The US Army War College Quarterly: Parameters

Volume 26
Number 3 *Parameters Autumn 1996*

Article 12

8-21-1996

Strategic Information Warfare: A New Face of War

Roger C. Molander

Andrew S. Riddile

Peter A. Wilson

Recommended Citation
Roger C. Molander, Andrew S. Riddile & Peter A. Wilson, "Strategic Information Warfare: A New Face of War," *Parameters* 26, no. 3 (1996), doi:10.55540/0031-1723.1794.

Strategic Information Warfare: A New Face of War

ROGER C. MOLANDER, ANDREW S. RIDDILE, and PETER A. WILSON

From *Parameters*, Autumn 1996, pp. 81-92. .

> "We live in an age that is driven by information. Technological breakthroughs . . . are *changing the face of war* and how we prepare for war." --William Perry, Secretary of Defense

Information warfare (IW) represents a rapidly evolving and, as yet, imprecisely defined field of growing interest for defense planners and policy-makers. The source of both the interest and the imprecision in this field is the so-called information revolution--led by the ongoing rapid evolution of cyberspace, microcomputers, and associated information technologies. The US defense establishment, like US society as a whole, is moving rapidly to take advantage of the new opportunities presented by these changes. At the same time, current and potential US adversaries (and allies) are also looking to exploit the evolving global information infrastructure and associated technologies for military purposes.

The end result and implications of these ongoing changes for international and other forms of conflict are highly uncertain, befitting a subject that is this new and dynamic. Will information warfare be a new but subordinate facet of warfare in which the United States and its allies readily overcome their own potential cyberspace vulnerabilities to gain and sustain whatever tactical and strategic military advantages might be available in this arena? Or will the changes in conflict wrought by the ongoing information revolution be so rapid and profound that the net result is a new and grave threat to traditional military operations and US society that fundamentally changes the future character of warfare?

In response to this situation and these uncertainties, in January 1995 the Secretary of Defense formed the IW Executive Board to facilitate "the development and achievement of national information warfare goals." In support of this effort, RAND was asked to provide and exercise an analytic framework for identifying key IW issues, exploring their consequences and highlighting starting points for related policy development--looking to help develop a sustainable national consensus on an overall US strategy for information warfare.

To accomplish this purpose, RAND conducted an exercise-based framing and analysis of what we came to call the "strategic information warfare" problem. Involving senior members of the national security community as well as representatives from national security-related telecommunications and information systems industries, the exercises led participants through a challenging hypothetical IW crisis involving a major regional political-military contingency. The exercise methodology, known by the label "The Day After . . . ," had been previously used for a variety of nuclear proliferation, counterproliferation, and related intelligence studies. The specific scenario chosen for the exercise involved a turn-of-the-century conflict between Iran and the United States and its allies, focused on a threat to Saudi Arabia.

The exercise was conducted six times in evolving versions over the course of five months from January to June 1995. Each iteration allowed for refinement of basic strategic IW concepts and provided further insights about their national security implications. This process provided an opportunity to assess and analyze the perspectives of senior participants from government and industry regarding such matters as the plausibility of strategic IW scenarios such as the one presented, possible evolutions in related threats and vulnerabilities, and the phrasing of key associated strategy and policy issues. It also provided an opportunity to identify emerging schools of thought and, in some cases, a rough consensus on next steps on a number of important strategic IW issues. In addition, the process yielded a badly needed multi- dimensional framework for sharpening near-term executive branch focus on the development of strategic IW policy, strategy, and goals--in particular regarding the implications of prospective major regional contingencies on defensive IW strategies, doctrines, vulnerabilities, and capabilities. It also provided a very useful forum for beginning to coordinate with industry on the future direction of IW-related national security telecommunications strategy.

As can be inferred from the foregoing, the methodology employed in the study appears to offer particular advantages for addressing many of the conceptual difficulties inherent in this topic. The subject matter is new and, in some dimensions, technically complex, especially for individuals typically found in policymaking positions. The challenge of finding techniques for accelerating efficiently the process of basic education on the topic and its implications for national security policy and strategy cannot be overstated.

This article summarizes the results of the study. It:

- describes and frames the concept of strategic information warfare
- describes and discusses the key features and related issues that characterize strategic IW
- explores the consequences of these features and issues for US national security as illuminated by the exercises
- suggests analytical and policy directions for addressing elements of these strategic IW features and issues

What is "Information Warfare?"

Ten years ago the answer to that question from a communications specialist, a codebreaker, or any other member of the US military or intelligence communities might have been either "What?" or, with a little encouragement, "Oh, you mean command and control warfare on the battlefield and in the theater, jamming and that other electronic warfare stuff." Within most of the US defense community today, you would still get an answer not far different from the preceding definitions of command and control warfare (C2W) or electronic warfare (EW).

In many circles within the US defense and broader international security community, however, the term information warfare is increasingly being used to encompass a broader set of information-age "warfare" concepts. These emerging new warfare concepts are directly tied to the prospect that the ongoing rapid evolution of cyberspace--the global information infrastructure--could bring both new opportunities and new vulnerabilities. The study focuses on one of these vulnerabilities: the prospect that this revolution could put at risk high-value national assets outside the traditional battlefield and theater of "over there" power projection in a fashion that affects both US national military strategy and broader US national security strategy.

We recognize that for some time the term information warfare in common usage will have no more than a general meaning, one that is recognized to be inescapably dynamic. Information warfare, like the evolving term "strategic warfare," is at a much too early stage of development to settle on an agreed definition for the concept.

However, we think there is an emerging element of information warfare--one that appears to be common to almost all currently evolving uses of this term--that warrants identification and definition. We have labeled this emerging realm of conflict, wherein nations use cyberspace to affect strategic military operations and inflict damage on national information infrastructures, as "strategic information warfare." As we have portrayed in Figure 1, we believe that strategic information warfare (in essence the intersection of evolving information warfare and post-Cold War "strategic warfare" concepts) warrants special recognition and attention as a legitimate new facet of warfare with profound implications for both US military strategy and overall US national security strategy.[1]

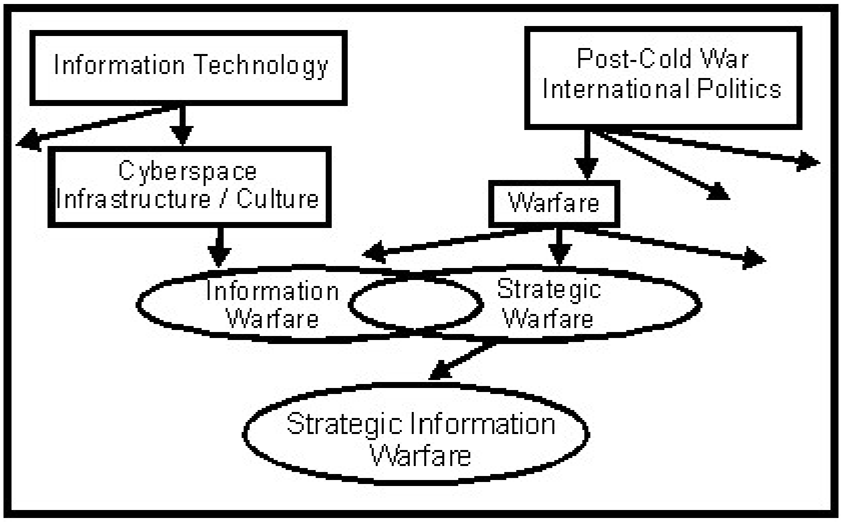
Information Technology
Post-Cold War International Politics
Cyberspace Infrastructure / Culture
Warfare
Information Warfare
Strategic Warfare
Strategic Information Warfare

Figure 1. Strategic Information Warfare

The new cyberspace infrastructure and culture depicted in Figure 1 has, in recent years, evolved almost exclusively outside the military context (although the contribution of the Defense Department's ARPANET to the origins of the Internet are well known). As argued elsewhere, the emerging elements and characteristics of cyberspace by their nature offer new opportunities for information warfare.

On a parallel track, there is the ongoing evolution in international politics, and within that context, the inevitable evolution of Clausewitz's warfare as an instrument of politics. In this context, new strategic interests are emerging for the United States and other nations, yielding new strategic dilemmas and new (and old) strategic targets against which to use leverage--including the threat of use of new (and old) kinds of strategic force. Thus, new strategic threats and new strategic vulnerabilities surface. It is increasingly clear, as this article seeks to portray, that the evolution in strategic warfare will include a dimension of cyberspace threats and vulnerabilities worthy of the label "strategic information warfare."

Strategic Information Warfare

The United States has substantial information-based resources, including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information-dependent items. US allies and potential coalition partners are similarly increasingly dependent on various information infrastructures. Conceptually, if and when potential adversaries attempt to damage these systems using IW techniques, information warfare inevitably takes on a strategic aspect.

Our exercise scenario highlighted from the start a fundamental aspect of strategic information warfare: There is no "front line." Strategic targets in the United States may be just as vulnerable to attack as in-theater command, control, communications, and intelligence (C3I) targets. As a result, the attention of exercise participants quickly broadened beyond a single traditional regional theater of operations to four distinct separate theaters of operation as portrayed in Figure 2: the battlefield per se; allied "Zones of Interior" (in our scenario, the sovereign territory of Saudi Arabia); the intercontinental zone of communication and deployment; and the US Zone of Interior.

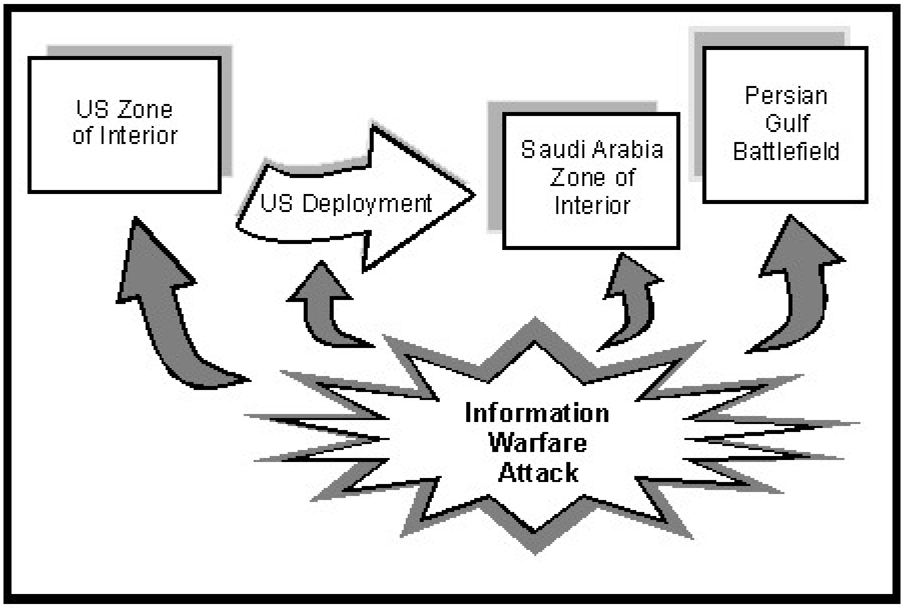

Figure 2. The Changing Face of War: Four Strategic Information Warfare Theaters of Operation

The post-Cold War "over there" focus of the regional component of US national military strategy incompletely describes this kind of scenario and is of declining relevance to the likely future international strategic environment. When responding to information warfare attacks of this character, military strategy can no longer afford to focus on conducting and supporting operations only in the region of concern. We now require an in-depth examination of the implications of information warfare for the US and allied infrastructures that depend on the unimpeded management of information.

The Basic Features of Strategic Information Warfare

The exercises highlighted seven defining features of strategic information warfare:

- *Low entry cost*. Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.
- *Blurred traditional boundaries*. Traditional distinctions--public versus private interests, warlike versus criminal behavior--and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure.
- *Expanded role for perception management*. New information-based techniques may substantially increase the power of deception and of image- manipulation activities, dramatically complicating government efforts to build political support for security-related initiatives.
- *A new strategic intelligence challenge*. Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. We may therefore have to develop a new field of analysis focused on strategic information warfare.
- *Formidable tactical warning and attack assessment problems*. There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage or accidents.
- *Difficulty of building and sustaining coalitions*. Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks, giving opponents a disproportionate strategic advantage.
- *Vulnerability of the US homeland*. Information-based techniques render geographical distance irrelevant; targets in the United States are just as vulnerable as in-theater targets. Given the increased reliance of the US economy and society on a high-performance networked information infrastructure, a new set of lucrative strategic targets presents itself to potential IW-armed opponents.

Through the course of our exercise-based analysis, policymakers and other experts from the public and private sectors were prompted to explore the character and consequences of these features. The discussion that follows summarizes our synthesis of observations made by the exercise participants on the characteristics and implications of these features for the strategic IW problem. Note that there is a "cascading" effect inherent in these observations--each helps to create the enabling conditions for subsequent ones.

Low Entry Cost

Interconnected networks may be subject to attack and disruption not just by states but also by nonstate actors, including dispersed groups and even individuals. Potential adversaries also could possess a wide range of capabilities. Thus, the threat to US interests could be multiplied substantially and will continue to change as more complex systems are developed and the requisite expertise is more widely diffused.

Some participants believed that the entry price to many of the IW attack options posited could be raised by denying easy access to networks and control systems through the exploitation of new software encryption techniques. Other participants acknowledged that this might mitigate some threats but emphasized that this approach would not remove other threats to an internetted system by a corrupted insider (systems operator), direct physical attack, or both. It also would increase the difficulty in developing intelligence related to strategic IW attackers at all three levels of concern: strategic, operational, and tactical.

Blurred Traditional Boundaries

Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to distinguish between foreign and domestic sources of IW threats and actions. You may not know who's under attack by whom, or who's in charge of the attack. This greatly complicates the traditional role distinction between domestic law enforcement, on the one hand, and national security and intelligence entities, on the other. Another consequence of this blurring phenomenon is the disappearance of clear distinctions between different levels of anti-state activity, ranging from crime to warfare. Given this blurring, nation-states opposed to US strategic interests could forgo more traditional types of military or terrorist action and instead exploit individuals or transnational criminal organizations to conduct "strategic criminal operations."

Expanded Role for Perception Management

Opportunities for IW agents to manipulate information that is key to public perceptions may increase. For example, political action groups and other nongovernment organizations can use the Internet to galvanize political support, as the Zapitistas in Chiapas, Mexico, were able to do. Furthermore, the possibility arises that the "facts" of an event can be manipulated via multimedia techniques and widely disseminated. Conversely, there may be a decreased capability to build and maintain domestic support for controversial political actions. One implication is that future US administrations may include a robust Internet component as part of any public information campaign.

Among participants, there was no support for any extraordinary maneuver by the government to "seize control" of the media and the Internet in response to a probable IW attack. Rather, there was an acknowledgment that future US administrations might face a daunting task in shaping and sustaining domestic support for any action marked by a high degree of ambiguity and uncertainty in the area of information warfare.

Lack of Strategic Intelligence

For a variety of reasons, traditional intelligence gathering and analysis methods may be of limited use in meeting the strategic IW intelligence challenge. Collection targets are difficult to identify; allocation of intelligence resources is difficult because of the rapidly changing nature of the threat; and vulnerabilities and target sets are not, as yet, well understood. In sum, the United States may have difficulty identifying potential adversaries, their intentions, and their capabilities. One implication of this is that new organizational relationships are needed within the intelligence community and between this community and other entities. A restructuring of roles and missions may also be required.

In the exercises, debate on this problem centered on the need for some interagency structure to allow for coordinated collection and analysis of "foreign" and "domestic" sources versus the desire to preserve the boundary between foreign intelligence and domestic law enforcement.

Difficulty of Tactical Warning and Attack Assessment

This feature of warfare presents fundamentally new problems in a cyberspace environment. A basic problem is distinguishing between attacks and other events, such as accidents, system failures, or hacking by thrill- seekers. The main consequence of this feature is that the United States may not even know when an attack is under way, who is attacking, or how the attack is being conducted.

As in the debate over what to do about the dilemmas posed by the strategic intelligence challenge, exercise participants split on this topic between those who were prepared to consider a more radical mixing of domestic law enforcement and foreign intelligence institutions and those strongly opposed to any commingling.

Difficulty of Building and Sustaining Coalitions

Many US allies and coalition partners will be vulnerable to IW attacks on their core information infrastructures. For example, the dependence on cellular phones in developing countries could well render telephone communications in those nations highly susceptible to disruption. Other sectors in the early stages of exploiting the information revolution (e.g., energy and financial) may also present vulnerabilities that an adversary might attack to undermine coalition participation. Such attacks might also serve to sever "weak links" in the execution of coalition plans. Conversely, tentative coalition partners who urgently need military assistance may want assurances that a US deployment plan to their region is not vulnerable to IW disruption.

There was general agreement among participants that as the United States develops and refines defensive systems and concepts of operations or techniques in this area, it should consider sharing them with key allies, but no specific policies were proffered in the discussions.

Vulnerability of the US Homeland

As noted earlier, information warfare has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the US economy will increasingly rely on complex, interconnected network control systems for such necessities as oil and gas pipelines and electric grids. The vulnerability of these systems is currently poorly understood. In addition, the means of deterrence and retaliation are uncertain and may rely on traditional military instruments in addition to IW threats. In sum, the US homeland may no longer provide a sanctuary from outside attack.

There was a broad consensus among exercise participants that no dramatic measures such as shutting down an infrastructure would be effective as a defensive measure (and some skepticism as to whether such action would, in fact, be possible during a crisis). There appeared, however, a broad consensus in favor of exploring the concept of a "minimum essential information infrastructure" based on a series of federally sponsored incentives to ensure that the owners and operators had procedures to detect IW attacks and reconstitution measures that minimized the effects of any one network disruption.

Conclusions--An Elusive Bottom Line on the Threat

Over the course of the exercise series, careful attention was given to the possible solidifying of a bottom line on the gravity of the cyberspace-based strategic IW threat. Many existing information systems do appear to be vulnerable to some level of disruption or misuse. At the same time, developments in cyberspace are so dynamic that existing vulnerabilities may well be ameliorated as part of the natural building of immunities to threats that accompany any such rapidly evolving entity. However, our dependence on cyberspace and information systems generally is also growing rapidly--raising unsettling questions as to whether the "immune system" process can keep up and thus prevent serious strategic vulnerabilities from emerging and being exploited.

We looked for, but did not find, any strong statistical consensus on just where people think we are now on the threat spectrum portrayed in Figure 3, or where we might be heading. We did observe, however, that over the course of the exercise, the general perspective on the magnitude of the strategic IW problem almost invariably appeared to move downward along the continuum of Figure 3. This experience mirrored that of the authors--the more time spent on this subject, the more one saw tough problems lacking concrete solutions and, in some cases, lacking even good ideas about where to start.

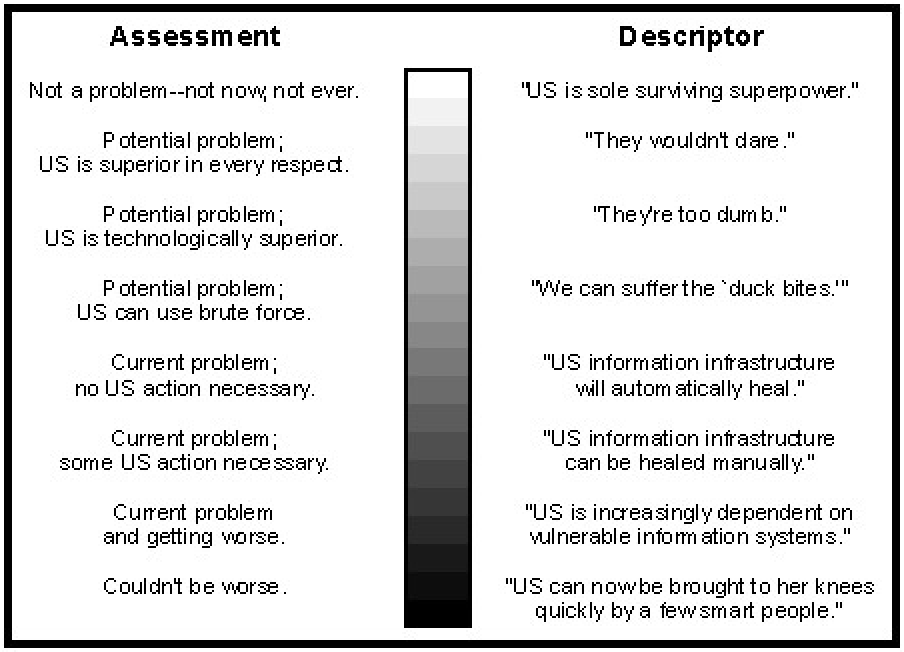
Assessment
Descriptor
Not a problem--not now, not ever.
"US is sole surviving superpower."
Potential problem; US is superior in every respect.
"They wouldn't dare."
Potential problem; US is technologically superior.
"They're too dumb."
Potential problem; US can use brute force.
"We can suffer the `duck bites.'"
Current problem; no US action necessary.
"US information infrastructure will automatically heal."
Current problem; some US action necessary.
"US information infrastructure can be healed manually."
Current problem and getting worse.
"US is increasingly dependent on vulnerable information systems."
Couldn't be worse.
"US can now be brought to her knees quickly by a few smart people."

Figure 3. A Broad Spectrum of Perspectives

The features and likely consequences of strategic information warfare point to a basic conclusion: Key national military strategy assumptions are obsolete and inadequate for confronting the threat posed by strategic information warfare. Five major recommendations emerged from the exercises as starting points for addressing this shortcoming:

1. *Leadership: Who Should Be in Charge in the Government?*

Participants widely agreed that an immediate and badly needed first step is the assignment of a focal point for federal government leadership in support of a coordinated US response to the strategic IW threat. This focal point should be located in the Executive Office of the President, since only at this level can the necessary interagency coordination of the large number of government organizations involved in such matters--and the necessary interactions with the Congress--be carried out effectively. This office should also have the responsibility for close coordination with industry, since the nation's information infrastructure is being developed almost exclusively by the commercial sector. Once established, this high-level leadership should immediately take responsibility for initiating and managing a comprehensive review of national-level strategic information warfare issues.

2. *Risk Assessment*

The federal government leadership entity cited above should, as a first step, conduct immediately a risk assessment to determine, to the degree possible, the vulnerability of key elements of current US national security and national military strategy to strategic information warfare. Strategic target sets, IW effects, and parallel vulnerability and threat assessments should be among the components of this review. In an environment of dynamic change in both cyberspace threats and vulnerabilities, there is no sound basis for presidential decisionmaking on strategic IW matters without such a risk assessment.

In this context there is always the hope or the belief--we saw both in the exercises--that the kind of aggressive response suggested in this report can be delayed while cyberspace gets a chance to evolve robust defenses on its own. This is, in fact, a possibility. The healing and annealing of an immune system that is under constant assault, as cyberspace is and assuredly will continue to be (if only, in Willy Sutton's words, because that's where the money is), will create the robust national information infrastructure that everyone hopes to use. But it may not. And we are certainly not there now.

3. *Government's Role*

The appropriate role for government in responding to the strategic IW threat needs to be addressed, recognizing that this role--certain to be part leadership and part partnership with the domestic sector--will unquestionably evolve. Obviously the government performs certain basic preparedness functions, such as organizing, equipping, training, and sustaining military forces. In addition, the government may play a more productive and efficient role as facilitator and maintainer of some information systems and infrastructure, and through policy mechanisms such as tax breaks to encourage reducing vulnerability and improving recovery and reconstitution capability.

An important factor is the traditional change in the government's role as one moves from national defense through public safety toward things that represent the public good. Clearly, the government's perceived role in this area will have to be balanced against public perceptions of the loss of civil liberties and the commercial sector's concern about unwarranted limits on its practices and markets.

4. *National Security Strategy*

Once an initial risk assessment has been completed, US national security strategy needs to address preparedness for the threat as identified. Preparedness will cross several traditional boundaries from military to civilian, from foreign to domestic, and from national to local.

One promising means for instituting this kind of preparedness could involve the concept of a "minimum essential information infrastructure" (MEII), which was introduced as a possible strategic defensive IW initiative in the exercise. The MEII is conceived as that minimum mixture of US information systems, procedures, laws, and tax incentives necessary to ensure the nation's continued functioning even in the face of a sophisticated strategic IW attack. One facet of such an MEII might be a set of rules and regulations sponsored by the federal government to encourage the owners and operators of the various national infrastructures to take measures to reduce their infrastructure's vulnerability, to ensure rapid reconstitution in the face of IW attacks, or both. The analog for this concept is the strategic nuclear Minimum Essential Emergency Communications Network (MEECN). Participants in the exercise found the MEII construct conceptually very attractive even though there was some uncertainty as to how it might be achieved. An assessment of the feasibility of an MEII (or like concepts) should be undertaken at an early date.

5. *National Military Strategy*

The current national military strategy emphasizes maintaining US capability to project power into theaters of operation in key regions of Europe and Asia. Because of the four emerging theaters of operation in cyberspace for such contingencies (see Figure 2), strategic IW profoundly reduces the significance of distance with respect to the deployment and use of weapons. Therefore, battlefield C3I vulnerabilities may become less significant than vulnerabilities in the national infrastructure. Planning assumptions fundamental to current national military strategy are obsolete. Consideration of these IW features should be accounted for in US national military strategy.

Against this difficult projection and assessment situation, there is the ever-present risk that the United States could find itself in a crisis in the near term, facing the possibility of, or indications of, a strategic IW attack. When the President asks whether the United States is under IW attack--and, if so, by whom, and whether the US military plan and strategy are vulnerable--a foot-shuffling "we don't know" will not be an acceptable answer. Finally, however, it must be acknowledged that strategic information warfare is a very new concept that is presenting a wholly new set of problems. These problems may well yield to solution--but not without the intelligent and informed expenditure of energy, leadership, money, and other scarce resources, expenditures for which we hope this article will be a catalyst.

NOTE

[1] See our more detailed report, also titled *Strategic Information Warfare: A New Face of War* (Santa Monica, Calif.:

RAND, 1996). The present article is drawn from the Summary and Chapter 1. The full text of the study is available at the RAND site on the World Wide Web. The URL address is:
http://www.rand.org./publications/MR/MR661/MR661.pdf

Roger C. Molander is a senior researcher with the RAND Corporation, focusing on information warfare and nuclear proliferation. Dr. Molander has served on the White House National Security Council staff, was CEO of the Roosevelt Center for American Policy Studies, and was executive director of Ground Zero, a nonpartisan nuclear war education project directed at the US public and media. He is also the coauthor of *The Day After . . . Study: Nuclear Proliferation in the Post-Cold War World*.

Commodore Andrew S. Riddile (USN, Ret.) is a RAND consultant working in the area of national security research.

Peter A. Wilson is a consultant with RAND and the Washington Institute, and has worked with the Institute for Defense Analysis, SAIC, the CIA, and the Department of State. He has coauthored several RAND reports, including *The Nuclear Asymptote: On Containing Nuclear Proliferation* and *The Day After . . . Study*.

Reviewed 21 August 1996. Please send comments or corrections to carl_Parameters@conus.army.mil.