NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Number 46, September 1995

Defining Civil Defense in the Information Age

by W. Oscar Round and Earle L. Rudolph, Jr.

Conclusions

1. With the advent of the information age the United States has lost the "sanctuary" that it has enjoyed for over 200 years. In the past ordinary citizens and businesses could be protected by control of the airspace, land, and the seas. Now an attack may be launched directly against a citizen passing right through (or around) all our traditional lines of defense.

2. The environment for developing and implementing national security policy is neither designed nor equipped to deal with events resulting from sources not rooted in the temporal or physical restrictions of the past.

3. Today's interagency approach to national security is not compatible with the speeds of the information age. Current government and civil institutions led by the Federal Emergency Management Agency (FEMA) are not designed to deal with attacks and natural disasters that move at the speed of light, crossing geographic and legal boundaries with impunity.

4. The National Security Council (NSC) needs to define the boundaries that separate technology-based attacks that are merely a nuisance from those that constitute national security threats.

The Emerging Threat

We have entered an era of immense global change and we must recognize that protection of the public during domestic emergencies has taken on new meanings with new consequences. A new process needs to be developed that defines the specific responsibilities of federal and state governments for

technological disasters.

The DOD has taken the initiative and has established new educational and training programs focused on Information Warfare and Strategy, Command and Control Warfare, and Information Operations. But solutions to the problem are larger than the DOD and other organizations must be engaged. Issues involving information technology, national security, and civil defense cross many if not all of the traditional governmental boundaries thus ultimately requiring a truly holistic solution.

Vice President Al Gore's announcement of a National Information Infrastructure was a harbinger of things to come rather than a fait accompli. Economic and public policy theorists widely tout the emergence of a "Global Economy," with its components inextricably linked as result of rapidly advancing communications technology. The nature of these linkages will help define economic, diplomatic, and military relationships well into the next century.

Modern societies (particularly the United States) increasingly rely upon the kind of information infrastructures that have enabled the emergence of the Global Economy. Infrastructures that do not and cannot stand alone but by their very nature must remain interconnected to function and survive are the dominant features of this new economy. The international banking and telecommunications industries are two obvious examples of vital internetted global systems that are essential for day to day governmental and commercial operations.

Both the public and the private sectors have been slow to acknowledge and deal with information age deliberate attacks, unintended consequences, accidents or natural disasters. The fact that hackers have gained access to sensitive government and commercial computer systems is common knowledge with small cults developing around some of the more charismatic. While steps have been undertaken to develop greater security for these systems, timely detection of intrusions and effective responses have yet to be achieved. Recent instances of service interruption affecting electrical grids, air traffic control and financial transfer systems have been interpreted by some as a warning of impending disaster resulting from the very linkages among our systems previously heralded as the key to progress.

Leveling the Field

Underlying this worldwide expansion in communications and computer networks is a global technological leveling that already draws theorists to discussion of information age battlefields consisting of databases, financial networks, as well as manufacturing and service centers. Because the private sector is leading the development and marketing of information age technologies, this technological leveling has accelerated as emergent technologies are made available to anyone with sufficient resources.

Unlike the vigorous policy deliberations regarding Nuclear, Biological and Chemical (NBC) threats from Nation-states and terrorists there has been precious little public debate on the ramifications of the information technological explosion on national security. Several questions need to be addressed relating the potential of the information age and its impact on national security.

In the national security community there is a growing awareness of the impact that the rapid advances in technology, specifically information technologies, are having on the definition and character of national security. As nation-states, and non-governmental organizations come to grips with the global technological leveling, they are beginning to understand that new national and international legal structures are necessary. The fact that physical, cultural and social boundaries may be crossed with relative impunity and that industrial capacity and population may no longer be the essential determinants of national power necessitate new governmental architectures and mechanisms.

Attacks on the United States and its information infrastructure, be they part of a larger conflict, state-sponsored terrorism or merely electronic mugging, can now be mounted without regard to the physical boundaries on which we have relied for over 200 years. We have been slow as a nation to realize that the temporal and geographical sanctuary that the US has always enjoyed has been lost. The sense of sanctuary lost, of personal privacy denied, and of a collective public safety at risk, has been reinforced by such diverse events as the Oklahoma City and World Trade Center bombings, the collapse of a British bank due to actions of a single trader resident in Singapore, amid the growing awareness of the "hacker/cracker" community's ability to penetrate and manipulate data.

In the aftermath of these events we should expect a rigorous examination of the way the federal and state governments need to reorganize and redefine themselves in response to the threats and opportunities presented by the emerging environment of the Information Age.

Status Quo

Currently the United States Government has established mechanisms to respond to a variety of national emergencies, including: natural disasters, terrorist attacks, and full scale military mobilization. As demonstrated in Hurricane Andrew, the California earthquakes and fires, and numerous other events, the DOD, federal and state governments have devised means (however imperfect) to cooperatively deal with catastrophes of varying magnitudes and types. For the federal government, organizational responsibilities are codified in the Federal Response Plan. The Department of Defense's role is spelled out in the DOD Manual for Civil Emergencies (DOD 3025.1-M). Within these directives, responsibility for coordination and direction resides largely with the Federal Emergency Management Administration (FEMA). The potential for a disaster or attack specifically related to the emergent technologies of the "Information Age" increases daily as the United States becomes more and more dependent upon, and thus vulnerable to, the vagaries of the Information Superhighway. Yet the Emergency Support Functions (ESF) that are assigned to lead agencies for contingency planning and response coordination contain only the briefest discussion of "technology emergencies." Current legal, cultural, and organizational establishments, intended to deal with threats to national security and civil emergencies, are also inadequate in light of the pace of technological change.

The gamut of legal issues range from individual's privacy to organizational and commercial intellectual property rights. Within the United States, personal and/or organizational privacy is at risk because of a lack of definition regarding the system of legal protocols, and sovereign boundaries in the infosphere.

The difficulties of melding the spectrum of nation-state national security policies into a codified system of new international law are not trivial. The historical experience with crafting international law to regulate commerce and the difficult undertaking to establish international standards does not augur well for a speedy resolution of these issues. If international agreements are not reached, nation-states may well be bypassed by the wealth-creating potential of the information age. Therefore, nations must begin now to work diligently to create a cohesive set of international information agreements. These protocols would eventually become a "law of the infosea" that evolves over time to establish an acceptable level of structure and cohesion to the medium without unduly inhibiting commercial or individual initiative.

The resolution of the legal and organizational issues are indelibly tied to a society's culture. The American public's aversion to what it considers intrusive governmental oversight has been the basis for active and sometimes violent protest throughout our history. The nature of our democracy is to be reactive rather than proactive to change (ie., seeking a broad consensus). Conversely, our free-market enterprises must be proactive in order to flourish. As a result, tensions resulting from the volume, detail, and transferability of information widely available concerning any organization or individual will ultimately motivate changes in both the legal and organizational climate.

The interagency process, which supports the National Command Authority in employment of the National Security Strategy is not well organized to deal with new "technology-based threats. Within the government, agreement as to what constitutes the actionable threshold between nuisance attacks and threats to the national security need to be defined and a robust response plan established. Assignment of a lead agency with adequate capability to meet the security demands posed by the evolving techno-threats would be a first step in building a viable Federal Response Plan.

The Next Step

Given the broad spectrum of potential impacts on the nation, there exists a pressing need for a non-partisan federal commission to address the legal, cultural, and organizational issues raised by the prospect of Information Warfare. As governments, businesses, and individuals gain increasing access to, and begin to use, and potentially abuse, the capabilities provided by the new technologies it is imperative that our legal systems be updated and that our current governmental arrangements be adapted so that a viable Civil Defense structure for the future can be developed. Failure to attain a bipartisan consensus may well make impossible for the US to prevail in a conflict that begins as an Information War.

Currently the structure of the Federal government is undergoing review as part of the Vice Presidents "reinventing government" initiative. This effort offers an excellent opportunity to bring the Disaster Response and National Security Policies in line with the technological advances of the revolution in information technology. As part of this study a wide ranging review of the functions of the fed-eral and state agencies and their respective roles in a new Civil Defense structure should be completed to assure the ability to respond on all fronts to techno-logy-based disasters. Now is the time to look at the emerging threats and response options precipi- tated by the compression of the technological advances.

The pace and complexity of change continues to accelerate with entire generations of computer systems becoming outdated every 18-24 months. We are presented with an environmental change that is impacting National Security in the broadest sense demanding a coherent response. Two broad alternatives present themselves for immediate consideration:

1. *Laissez faire:* Allow current mechanisms and policies to continue to deal with individual instances. It is possible, given time, that today's bureaucracies would self organize, forming a protective system as threats and vulnerabilities evolve. The govern- ment, by allowing the commercial sector to lead, would be relying on economic interest to force innovation with the protection of national security as a byproduct. This view is the argument that perhaps it is too early in the game to raise the significance of the information revolution to the national security level.

2. *Seize the Initiative:* Develop the appropriate areas of the Federal Response Plan by clearly identifying and funding a lead agency. While the DOD has a certain degree of discipline, organizational structure and experience dealing with classified information systems the military vulnerabilities are only a segment of the issue. Thus a new set of roles and missions need to be addressed with the various agencies and departments of government to clearly address the broader requirements of a National Security Strategy in order more narrowly resolve the questions of a Civil Defense.

Recommendations

1. Seize the initiative to force corporate thinking at the senior policy development level.

2. Initiate an Interagency meeting as the departure point for future action with respect to policy development.

3. Establish a bipartisan commission with the charter, authority and funding to codify national response to the information age threats.

About the Authors

Commander Earle Rudolph USN (Ret), is a former professor of information warfare and strategy at the Information Resources Management College School of Information and Strategy (SWIS). Captain W. Oscar Round is currently the Director, Center for Advanced Concepts and Technology (ACT) at the Institute for National Strategic Studies. For additional information, Cmdr. Rudolph can be reached at (703) 360-5327 or e-mail erudolph@erols.com and Capt. Round can be reached at (202) 287-9210 x545 or email roundw@ndu.edu.

NOTE

|Return to Top | Return to Strategic Forum Index | Return to Research and Publications |