions necessary to computer security. So they quit and go where they can do what they have to do and get paid twice as much for it.

Moreover, the emphasis on central defense against theoretical threats thoroughly obscures the fact that there is not much pressure anywhere to develop commercial use software that is robust from a computer security viewpoint. The focus on fixing "external" threats is a symptomatic approach—it does not get at the real roots of the disease—which is that software and hardware have heretofore been developed in an environment that views secure computing as an afterthought, not a necessity. To change that takes education at a basic level. For example, computer scientists and programmers should be more thoroughly schooled early with regard to taking security into account when developing software in future businesses.

To summarize, does this mean that there is no threat to computer networks? No. It just means that we have met the enemy, and it is our own lackadaisical computing habits and incompetent reporting that threaten us.

Now let me turn briefly to comments on one of the previous speakers. Mr. Glabus is correct that there is no doctrine for viral warfare, but there is no doctrine for many possible threats like bioterrorism and nonlethal threats. Metaphors are often greatly exaggerated or distorted because we have few actual examples from the past; we should not give much credence to them. Biological viruses

have a psychological impact, producing a visceral, terrified response. But, like computer viruses, they have perhaps been ballyhooed excessively. Israel has dealt for years with the threat of terrorism, but people do not overreact to possible attacks because it is a part of life, more so than here. People eventually will have to get smarter about passwords and computer protection, but that does not mean that hacker attacks will never succeed.

Discussion.

Discussion at the end of this session focused on three topics: the possible legitimization of terrorist attacks, particularly because of the ill-defined yet strategic nature of terrorism and information warfare; asymmetric warfare and the ability of the American public to filter out media bias; and the problems of hoaxes and incorrect framing in understanding "virtual terrorism."

Terrorism and Asymmetric Warfare.

Dr. Sloan: There really is no agreement on the nature of terrorism. The Vice President's report on terrorism pointed out the difference between an act of war and a criminal act, but terrorism can be clothed in legitimacy by calling it war. Asymmetric warfare is a concern. Despite the global military power of the United States, given our shaky preparedness and the force drawdown, there are new questions about our ability to engage in the regional contingencies which are still out there. Conventional war is still a reality, and though asymmetric warfare will be important in the future, we may be focusing too much on it.

Asymmetric Warfare and Media Bias.

Mr. Glabus: If one looks at recent coverage in the *San Jose Mercury* about hacker operations, it was a relatively sincere effort, and it went back and apologized later for

some misreporting. Both spin doctors and the media have to go back and fix their reporting later if possible.

Dr. Isenberg: There is a bifurcation in society between those who follow the mainstream press and those who follow alternative outlets or sources. People following mainstream news in the future will not "get it."

Virtual Terrorism, Hoaxes, and Framing.

Dr. Sloan: Of course the government is trying to bring order out of chaos, and often focuses on the threat *du jour.* Following the Oklahoma City bombing, people immediately blamed Middle Eastern terrorists because it was easier to demonize a foreign enemy. One of the issues in information warfare is that the American portrayal of what terrorists look like is inaccurate and unhelpful. Incorrect framing of terrorism gets in the way of meaningful analysis. Those frames take on their own legs, and the dynamics are that you do not get down to the truth. Consider the sound of silence about Pan Am 103—we do not blame the real culprit of that attack, Libya.

SESSION 5 - ENDNOTES

1. David A. Fulghum, "Telecom Links Provide Cyber-Attack Route," *Aviation Week & Space Technology*, November 8, 1999.

2. Sig Christenson, "Pakistani Hackers Tap Lackland," *San Antonio Express-News*, November 3, 1999.

3. Bob Drogin, "U.S. Scurries to Erect Cyber-Defenses," *Los Angeles Times*, October 31, 1999, p. 1.

4. John Markoff, "Cyberwarfare Breaks The Rules of Military Engagement," *New York Times*, October 17, 1999.

5. Bob Drogin, "In Theory, Reality, U.S. Open to Cyber-Attack," *Los Angeles Times*, October 9, 1999, p. 16.

6. Bill Gertz, "China Plots Winning Role in Cyberspace," *Washington Times*, November 17, 1999, p. 1.

7. John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, 1997; Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, *Cyberwar: Security, Strategy and Conflict in the Information Age*, AFCEA International Press, 1996; Stuart J. D. Schwartzstein, ed., *The Information Revolution and National Security*, Center for Strategic and International Studies, 1996; Edward Waltz, *Information Warfare: Principles and Operations*, Artech House Publishers, 1998; and Jean Guisnel, *Cyberwars: Espionage on the Internet*, Plenum Press, 1997.

8. Peter De Feaver, "Blowback: Information Warfare and the Dynamic of Coercion," *Security Studies*, Vol. 7, No. 4, Summer 1998, pp. 88-120.

9. "CyberTerrorism: The Risks and Realities," November 16-17, 1999, Washington, DC, Jane's Conferences.

10. To quote a past U.S. Government Accounting Organization (GAO) report, "Defense Information Superiority: Progress Made, But Significant Challenges Remain," Letter Report, 08/31/98, *NSIAD/AIMD*-98-257:

> Achieving information superiority will be expensive and complex. Based on its analysis of the fiscal year 1999 through 2003 Future Years Defense Plan, DoD estimates it will budget an average of $43 billion a year (nearly 17 percent of the $257 billion budget request for fiscal year 1999) for C4ISR systems and activities during the plan period.

> Though information warfare spending (both for defensive and offensive information operations) is certainly likely to be a smaller subset of this, it still is likely to be billions of dollars a year just within DoD.

11. See *http://kumite.com/myths/*.

12. A few random examples are *http://www.uta.fi/~ptmakul/infowar/index.html*; *http://www.aracnet.com/~gtr/archive/index.html*; *http://www.rand.org/publications/MR/MR661/MR661.html*; *http://www.psycom.net/iwar.1.html*; and *http://www.infowar.com/*.

13. "Threat of 'infowar' brings CIA warnings," *Network World*, September 15, 1999.

14. See *http://www.soci.niu.edu/~crypt/*.

15. Personal e-mail, September 15, 1999: "Ahhh, the fruits of Schwartau, Inc. All the kooks always come out for it. The CIA/NIPC dude warning about Bulgaria and Cuba making viruses is a hoot. He's only a decade late. Those stories stem from the late 80s."

16. See *http://sun.soci.niu.edu/~crypt/other/sped.htm*

17. James F. Dunnigan, *Digital Soldiers: The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield,* New York: St. Martin's Press, 1996, pp. 278-279.

SESSION 6:
RESPONDING TO SECURITY THREATS

The goal of this session was to consider the U.S. response to threats to the national information infrastructure, and how those responses might be enhanced.

"From Incident Data to Intelligence Analysis"

Jon Ramsey
CERT Coordination Center

In 1988 the Morris Worm, developed at Carnegie-Mellon University, attacked the Internet. The Defense Advanced Research Projects Agency (DARPA) responded immediately, and out of that incident was born the Computer Emergency Response Team (CERT). We now provide 24-hour technical assistance to Internet sites, assess their vulnerabilities, issue advisories, and offer guidance on flaws in information technology.

CERT operates on a number of principles. First, we try to provide valued services. The "response" in our title implies that we are reactive, but we are also proactive. We educate vendors on what they should and should not do, work with security administrators, and do evaluations for a variety of constituents. Second, we ensure the confidentiality and impartiality of our services. We do not identify the victims of cyber-attacks, but can pass information on anonymously to warn others. We are also an unbiased source of trusted information. Third, we coordinate with other organizations and experts in the community, government, and private sector. We utilize a distributed model for Incident Response Teams, emphasizing coordination and cooperation, not control. The CERT Coordinating Center helps these other teams coordinate their analysis—we provide intelligence that only aggregate information can produce.

Our constituency really includes everyone on the Internet. As of January 1999, there were 43 million host computers around the world, including a diverse set of users: academic and research institutions, government, corporate users, and home systems. Anyone can turn to us for assistance.

Regarding the collection of data for intelligence analysis, we call our collection the Haystack. We collect the data for operations but not for analysis—how long did it take to recover, what cost, what preventions? What are the risks, mitigation strategies? We are working on an automated process to handle the reports of 45-60 incidents we receive each day. The data is stored in e-mail messages and status files, but there is a problem with solving syntax and semantics problems in those reports and messages. Additionally, whereas in 1988 CERT handled six incidents, in 1999 the number of incidents exceeded 9,000. So the overall Haystack includes 22,940 incidents, 251,000 e-mails, and 17,000 hotline calls.

Processing Data to Produce Information.

Our information is derived directly from the data and from other open sources. We use these to find trends, to discover classifications and categorizations of incidents, and to create advisories and reports on intruder tools. We also use nontraditional information such as political and social events. For example, we have found that virus and worm attacks seem to correspond to mid-semester breaks for college students, and our advisories seem to increase the number of reports rather than reduce them.

One of the things we have done with the data is to create a root cause taxonomy of the vulnerabilities we have discovered. The taxonomy shows which root causes to go after (such as buffer stack overflows, and configuration and authentication problems). We have also created a Distributed-Systems Intruder Tools Report which analyzes the newest sets of intruder tools being used. The report is

available online at: *http//:www.cert.org/reports/ dsit_workshop.pdf*.

The next step for CERT is to turn information into intelligence products. We hope to do this using a multi-disciplinary approach. This includes, for example, trying to understand an intruder's motive through the help of criminology, psychology, and sociology. We are also using some recent advances in technology such as data mining and automated learning and discovery to assist in the analysis process. In fact, the mission of the CERT Analysis Center is to use a multi-disciplinary approach to the creation of intelligence based on computer security incidents, vulnerabilities, and related information.

Let me conclude by reemphasizing our main goal, which is to use intelligence to protect our national information resources by capitalizing on data collected at the Center over the last decade.

"A Computer Crime Overview: National Infrastructure Issues"

Dan Larkin
Supervisory Special Agent
Federal Bureau of Investigation
National Infrastructure Protection Center

I am a realist, and am somewhat skeptical about the problem of computer crime. There is a problem, but I am not sure it is an international threat. Most cases we have seen in the FBI are domestic, although there are some ongoing international elements.

How do computer crime issues at the federal level translate down to the local level? There is significant computer-related crime in the Pittsburgh area. This region has 450 software firms and 800 high-tech companies, and a number of these facilities have been targeted by criminals. What we are trying to do is focus on the real threats,

reaching out to the experts in the military and in industry to locate those threats, and there are some new efforts at least at the local level to find an approach to the problem.

The Internet and increasing interconnectivity have led to vulnerability because of the need for speed and more information. What has happened is that we have had lots of juvenile Internet hackers, and the reality of the threat is vulnerability. I started working with CERT 5 years ago as part of the first national computer crime squad in Washington, DC. One hacker got into the National Oceanic and Atmospheric Administration (NOAA) satellite system, and the FBI started working with CERT; now there is a full-time agent from the FBI at CERT. We are making more and more efforts to get business on board to work with us, confidentially, to inform industry about information that might be targeted.

The fact is that hackers are mostly juveniles, and they really fear prosecution. There are other criminal types involved, however—hackers, insiders, national, or international industrial-commercial spies. The FBI has had some success against economic espionage. For example, a celebrity came for treatment at the University of Pittsburgh Medical Center, and the hospital tried to protect her identity; a hospital employee hacked in to steal her medical records to sell them to a magazine. This event actually led to federal legislation to protect computer records. At Pittsburgh Paint and Glass, people were caught trying to peddle company secrets, and two were prosecuted.

The Internet provides criminals with a number of advantages: it makes it easy to locate victims; it creates an environment where victims do not have to see or speak to the criminals; it is a persuasive vehicle for fraud; there are only minimal costs to setting up a web page; and technology has exploded exponentially in the recent past. As a result, we have seen several particular types of Internet crime come to predominate: financial crimes such as money

laundering and on-line gambling, terrorism, extortion, child pornography, and a wide variety of frauds.

Let me conclude by highlighting several of the government's responses to these problems. First, Presidential Decision Directive 63 (PDD-63) created the President's Commission on Critical Infrastructure Protection, the goal of which being to network on the key issues and vulnerabilities in our critical infrastructure. Second, there is a new Internet Fraud Center coming on-line soon in West Virginia. Third, the whole Y2K crisis has been useful in forcing us to look more carefully at our vulnerabilities, and we are getting more feedback on vulnerabilities from industry than before. Finally, we are instituting a program called InfraGard, in which we go inside industry to work together on vulnerabilities, and boil that information down to disseminate to others (while retaining confidentiality). So far local industry has been quite responsive.

"Gaps in Response"

Frederick G. Tompkins
Information Security Principal
UNISYS Corporation

What we are concerned about in the business sector is that the government community (primarily intelligence and law enforcement) is primarily looking at postulated or perceived threats. Our concern is that postulated/perceived is on the opposite end of the spectrum from where we are looking, which is what is real and what is probable.

Last February Dick Clark of the National Security Council (NSC) came to a financial industry session to discuss private sector samples of attack signatures. He indicated that the government had a database of 100s of attack signatures, and would make them available to industry with no conditions and no charge, with no expectation of return information. We were working on a

111

vulnerability assessment methodology for the financial services infrastructure, and told the government we wanted a threat and indicator briefing, and that the database needed to be made available right away. However, soon the government told us that we needed clearances to get into the threat briefings, since they were not open after all. We did get a secret level briefing, and what we heard was based on secret information sources that we were not allowed to know about, and so on. So we are skeptical, to say the least. When we are told that information will be made available to us, we usually do not get it.

Let me put this issue in context. What is reality for the commercial sector? Our problem is now, not just down the road.

• **Commercial off-the-shelf technology**. The problem we face is that we no longer custom-design software, so that every unique problem we face must be dealt with using generic software. We cannot influence the design and development of the products we must purchase. In terms of risk, this increases the degree of uncertainty. Now we are changing internal business processes to employ software that was made by someone else; technology is the driver, not the servant, and this is a dangerous trend. A major Y2K risk concern is that 85 percent of the remediation code being written is from India.

• **Rate of technology change**. The half-life of technology is now 5 months. This shortens internal industry planning time frames from years to months, even down to days/hours. The strategic planning time frame used to be 3-5 years, now it is 8-10 months; tactical planning was 1-3 years, now it is 30 days; operational planning was 1 month to 1 year, today it is 48-96 hours. We simply have to move on to the next problem if we cannot fix the first one.

• **Risk acceptability**. How do we manage the synergistic effects of risk across the infrastructures? Typical government responses are all about sandboxes and turf; people are talking about threats and vulnerabilities,

but not risks, which is what we deal with. The arithmetic of the Cold War was easy; we could quantify the threat by counting. But we cannot do that now; we cannot do quantitative risk management. It is not possible to eliminate all vulnerabilities; the best we can do is pursue risk avoidance. For example, there is a trade-off with multi-programmed operating systems, which are actually serial, not simultaneous. Data is transferred between programs during wait times—control can be taken away from outside thanks to a flaw in how these operating systems are designed; the only solution is single-task operations, which are no longer feasible in the business environment. There is a trade-off between security and speed/flexibility.

• **Speed of business**. Little academic work is being done in this area. Just-in-time logistics in business is everywhere. At the Chrysler plant in South America, parts arrive just two hours ahead of when they are needed. Wal-Mart has no stockroom; each store instead has a satellite dish which enables it to order resupply as needed.

National and International Security.

Let me make several observations on national security. Essentially, a different model of national security is needed. Former Deputy Secretary of Defense John Hamre has said that what is at stake is security "pre-Eisenhower," which means economic security. This was recognized in the President's Commission on Critical Infrastructure Protection (PCCIP) report, which stated that "our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society." The commercial sector actually owns the infrastructure, and we control it within certain risk levels; the commercial sector wants to enrich its stock-holders, not arrest criminals. It needs a competitive edge to stay ahead in the marketplace where the product cycle is now 18 months.

The interim Hart-Rudman report (September 1999) emphasized the economic security impacts of technology vulnerability. It concluded that "the national security of all advanced states will be increasingly affected by vulnerabilities of the evolving global economic infrastructure" and that "global forces, especially economic ones, will continue to batter the concepts of national sovereignty." What is at stake, then, is not only the nation's security in the constitutional context, but also the nations' security because of the interdependence of economic relations and the international operations of American companies. For example, UNISYS does 60 percent of its business overseas; it controls NASDAQ operations, manages over half of all check clearances, and is used by most large banks in the world.

In summary, I would suggest several things. First, there are still significant cultural differences between industry and government which are bigger than paradigms and language. We are in a Kuhnian revolution in knowledge, and the current paradigm is in crisis; shifts are occurring and we do not know they are happening. The scientific community is at least 5 years behind in understanding the problems. Second, we all have a stake in the nation's security. Third, risks must be managed, not avoided. Nobody is saying how to do it, but compliance is not the answer. Fourth, our predilection for the countermeasure *du jour* must be overcome. Finally, what we are witnessing is not an information revolution, but a relationship revolution, with profound implications for how we do business.

Comments

Mac Fiddner
University of Pittsburgh

My challenge is to try to bring these presentations into perspective on the theme of the conference, but in the interest of time my comments will be brief. Responses are

the most difficult aspect of the problem, not just the technological complexities, but also the types of information being transmitted (public, private, and classified) and problems of sources, all while maintaining confidentiality and integrity. I would conclude that at the moment the government does not have a real policy in regards to information security. There is perhaps a de facto policy from the President's Commission on Critical Infrastructure Protection, but it is not a well-articulated policy.

Discussion.

Discussion revolved around the idea of cyber-mercenaries and the confidentiality of information provided by business to the government. The FBI has seen a relatively small number of cases of hackers for hire, and of the three most recent cases, two had significant international elements. The FBI's response has been to improve networking within the intelligence community to create early awareness, including broadening its network of intelligence to include groups like CERT. CERT does not investigate the origin of a threat; rather it reacts to the event itself. Mr. Ramsey believes that the majority of such incidents are international, raising important legal and jurisdictional questions.

Industry is concerned that the government may misuse corporate proprietary information (e.g., turning it over to the Securities and Exchange Commission), with no guarantee from the government that the information is going to be held confidential, particularly in response to Freedom of Information Act (FOIA) requests from business competitors. The FBI's position is that while business does not get satisfaction every time, the level of security from the FBI is appropriate, and business is protected from FOIA.

NOON SESSION:
Video Teleconference

This session built on the previous session on responses to security threats.

"Towards a National Information Security Strategy"

Dr. John Arquilla
Naval Postgraduate School of Monterey
and
David Ronfeldt
RAND Corporation

Let me begin with a definition of information strategy. It is the pursuit of policy through informational ends and means, and it includes several components. First, supporting existing political, economic, and military domains of statecraft, and emergence as a distinct new domain itself. We want to conceptualize information as a distinct dimension of American power. Second, managing our own capabilities and resources, and interacting with others in peacetime, crisis, and war. It is at least as important that we learn how to manage our own resources as it is that we determine how to attack the enemy. Third, attending to both the contents and conduits—both the structuring and the processing—of information. It applies to the message as well as the medium. And finally, realizing that "information strategy" corresponds, at the highest level, to "knowledge strategy." What does one know about the battle for Seattle? Black helicopters and 135 nation-states were upended by nongovernmental actors.

As the information revolution alters the world, we see some crosscutting trends. First, the information revolution is resulting in a vast new technological infrastructure. We

have global access and interconnectivity, and the United States is the primary beneficiary of this, but as we become more dependent on it we also become more vulnerable. Second, the power of networked non-state actors is increasing. In civil society we are seeing nongovernmental organizations (NGOs) and activists, but we also see the emergence of "uncivil" society, such as criminals and terrorists. Third, the information revolution is enhancing the effects of "soft power" and "information operations," giving people greater ability to influence events. This is true of the Zapatistas in Mexico, of radio station B92 in Serbia, and Suu Kyl in Burma, for example. For states, this can also have some positive effects, perhaps allowing us to act at lower cost and with less risk, and perhaps also to target our actions better. We use economic sanctions quite frequently but with many unintended consequences. Information operations might allow us to pursue our aims without hurting a lot of people. Fourth, states are being altered in some ways, and perhaps diminished, but they will have to learn how to deal with these new actors.

David Ronfeldt and I are trying to articulate a four-part vision of where we should go with U.S. strategy. First, there is an emerging set of strategic opportunities and imperatives.

• On the defensive side, we need to maintain "guarded openness." Our economic and political security depend on open relations with our allies, but we have to be guarded because almost all information technology is dual-use in nature.

• Integrate a "sensory apparatus" to warn and monitor. In other words, we need to learn how to network better, something we do not do well in government.

• Develop the "noosphere" proactively. David and I like to coin a new term at least once a year, or else we are not doing our job, and this is taken from Des Jardin's notion of a "realm of the mind." This subsumes both cyberspace and the media-driven infosphere, and our corollary is that a new

type of politics will emerge alongside it, "noopolitik" rather than "realpolitik."

• Project the right "story" via soft power. Whose story won during coverage of the demonstrations against the World Trade Organization in Seattle? Clearly, the demonstrators' story prevailed.

• Use "strategic swarming" to mix hard and soft power. Swarming is a kind of tactical or doctrinal approach that allows one to strike from all directions simultaneously, whether it is social activism in downtown Seattle or the Zapatistas in southern Mexico. An interesting example of this was General Shelton's actions in Haiti a few years ago, where a small number of Special Forces were able to spread out and maintain control of the island during a period of intense coercive diplomacy.

Second, there is some concern or sensitivity over the role of the United States in information sharing versus information domination. Even our allies are worried about intelligence cooperation with us because they are afraid of some kind of exploitation. And if you listen to the Iranian or Vietnamese media's depiction of world opinion, they perceive that we are seeking domination over the world through cultural exports like reruns of Baywatch, although I do think some of this is tongue-in-cheek.

National Information Strategy.

How do we move toward formulating a national information policy and strategy? We have to rethink how we are applying "information" in the current political, economic, and military domains of our grand strategy. Then we need to identify the building blocks and measures for the development of a new information domain of granted strategy. This idea first appears in President Reagan's National Security Strategy in 1981, suggesting the notion of information as a fourth dimension of national power. At the same time, we have to think about how this problem applies

to the offense-defense dilemma and its implications for deterrence and coercion, as well as what it means for alliances and conflict resolution.

Current grand strategy is already replete with information-driven elements. On the political level, our goal of democratic enlargement is greatly aided by interconnectivity because it puts such pressure on authoritarian regimes. But there are places where we need to apply some prudence because we do not want to see change come too quickly. We do not want it in Saudi Arabia yet, and who wants democracy in Algeria if the radicals take over?

In the economic domain, information creates a tremendous new profitability for the United States; the expansion and growth we have seen in the 1990s is the product of the information revolution. But we are looking at technology that is all dual-use, having both commercial and military applications, so we may inadvertently be endangering our information security and empowering our rivals. One of the great problems in our relations with China has to do with the ballistic missile and other technologies that they are acquiring.

On the military side, it is a fascinating time. It is difficult to find another period in time where one power had such predominance in military power over all others. What the information revolution is allowing us to do, in terms of information operations and the information used in our weapons systems to improve their accuracy, is to use extremely limited and discriminate force. But there is also a danger of information arms races, and the possible spread of weapons of mass destruction (WMD), if the U.S. edge in information technology is not shared. Opponents may feel the need to offset our capabilities with dirty, old-fashioned WMD. Recent Russian military exercises called ZAPAD [WEST] 99 featured extensive use of tactical nuclear weapons.

A Framework for the National Information Strategy.

If we want to conceptualize a framework for information strategy as a distinct domain, we need to think not only about offense and defense, but also about a more general posture. We need to think about the ideational tenets and organizational and technological principles, but the real defining level is that of ideational concepts. (See Table 3 below.)

We have a policy choice to make: are we going to focus narrowly or broadly? If narrowly, then our focus will be on cyberspace security and safety. This includes infrastructure protection and assurance, intrusion detection and rapid-response strategic information warfare, and public-private intelligence coordination. This is where we are right now. If our focus is broad, then we need to place additional emphasis on global "soft power." We would pursue this notion of "noopolitik," which is an international system based on ethics, norms, and values. It is really a revolution in diplomatic affairs, and the next step beyond constructivism. Such a strategy at a broad level would include the right of communications and information for all, and the deep coordination of government and NGOs. For example, why were none of the NGOs invited to the World Trade Organization meeting in Seattle? In either case, we need to pursue guarded openness, strategic swarming, organizational networking, and infrastructure expansion.

At the organizational design level, we recommend interagency networks and some new organizational structures, as well as better public-private cooperation. Half of all military communications traffic goes across commercial systems, so we need to learn how to cooperate better.

On the level of technological applications, we recommend wide diffusion of strong encryption technology because the bad guys already have it, so we might as well

use it. As to defensive measures, we need better depth defense—there is a kind of Maginot Line mentality about information security with firewalls or orange book systems that (supposedly) nobody can break into. However, every day we find new evidence that this is not true. What we need is depth defense that may allow the bad guys in, but all of our information is protected by strong encryption so little damage is done. Regarding offensive capabilities, we are not talking just about taking down somebody's power grid, we need to be considering how to use our great media howitzers to get the story across that will win.

David and I would recommend that we fill in the framework broadly as follows:

	General Posture	Defensive Measures	Offensive Capabilities
Ideational Tenets	Development of noosphere, noopolitik, plus a RDA*	Guarded openness, no first use of SIW**	Discriminate swarming
Organizational Design	Interagency networks, hybrids with hierarchies	Public-private cooperation for information security	Coalition information-sharing and interoperability
Technological Applications	Wide diffusion of strong encryption; connectivity	Preclusive and depth defense architectures	SIW** measures; media broadcast capabilities
*RDA = Revolution in Diplomatic Affairs			
**SIW = Strategic Information Warfare			

Table 3. The Ideational Tenets and Associated Principles.

Across the ideational level, as I suggested earlier we need to explore the noosphere, this realm of ethics and ideas. Defensively, we need not only guarded openness, but the United States might find some benefits in a no-first-use statement regarding strategic information warfare (SIW) in order to reassure other countries. Offensively, we believe swarming will be the best doctrine.

Finally, we should consider some new and varied issues on the agenda. First, those that are defense-related:

• Defending the homeland against "cybotage."

• Elaborating behavior-based arms control. We are talking about behavior because we simply cannot control the technology any more with SIW.

• Operating in coalitions, projecting forces. These problems are immense. Disruption of our deployment schedules or air tasking orders could cause us a great deal of trouble.

• Coping with non-state actors, both civil and uncivil.

• Shaping a strategic information doctrine (SID). This is a change from the Single Integrated Operational Plan (SIOP).

Second are those that are community- and country-related:

• Constructing a globe-girdling noosphere, a global civil society that allows us to resolve many of our disputes with more peaceful means.

• Fostering a revolution in diplomatic affairs (RDA). This means building a diplomatic system that is not based on embassy edifices and putting the President on the front line of every diplomatic crisis.

• Developing a capacity for strategic swarming.

• Pressuring authoritarian rulers. The information revolution gives us quite a bit of leverage in places like Cuba.

• Settling high-risk conflicts such as Kosovo. Peace will come there not through a negotiated military settlement but through an agreement on some common future.

What we need for an information strategy then is a concept of operations for the 21st century. Lord Nelson, for

example, suggested new naval tactics that allowed his ships to concentrate on smaller parts of the enemy's navy and achieve a striking advantage. At Trafalgar and a number of other battles, he did just this. In the German concept of *blitzkrieg*, the tank, airplane, and advanced communications were conjoined to enable maneuver warfare. We need to get to this point in our thinking.

At present, there are more questions than answers. What issues get priority or provide us with the best leverage? Do the issues and the framework relate well? How much can reorganization alone accomplish? At least, shifting the current direction of our thinking seems advisable. The prevailing concept of operations has emphasized the technical and defensive dimensions, keying on U.S. vulnerabilities. The focus of the next concept of operations should be on ideational and organizational dimensions, and on opportunities to be proactive. This requires a great strategic shift in thinking that we hope will be evidenced in the next Presidential Decision Directive (PDD) on the subject.

To explain where we are today, let me return to Table 3. We are already implementing most of the defensive measures recommended (except the no-first-use statement), and we are utilizing most of the technological applications except for the diffusion of strong encryption. What is not getting done is thinking about the general posture, including the need for new, hybrid hierarchies. On the offensive side we are not doing well at figuring out how to share information with our most trusted allies. We are also not really considering offensive doctrine; we are stuck with the doctrine of Curtis LeMay, which was something along the lines of "nuke them into glass." What we would introduce is something a bit more discriminate, with strategic swarming allowing us to place our efforts where we need them.

Discussion.

Dr. Arquilla was asked to comment on four issues: the place of physical violence in this approach; the empowerment of nongovernmental organizations; information warfare attacks against the economy; and the outlook for success in devising a national information strategy given bureaucratic realities.

Violence and Strategic Information Warfare.

Violence does not go away. At the military level, the concepts that David and I have elaborated about cyberwar and netwar suggest that you can achieve your aims with a lot less destruction than you used to. We think you can avoid having to use annihilation or destruction to win, and that you can win with disruption. Violence is a key to terror and always will be, and my great fear is not that the cyber-terror threat will become real—though it is now a lot less than it is given credit for in official circles. My fear is that terrorists are learning how to become "informatized," and they are using information now openly available to guide and target their violent operations. Recently I was able to go on-line from my desktop computer and take virtual tours of U.S. military bases; I briefed this to some base commanders, and partly as a result that information is now off the Web. I see the terrorists using information in a variety of ways, most importantly as a tool for supporting their active combat operations because there is a lot of information out there. Secondly, I think terrorists are going to be increasingly using the Internet for fundraising. The Tamil Tigers have showed an ability to reach out to a large diaspora for material support. Those kinds of uses are what I am more afraid of than cyber-terror itself. Today the notion of using bits and bytes to bring whole systems down is very much exaggerated.

Empowerment of Nongovernmental Organizations.

Clearly in the case of the landmine issue, the Net was not the only resource out there. There was a lot of media coverage, and there was a lot of use of classic activist tactics. Aerial bombardment began with zeppelins dropping bombs on English pubs, and it took another 25 years for airpower to come to fruition as the defining force of 20th century conflict. In much the same way, I think the information revolution is now just getting on its legs in terms of civil activism. The case of the Zapatistas is interesting. It is clear that the Mexican government was influenced to end its military activities against them in part as a response to their use of information operations. In Burma, government behavior has been somewhat restricted because of Net-based activity. This is still at an early stage, and use of the Internet is not going to be effective every time. We need to be careful not to hype the capability, much like we have to be careful not to hype the threat of cyber-terror, either.

Strategic Information Warfare against the Economy.

I do not think the threat exists today, and it is not clear when it will. What we saw with the rise of airpower was two different viewpoints. One was that it would have an important effect on the battlefield, and it took about 25 years for that to happen. The other view of the early theorists was that airpower changed everything—you did not have to engage the enemy's field army to strike his homeland. For 85 years people have been trying to realize the potential of an independent striking force. I am afraid we are going to have a similar debate over information warfare that may last just as long. There are those who think we can bring the enemy to his knees simply through an information attack on his economic, political, and transportation infrastructures. Yet we built infrastructure that could withstand nuclear war—that is why we built the Internet. I think that information warfare is as doomed as

the early, grandiose expectations of airpower. However, I think information warfare can have strategic effects if used against militaries. Disruption of American deployments could make all the difference, especially if an opponent has limited goals and threatens the use of WMD after he has achieved his goals and before we can respond. Such fait accompli strategies may be enhanced by information warfare. I think that like airpower, information warfare is going to have its main effects on the battlefield and will cause homeland disruption, but it will never be able to obtain a state's political aims in a true Clausewitzian sense.

Strategy vs. Bureaucracy.

What we have is a dismal landscape of bureaucratic pulling and hauling. I see few opportunities to break through it. I have been looking at this issue for 10 years, and progress is only made slowly, and here and there. When I walk the halls of the Pentagon, the locus of world power, everyone I meet seems to think fatalistically that he can accomplish or influence nothing. So I think our greatest problem is sociological, in persuading people that they can make a difference in what they do. There are pockets here and there where people are trying to make a difference. We are beginning to get some interservice coordination, and a little bit of interdepartmental cooperation. The challenge in the years ahead of us is organizational, not technological. Unless we begin to develop some sense of loyalty to an entity greater than an individual service, or the State Department, or one of the other governmental actors involved, we are not going to move ahead. Ten years from now I do not know if we will yet have a real information strategy, although I am sure it will be an improvement on what we have now. We have enough of a cushion in the international arena right now that perhaps we can continue to muddle through for awhile.

SESSION 7:
THE U.S. MILITARY AND INFORMATION OPERATIONS

The aim of this session was to provide an overall assessment of the information revolution and its impact on the way U.S. military forces conceptualize, organize, and train for information warfare.

"Seizing the High Ground: Land Operations and Information Operations"

Lieutenant Colonel Michael L. Warsocki, U.S. Army Land Information Warfare Center

Imagine being a commander in ancient Greek warfare. You could not see what was happening very well, so you had to seize the high ground. For centuries we have thought that we could win the battle if we were able to see better. Information has evolved into another dimension of warfare. We have now gone to the limits of physical height (space), but the new "high ground" is information.

Information operations (IO) is an integrating strategy of actions taken to affect an adversary's decision cycle, information, and information systems while defending one's own information and information systems. Physical security, psychological operations, deception, intelligence—IO encompasses all these things. The trick is to manage behavior through perception management. We want to modify the enemy's perception of the situation and change his behavior, to get into his decision cycle and influence it.

The older concept of command and control warfare (C2W) is the antecedent to IO. C2W was focused on the last two parts of Colonel John Boyd's notion of the OODA loop (Observe, Orient, Decide, and Act). We figured that if we

could impact the information that the enemy's decision-maker was getting, he would make bad decisions or give bad orders to execute them. This was seizing the high ground to create an advantage. It was not always easy to execute this kind of warfare, but it had the advantage of using force or kinetic energy, which we had plenty of. That does not work when you are in a peacekeeping situation, where force is impermissible, and we are doing that more and more.

Offensive information operations are centered on attacking the enemy's most vulnerable points. If we can create a situation where the enemy is giving orders and counterorders to the point that he is completely confused and all we have to do is come onto the battlefield and clean up, that is effective information operations. Think of police actions. A policeman can be dressed in a variety of ways, from McGruff the crime dog to kinetic energy-SWAT team guys that break down your door. The ultimate means of behavior modification is a bullet in the head, and that is what the military is good at. But that is not the first choice any more. The military has to figure out how to get into the unobservables: the willpower, perceptions, and situational awareness of the enemy's decision cycle.

Defensive information operations occur not just in the cyber-world, but on television, and in places like Bosnia and Somalia. By the way, the poor defenseless Albanians we saw on TV were also running black market operations, and we were confused as to what to do with them. They were successfully attacking our information systems.

The goal of information operations is to buy time. When chased by a bear you only have to be faster than the guy behind you. Strategically, I do not need to win the world, just buy time. Get a commander more time by condensing his decision cycle or disrupting the opponent's, and he now has command of a new dimension of warfare. The battlefield can be peacekeeping or anything, but time is the critical piece of the puzzle.

The threat is anything that counters my plan, whether I am a businessmen, politician, soldier, or what have you. I have a plan, and defense is strong but offense is decisive. If someone has a plan countering mine, that has to be disrupted or delayed. An election campaign is an example of information operations interfering with the other side's plan. When I am a peacekeeper, the opponent is anyone who opposes my plan; it could be an NGO, an ally, or the enemy, and you deal with each differently.

The threat is also likely to be asynchronous and asymmetrical. The next time we go to fight we may not have 6 months to prepare our logistics, and we may be attacked asynchronously to disrupt our debarkation points, our bases, our supply and logistics net. There was a joke that went around in Bosnia about how to stop a NATO air strike: get five Canadians and handcuff them to the target. That's asymmetry. You do not need military power if you can get into the enemy's decision-making cycle by using the news media, and that is getting easier all the time thanks to television. In Serbia, Dutch footage of a U.S. helicopter going down with no bullets fired (it had clipped a high power wire) forced us to waste a week having to respond to it.

We are likely to face some changing threats, including the actors I would call "mugs, thugs, and wackos," who are getting more creative and adaptive. We are going to be dealing with social fabric issues with implications for policy, such as black markets, multinational areas, and criminal elements. For example, the Kosovo Liberation Army (KLA) was supposed to be protected by U.S. forces, but we did not know what to do with the Albanian black market that cropped up. It was not our policy to fight it; the rules of engagement were not clear.

There may be larger threats, as well, like the Chinese. A Chinese military document from June of 1999 titled *On New Warfare* outlined new principles of war which must be directed against the United States. It suggests the use of all means possible, including armed force and nonarmed force,

and lays out eight laws for a secure strategy, including asymmetric, omni-directional, nontypical, flexible attacks. The Chinese are talking like they are at war, at least a reconnaissance war, and we need to do what we can to stop the reconnaissance.

This is not new. As far back as 1959 it was argued that the point of war is not to kill the enemy but to make him do what you want. What has changed is that information is now so ubiquitous that I can reach behind my opponent's front line and attack his systems through information operations. So how does the Army deal with this?

Information Operations.

The planning principles of information operations are knowledge and synchronization. We need to know the target audience—at home, in allied countries, or in the opposing country. There are a number of principles, but the key is synchronization, getting people moving like a football team where everyone is working together and doing their individual jobs. This is easier said than done.

There are some processes in information operations that are worth exploring. We face a variety of crises, campaigns, and routine tasks, so we have coordination cells to vet problems, to put together a plan and get down to the level of executable tasks. These include a whole series of intelligence and civil affairs activities: community relations, working with nongovernmental organizations (NGOs), giving instruction to local police forces, and working with the media. The G-5 has to do the job of a real politician in working with the NGOs, but he has to stress that we need their cooperation because we are not just there to protect the NGOs.

What does the Information Operations Working Group (IOWG) do? It assists the IO staff officer plan, coordinate, and implement the IO campaign. Sometimes there is a

question of who it is working for—the commander, the decisionmakers, or itself; it depends on the situation.

The key is orchestration of all these things. A lot of things are happening all at once, but they all have their own rhythms and cycles, and it is difficult to coordinate them. There is a lot of friction in this process. You have to get down to the nitty gritty details, by day and by month—press releases, plans, etc. People's perceptions are often shaped by how well you manage the day-to-day implementation problems.

Intelligence support in this process is crucial. There is a lot of information coming in, and synchronization of it all becomes important because the enemy may exploit it if you do not. There are lots of data out there, but we have to coordinate and share that knowledge. With some new databases like Oracle we can dump in both structured and unstructured data and turn the computer to the task of making sense of it. The trick is to take a lot of disparate databases and pull out of that haystack the needles that are truly useful.

One of the tools we are using to do this is called Themescape—we take lots of data, put it on the web, and bring out the themes. We take the information and use it to create connections between concepts or individuals, to visualize these in three dimensions, and bring out similarities and relationships among databases which may reveal to us a center of gravity that we should target.

How does the Army put all of this together? Until recently, this was not possible. We have opened what we call the Information Dominance Center, which is a central facility where teams from around the world can connect with us and work on coordinating information operations. Here we can bring together the entire execution of IO, including feedback and putting all the pieces together.

In conclusion, we need to know what IO can really do. The main goal is seizing the high ground of time, timely

information being so vital. Short-term IO modifies behavior, mid-term IO changes attitudes, and long-term IO changes deep-seated beliefs. The point is that we need to have realistic expectations about what IO can do for us. IO is not a silver bullet, but it can be an enormous help in avoiding the need to use lots of bullets.

"New Approaches to Information Warfare"

Lieutenant Colonel Charles Ayala, U.S. Air Force

I am not going to outline the ways in which the Air Force tries to do the kinds of things Colonel Warsocki has just described, because there is a lot of commonality with the Army approach. I spent a year as a National Defense Fellow at the University of Pittsburgh to encourage out-of-the-box thinking about information warfare (IW), and I want to share with you some of the ideas I encountered during that year that I am bringing back to the Air Force in the hope of shaping the debate further.

The rationale for studying information warfare is that information is the key to situational awareness for the airman and to the command and control of airpower As the country comes to rely more and more on airpower, we need to be looking at this from a variety of angles. Now within the Air Force, IW is very fragmented. All kinds of specialties have a piece of it, from the traditional computer geeks, to the intelligence people, communications and electronic equipment experts, the security folks, education and training teams, and public affairs specialists. In the Air Force, all the camps are contending for their slice of the budget, over what part of IW they can gain control.

Broadly, what I want to cover includes understanding the nature of IW, picking a definition of it, and finding some alternative approaches to IW.

Understanding the Nature of IW.

IW is much more than just the interesting features of the Internet. There are 165 million users on-line, and more than 800 million pages on the web. But more than just the statistics, the bottom line is that the Internet is about money—e-commerce already generates more than $200 billion a year. IW is also about changing technology. Data transfer rates and volume have grown exponentially, while the number of soldiers needed to cover an area has shrunk, and there are all kinds of new tools available.

There are a variety of IW definitions outside the Department of Defense, and most of these focus on asymmetry. The military service definitions are typically action oriented.

Now we do face a significant threat from nation-states, but we also face substate threats: first, widespread and validated (by the Defense Sciences Board)—incompetents and amateurs, hackers, disgruntled employees including military personnel, and crooks. Unhappy employees are really a big problem. The second type of substate threats are validated but limited, such as organized crime, foreign espionage agents, and enemy proxies. The last type of substate threat includes those whose existence is deemed likely but has not been validated, such as political dissidents and terrorists. We have found actors like Osama Bin Laden using laptops, but we are not sure what the uses are. Again, these substate threats are dynamic and moving, they are not static. When you group all of the threats together and consider the probabilities and consequences, the vectors are moving increasingly towards both.

Now IW can be carried out at all levels of understanding. As suggested earlier, it is true that the next time we are not going to get 6 months to prepare. However, we also have to be concerned with others who will give us 10 years—they will take a more strategic approach.

Choosing a Definition of Information Warfare.

Existing approaches are oriented toward process or a concentric ring model, where we try to create system paralysis in the enemy by hitting his centers of gravity all at once. The Air Force strategy is operational risk management—everything we do in the military is inherently dangerous, but we do not stop because it is dangerous, rather we try to manage the risk. This concept of risk management has proven successful in flight operations, and it is being applied by the Air Force to networks and to how we deal with the media.

I would propose a modified definition of information warfare, which is to take "war" out of "information warfare." Let me explain by breaking it down further. Information is defined as text that answers the prerogatives of who, when, what, and where; knowledge is text that answers the questions of how and why. Text is a stimulus for those of us who have sight, but we need to modify the traditional definition to include stimuli of all the senses, not just sight. War is stimulating the senses in a violent way. What if we could create the reaction we desire while using nonviolent stimuli?

In looking for a better definition of IW, I have come across several new approaches that are worthy of mention. First, the approach taken by academics at King's College in London (what I call a "Scotland Yard" approach) is based on crime. They emphasize understanding the organization, capabilities, motive, and objectives of the opponent, then taking a matrix and applying a network analysis. This does not require a lot of sophistication, but it is a disciplined approach involving categorization and linkage that may be useful to the military for determining what we want to do with IW.

Second, the Bulgarian military's general staff approach is OODA loop derived, the goal being to reduce uncertainty. Their notion is that information warfare is an oxymoron—

there is no war if you are doing the information part correctly. This is truly out-of-the-box thinking for the Air Force, and it is dicey because it throws responsibility for IW down to the level of the individual soldier or airman. Ultimately this may push the issue into the civilian sector and away from the experts in violence management.

The third approach is the Massachusetts Institute of Technology "Oxygen System." The idea here is that information is like oxygen—we all need it, and even after being used it recycles itself. This is a useful model because of its ease of use, transparency, and criticality.

Finally, the People's Republic of China has come up with the notion of setting up a fourth branch of its armed forces to do information warfare. This reflects a different viewpoint and more fundamental Chinese thought based on Sun Tzu and the idea of *chi* or wisdom—a different way of thinking about the whole process. It deals in the realm of chaos—creating order out of a disordered situation.

These new slants on information warfare have serious implications for how we organize, train, equip, operate, and maintain our forces. Sometimes the Air Force has undergone change for the sake of change, but these are fundamental changes that we cannot avoid.

• We will need changes in how we *organize*, through increased teaming. The Air Force tried a Total Quality Management (TQM) approach in the Air Combat Command, and took the sortie rates of poor teams and brought them up dramatically.

• We will have to *train* differently, using things like collaborative, computer-based training, video teleconferencing, and distributed learning. We will train soldiers to their task, to the language required, to the cultures they will need to know.

• We will *equip* soldiers in new ways, issuing technology to the lowest echelons. We are just starting this process. Every cadet at the Air Force Academy now receives a laptop,

whereas they used to be given a slide rule or calculator. In the future we will give everyone Palm Pilots or similar technology, so that soldiers and airmen will become familiar with the technology from the very beginning.

• How we *operate* will be changed. We will need to move to a more relaxed structure, a so-called "skip echelon" where the boss does not mind going around the system. Communications will take on special value, and we will have to emphasize individual accountability and a back-to-basics approach.

• Finally, we will have to alter how we *maintain* our forces. We are already going to more modular designs which can incorporate commercial, off-the-shelf technologies. Eventually we will supplement most high-cost upgradable equipment with low-cost throwaway equipment.

Let me conclude with three ideas. The threat of IW is real but distorted. We are usually focused on the systems and the medium, and we are not paying enough attention to the content. Alternative tools and models do exist outside of the military, and they need to be considered more fully. And finally, the potential exists for decreased, instead of more efficient, violence.

Discussion.

The panelists were asked to comment on two ideas. First, it was suggested that the concept of "chaorder," a mixture of chaos and order, is reflected in the blurring of distinctions among war, crime, terrorism, social protest, black markets, etc. This creates new policy dilemmas, yet the military still seems to be training for the old paradigm. Second, it was offered that the military operates only where directed by civilian authorities, yet those authorities are more and more removed from the reality of the military. The military may have to take a more active role in informing the civilian authorities just what it is capable of doing.

Training for the Old Paradigm.

Colonel Warsocki: Training is indeed critical. The Command and General Staff College at Fort Leavenworth wants to talk about IO, but the reality is that this is not what we train people to do. Now what they are getting is lots of information with some kinetic energy—training people to be police and handle situations first before resorting to violence. The good news is that the new generation of leaders has been in Bosnia and learned how to deal with the locals and the media. They are learning from the school of hard knocks rather than formal training. The learning curve was steep in Bosnia, and the learning was not institutionalized, but for better or worse we are learning the hard way. This may not be happening doctrinally at the Joint Readiness Training Center, and the schools are still not ready to teach it, but everyone is learning it.

Colonel Ayala: In the Air Force we are training for the future, but not enough. At the Air Command and Staff College and the Air War College, information has been taught as an instrument of power at least since the time of the Gulf War. So many officers are learning about it, although a lot of officers do not have the opportunity to go through these schools. Many on the enlisted side are getting it in their leadership schools. However, it is still not far enough. I would add that as the Air Force is standing up the Expeditionary Air Force with all its new packages and coordination issues, the process has caused a good bit of confusion, but I think we are moving in the right direction.

Civilian Control of the Military.

Colonel Ayala: I think the civilian population may be getting out of touch, perhaps because people do not serve any more and we no longer have a draft. At the same time, we are an all-volunteer force, and what we do is instantaneously on TV. It is one thing to see it on TV and another to serve. What could be done? We need to bridge that gap somehow, maybe through the reinstitution of the

draft or some kind of national service. What is important is that citizens be familiar with the forces that guard our way of life. Second, politicians do have to point us in the right direction, but the situation now is such that even the regular airman or soldier is the contact point where the military interacts with the media and the public. Cockpit voice recordings are used to get a message across about our honesty and truthfulness in admitting mistakes, and others are sharing in that pilot's hectic experience but judging it publicly after the fact. You cannot time it or manage it; it is not going to be as orchestrated as a press conference by the commander.

Colonel Warsocki: The fight is on today, and the military has to get engaged early. There are questions about overreaching the bounds of military structure, but we are in whether we like it or not. Now how do we fix this? One, policy-makers need to be intellectually honest. Take the example of the Kosovo Liberation Army and how policy-makers like Secretary of State Madeleine Albright and then-Assistant Secretary of State Richard Holbrooke became emotionally involved with the Kosovar Albanians. There was a degree of disingenuousness about the Albanians being our "friends." The Albanians wanted the world's best air force to support them, so they engaged in a campaign that was orchestrated to bring the United States into the fight. Factual intelligence on the ground made no difference to the policy-makers. Intellectual honesty has to take over from emotional language.

Dr. Metz: The military realizes it needs speed, not just in mobility but in operations, before the enemy gets there. The problem is that we are moving toward a fast military but we still have a slow-moving political system. It is a good thing that politics takes a long time, because we need consensus in a democracy. However, wargames we have conducted at Carlisle (at the Army War College) reveal the real tension between a quick military and the slower executive branch decisionmaking process. We are going to continue to see a tension between these speeds.

Colonel Warsocki: An example of that tension occurred when the Army crossed the Sava River into Bosnia. The Army got calls from the National Security Council on down asking what we could do about the situation in Sarajevo. The answers went up and down the chain, but it ultimately came down to what was politically acceptable and physically doable. We settled for taking the airfield. The determining factor was what politics would accept, rather than what was needed, and this put soldiers' lives at risk.

U.S. ARMY WAR COLLEGE

Major General Robert R. Ivany
Commandant

*****

STRATEGIC STUDIES INSTITUTE

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Earl H. Tilford, Jr.

Editor
Mr. Thomas E. Copeland

Director of Publications and Production
Ms. Marianne P. Cowling

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Mrs. Christine A. Williams

Cover Artist
Mr. James E. Kistler