
**U.S. STRATEGIC VULNERABILITIES:
THREATS AGAINST SOCIETY**

Roger C. Molander, Peter A. Wilson, and Robert H. Anderson

Previous chapters have discussed military opportunities and vulnerabilities arising from information operations and information warfare. But do information operations and warfare constitute a strategic threat to U.S. society? What, indeed, would constitute “strategic information warfare” (SIW)? In this chapter, we address these questions and present a framework for thinking about SIW issues.¹

WHAT IS SIW?

In the future, the possibility exists that adversaries might exploit the tools and techniques of the information revolution to hold at risk (not of destruction, but of large-scale or massive disruption) key national strategic assets, such as elements of various key national infrastructure sectors (energy, telecommunications, transportation, financial, etc.). This potential danger constitutes the principal fact of the SIW environment as conceptualized here.

Both regional adversaries and peer competitors may find SIW tools and techniques of use to them in challenging the United States, its allies, and/or its interests. In the near term, SIW weapons may be most useful to regional adversaries applying *asymmetric strategies* (See Figure 9.1) as a way to avoid directly challenging U.S. conventional battlefield superiority. Such strategies involve using some combination of nuclear, chemical, biological, highly advanced conventional, and SIW instruments.

¹This chapter is adapted primarily from Molander, Wilson, Mussington, and Mesic (1998).

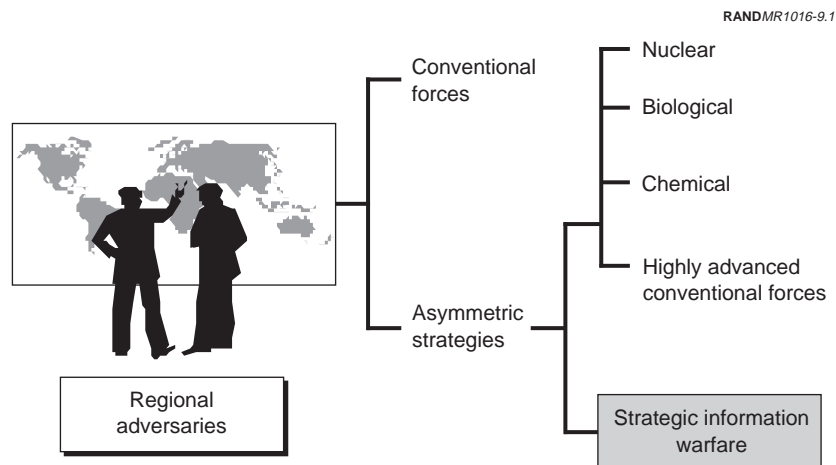


Figure 9.1—Future U.S. Regional Adversaries Might Seek Asymmetric Strategies

SIW tools and techniques present a two-pronged threat to U.S. security:

1. **A Threat to U.S. National Economic Security:** the holding at risk to massive disruption of infrastructure targets critical to the U.S. economy. A successful SIW attack on one or more infrastructures could produce a strategically significant result, including public loss of confidence in the delivery of services from those infrastructures with a resulting loss in confidence in the government.
2. **A Threat Against the U.S. National Military Strategy:** the possibility that a regional adversary might use SIW threats or attacks to deter or disrupt U.S. power-projection plans in a regional crisis. Targets of concern include infrastructures in the United States that are vital to overseas force deployment and comparable targets in allied countries. A key ally or coalition member under such attack might refuse to join a coalition—or worse, quit one in the middle of a war.

In the history of strategic warfare, it is hard to find a conflict worthy of the label *strategic* that did not manifest some important informa-

tion component. Sun Tzu, for example, recommended the creative use of information to achieve strategic objectives while avoiding conflict. It is also noteworthy that one could undoubtedly produce a list of historical instances in which fundamental changes in technology produced fundamental changes in the information component of strategic warfare.

Yet the potential impact of the information revolution on strategic warfare may be unprecedented. Whereas SIW may have largely played a subordinate role in strategic warfare in the past—in early times, to the strategic impact of conventional armies and navies, and later, to the likes of airplanes, rockets, and/or nuclear weapons—it might play a much greater role in such warfare in the wake of the information revolution. Furthermore, the potential impact of the information revolution on the vulnerability of key national infrastructures and other strategic assets may, over time, give rise to a wholly new kind of information-centric strategic warfare on wholly different time lines (more like the time lines associated with economic embargoes), worthy of consideration independent of other potential facets of strategic warfare, such as those portrayed in Figure 9.1.

Under normal circumstances, SIW might develop in something like the following stages (Figure 9.2):

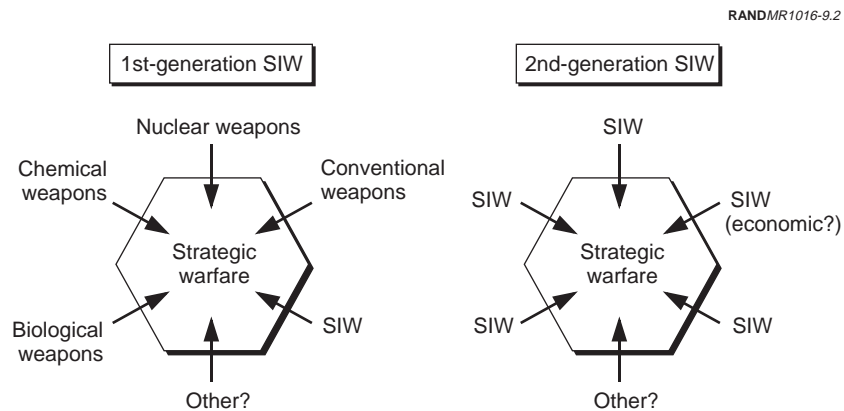


Figure 9.2—Two Concepts of SIW

1. **First-Generation SIW:** SIW as one of several facets or components of future strategic warfare, the latter broadly conceptualized as being carried forward through the orchestration of a number of strategic warfare instruments (as indicated in Figure 9.1)
2. **Second-Generation SIW:** SIW as a freestanding, fundamentally new type of strategic warfare spawned by the information revolution, possibly being carried out in newly prominent strategic warfare arenas (e.g., economic) and on time lines (e.g., years versus days, weeks, or months) longer than those generally, or at least recently, ascribed to strategic warfare.

For established powers, such as the United States, and emerging regional powers, such as Iran, the authors tend to believe that first-generation SIW is the more likely form to be initially manifest. This, however, is an arguable proposition. The United States, for example, might find itself in a situation in the near future where it chooses to exploit its current information-technology advantages and employ second-generation SIW to prevail in an international situation that otherwise would have led to troop deployments, a long campaign, and almost certain high casualties.

For less-developed nations—which may not possess any other effective strategic warfare instruments—second-generation SIW may be more immediately attractive. In fact second-generation SIW use by or against lesser powers might follow close on the heels of the demonstration of first-generation SIW.

If some nation-state or nongovernmental organization decided to conduct SIW against the United States, what vulnerabilities in our infrastructure could it exploit, how serious are they, and what would be the resulting strategic threats to our country? Before describing a framework for considering SIW issues, we address these important questions.

U.S. STRATEGIC INFRASTRUCTURE VULNERABILITIES AND THREATS

Vulnerabilities of essential U.S. infrastructures to attack, and possible threats against those infrastructures, have been the subject of substantial recent study by the President's Commission on Critical

Infrastructure Protection (PCCIP). We present here a synopsis of the threats and vulnerabilities for five U.S. infrastructure sectors, abstracted primarily from Appendix A of the commission's final report (PCCIP, 1997)—with special attention to the information and communications sector on which so many other sectors' services depend. Interested readers should consult the full PCCIP final report for additional details and discussion of these issues.

What, in fact, are the essential U.S. infrastructures, whose incapacity or destruction would have a debilitating impact on our defense or economic security?² The commissioners compressed an initial list of eight sectors into these five, for which they discussed both vulnerabilities and threats:

- *Information and Communications*—the public telephone network; the Internet; and millions of computers in home, commercial, academic, and government use
- *Physical Distribution*—the vast interconnected network of highways, rail lines, ports and inland waterways, pipelines, airports and airways, mass transit, trucking companies, and delivery services that facilitate the movement of goods and people
- *Energy*—the industries that produce and distribute electric power, oil, and natural gas
- *Banking and Finance*—Banks, nonbank financial service companies, payment systems, investment companies and mutual funds, and securities and commodities exchanges
- *Vital Human Services*—water-supply systems, emergency services, and government services.

Before discussing vulnerabilities and threats in each of the above sectors, it is useful to consider an overall assessment spanning the various sectors:

The threat is real enough. . . . Skilled computer operators have demonstrated their ability to gain access to networks without authorization. . . . Whatever their motivation, their success in entering networks to alter data, extract financial or proprietary informa-

²Executive Order 13010 calls infrastructures meeting these criteria "critical." We prefer the terminology "essential."

tion, or introduce viruses demonstrates that it can be done and gives rise to concerns that, in the future, some party wishing to do serious damage to the United States will do so by the same means.

Real vulnerabilities also exist. Infrastructures have always been subject to local or regional outages resulting from earthquakes, storms, and floods. . . . But physical vulnerabilities take on added significance as new capabilities to exploit them emerge, including chemical, biological, and even nuclear weapons. As weapons of mass destruction proliferate, the likelihood of their use by terrorists increases. . . .

Our dependence on the information and communications infrastructure has created new cyber vulnerabilities, which we are only starting to understand. In addition to the disruption of information and communications, we also face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications. . . . (PCCIP, 1997, p. 5.)

Are the vulnerabilities and threats in fact of strategic significance? Many thoughtful analysts agree, and we concur, that a coordinated, repetitive information warfare attack (including perhaps some physical damage to essential nodes) on components of essential U.S. infrastructures could have strategic consequences, especially if conducted in conjunction with other events—e.g., just preceding or during a major deployment of U.S. forces to an overseas theater. This view was reinforced by an exercise conducted by a group led by one of us (Molander) hypothesizing a crisis involving the United States and a peer competitor, in which SIW and other instruments of strategic warfare were brandished and employed against elements of the U.S. infrastructure (Molander and Wilson, forthcoming). We note that such infrastructure attacks might be conducted by non-governmental organizations loosely networked together. Such coordination is made increasingly possible by the Internet and other new network communication options. See, for example, the writings of our colleagues John Arquilla and David Ronfeldt on the concept of netwar:

an emerging mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use—indeed, depend on using—network forms of organization, doctrine, strategy, and communications. (Arquilla and Ronfeldt, 1997.)

It is important to distinguish different forms of information warfare. Martin Libicki, in a seminal report asking, “What Is Information Warfare?”, distinguishes among seven forms: command-and-control warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare, and cyber-warfare. (Libicki, 1995.) Although all have importance, the last four are most relevant in considering attacks on essential components of the U.S. infrastructure.

We summarize below the vulnerabilities of, and threats to, the five infrastructure sectors highlighted by the PCCIP.

Information and Communications

The information and communications infrastructure sector is perhaps the most essential of all, acting as the “nerves” and control for all other sectors. It is also one of the most vulnerable, both to physical attacks on key nodes and switches and to “cyber” attacks through the network itself. The sheer redundancy of the interlinked networks this sector comprises may be reduced somewhat by the new competitive environment launched by the Telecommunications Act of 1996; former cooperators are now competitors.

The public telephone network is extremely complex and interrelated, governed by no single body, and evolving rapidly in time. There is, therefore, no model or simulation that accurately captures its richness; hence, it is difficult to analyze its multifarious failure modes, cascading effects, and the like. As a whole, it has proved quite resilient to periodic natural disasters, but its survivability in a coordinated, repetitive attack by a knowledgeable, determined adversary is unproven and probably unknown.

The vulnerabilities of this sector highlighted in the PCCIP report include *switches* susceptible to software-based disruption (e.g., through remote maintenance dial-in modem ports); a *transport* architecture based on synchronous optical networks, which are remotely managed through packet data network connections that are vulnerable to electronic intrusion; *signaling* systems based on the Signaling System 7 protocol; and *control* signals in an “advanced intelligent network” design that allow changes to be made from remote locations to switch software. Some signals can increasingly

be sent from private branch exchanges to control portions of the operation of the network.

As with all other sectors, the threat to these systems may arise from five categories of “bad actors”: (1) incompetents, hackers, and disgruntled employees; (2) crooks and organized crime; (3) political dissidents and terrorist groups; (4) adversaries conducting foreign espionage, tactical countermeasures, and orchestrated tactical information warfare; and (5) adversaries seeking to achieve major strategic disruption of the United States. In all sectors, the worst threat comes from the trusted insider, who already possesses physical access, knowledge of systems and procedures, and relevant passwords and system access.

The overall assessment for this sector is not promising. As the PCCIP report concludes:

The numerous security vulnerabilities in today’s I&C [information and communications] infrastructure afford little basis for . . . confidence today, and the trends are not encouraging. In the meantime, the payoff for successful exploitation is increasing rapidly . . .

The second and more critical risk is that presented by cyber and physical attacks intended to disrupt the US I&C infrastructure and the critical societal functions that depend upon it. With network elements increasingly interconnected and reliant on each other, cyber attacks simultaneously targeting multiple network functions would be highly difficult to defend against, particularly if combined with selected physical destruction of key facilities.

The possibility that such disruption could cascade across a substantial part of the PTN [public telephone network] cannot be ruled out. . . . (PCCIP, 1997, p. A-7).

Physical Distribution

The physical distribution sector includes roads and highways, trucking companies, personal vehicles, railroads, airline operations, seaports and inland river terminals, oil and natural gas pipelines, and delivery services, including the U.S. Postal Service. At present, this “system” is quite robust because of its geographic dispersion, manual procedures in place to handle problems, and multiple options that are often available for physical transportation between sites.

Within the next five to ten years, however, the picture darkens. By 2010, the Federal Radionavigation Plan calls for the Global Positioning System (GPS) and its augmentations to be this nation's sole radionavigation system. Present GPS signals are quite susceptible to local jamming. Increased use of commercial off-the-shelf software and hardware and shared use of communication networks create additional opportunities for "trap doors" or other implanted devices in software or hardware.

Although attacks against transportation systems account for about 20 percent of all terrorist attacks, the PCCIP found that

No tested and effective means exist that facilitates reporting and transfer of information between the government and transportation infrastructure stakeholders on threats and attacks. Information-based threats to the physical distribution system are not addressed by DOT [the U.S. Department of Transportation]; private sector concern is on a sector-by-sector and company-by-company basis (PCCIP, 1997, p. A-16.)

In addition, one can easily imagine scenarios (e.g., during U.S. troop deployments) when individual railheads, shipping points, or air traffic control centers are crucial for shipment of specific items of ammunition and materiel, or for units being deployed. In those cases, the geographic dispersion and diversity of the transportation system are little consolation, since rerouting and rescheduling—when possible—could involve significant delays.

Energy

Energy production and distribution systems, including electricity and oil and natural gas systems, are perhaps the second most important and ubiquitous infrastructure, along with information and telecommunications. Recent widespread multistate electric outages in the northeast and on the west coast, illustrating cascading effects during a failure, provide little comfort.

Increasingly, energy industries are introducing

industry-wide information systems based on open-system architectures, centralized operations, increased communications over public telecommunications networks and remote maintenance. [In

addition,] Supervisory Control and Data Acquisition (SCADA) systems . . . are vulnerable because of use of commercial off-the shelf (COTS) hardware and software, connections to other company networks, and the reliance on dial-back modems that can be bypassed. (PCCIP, 1997, p. A-26.)

As a result,

significant disruption would result if an intruder were able to access a SCADA system and modify the data used for operational decisions, or modify programs that control critical industry equipment or the data reported to control centers. (PCCIP, 1997, p. A-27.)

With the increasing commercialization and competitiveness mandated in the energy sector, suppliers and distributors are likely to view implementation of the additional security measures needed as a deferrable cost.

Banking and Finance

Anyone wishing to have a strategic impact on the United States need only tinker with a financial system within which about \$3 trillion in daily payment transactions are transferred among banks and financial institutions. Of all the infrastructure systems, this is clearly the most protected and the one for which security and sustainability are extremely high priorities. Nevertheless, as with other sectors, there is danger from a subverted or disgruntled insider working for a malevolent group or nation-state.

This is also possibly the place to mention a one-time threat, but one not unique to this sector: the fact that many of the complex information systems serving this sector and its affiliated organizations must be updated to handle the so-called Year 2000 (Y2K) software problem associated with the turn of the century. The problem is widespread enough that source code for these essential systems is being accessed, viewed, and manipulated by consultants, temporary employees, and other organizations, since information operations internal to banks, stock exchanges, etc., may not have sufficient resources to handle the task in addition to their normal jobs. Other database and coding changes are needed to handle the conversion to a common currency in Europe. It is not possible to review and vali-

date every binary file resulting from the necessary recompiling of source code within this entire sector.³

Vital Human Services

This sector includes water-supply systems, emergency services, and government services. These services are highly localized, not forming a strongly interconnected national infrastructure. Failures are therefore likely to be localized. However, because of their importance, failures can have significant psychosocial effects. Communication of vulnerabilities and threats in this sector requires cooperation (largely currently lacking) among thousands of state, county, and city departments, as well as federal agencies. Perhaps the greatest vulnerability in this disparate, decentralized sector comes from increasing reliance on the Internet and the global public telephone network; vulnerabilities and threats to the telecommunications sector were surveyed above.

THE NEED FOR NEW DECISIONMAKING FRAMEWORKS

The above quick overview of sector threats and vulnerabilities cries out for a framework within which their strategic importance to the United States can be evaluated. What national policies should be instituted to deal with the threat that some nation-state or non-governmental organization might conduct SIW against the United States? How, indeed, should decisionmaking be conducted in this realm?⁴

We wish to formulate a common U.S. strategy and policy framework for addressing the challenge of SIW. But what is a strategy and policy decisionmaking framework? Its most useful form, a decisionmaking framework, is likely to be a series of relatively simple steps—a process—that presents the strategy and policy (and related) issues that need to be addressed in some particular arena in a logical architecture and along a logical path in a fashion that facilitates decisionmaking on those issues.

³“Back doors,” logic bombs, etc., may be implanted in the binary code by gimmicked compilers, leaving no trace in the corresponding source code; see Thompson (1984) for details.

⁴Adapted from Molander, Wilson, Mussington and Mesic (1998).

New strategy and policy decisionmaking frameworks are born in the crucible of necessity (or perceived possible imminent necessity)—when a specific problem area (1) appears to demand action (or might soon demand action) and (2) is of such a character that no readily applicable decisionmaking framework is available to forge an implementable action plan.

In some situations, there may be an older candidate decisionmaking framework that has been tested for its applicability to the needs of the subject problem area and found wanting. Those who favor formulating the subject area as a rapidly evolving old problem area versus a new problem area may in fact have championed use of such an older framework. Failed attempts to apply an older decisionmaking framework may even have contributed to a delay in the more forthright expression of the need for a new framework.

AN EVOLVING SERIES OF FRAMEWORKS

An initial search for a single, temporally stable framework to serve the stated function for SIW soon led to the conclusion that the concept of a *single framework* at this stage of development was illusory. Rather, the correct construct for responding to a new strategic warfare component—one truly worthy of the label *strategic* rather than being just another “strategic warfare wannabe”—would have to be dynamic, capable of responding to ongoing changes in both the international security and information-technology environments. The correct construct would in fact have to be (1) *an evolving series of frameworks*, recognizing and accepting the “punctuated equilibrium” realities of convening and executing strategy and policy decisionmaking processes and (2) *a process* that recognizes and supports the dynamic and highly evolutionary character of such a construct (especially in its early stages).

AN INITIAL FORMULATION

A clear and primary objective in this conceptualization of the SIW decisionmaking framework problem is that the initial formulation of such a framework be one that can in fact evolve in response to changes in its environment—that it have an evolutionary potential rather than being merely a temporary expedient to get decisionmaking going but not have much utility thereafter.

The absence of a precursor framework in this issue area also means that the initial version of the framework will attract attention from stakeholders interested in the future of the information revolution and, of course, from the media. With this perspective in mind, the process of designing an associated inaugural first-generation SIW decisionmaking framework—a generic process that in fact *constitutes* the framework—can be divided into the following distinct steps (see Figure 9.3):

1. **Key Dimensions of the SIW Environment.** Gain an understanding of the key dimensions of the future first-generation SIW “environment” or “battlespace,” i.e., the dimensions of that environment that might in principle be shaped or influenced (presumably in some favorable direction) by effective near-term strategy and policy decisionmaking. Achieve this objective by (1) identifying the principal defining features of first-generation SIW within a spectrum of plausible first-generation SIW contexts and (2) selecting from among them the features that might be cast as key dimensions amenable to change as described above.

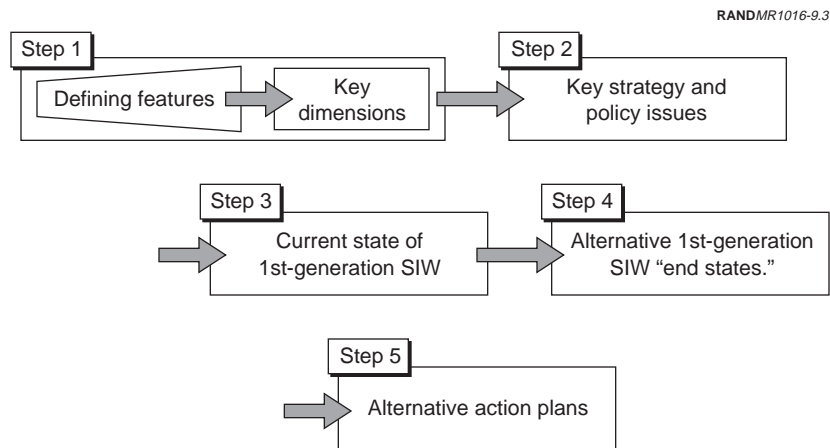


Figure 9.3—Designing a First-Generation SIW Strategy and Policy Decisionmaking Framework

2. **Key Strategy and Policy Issues.** Identify those key strategy and policy issues (and other issues, such as organizational issues) germane to the first-generation SIW problem (i.e., issues on which near-term decisionmaking could shape or influence the above-identified key dimensions of the SIW environment).
3. **Current State of First-Generation SIW.** Assess the current state of first-generation SIW in terms of absolute and relative offensive and defensive SIW capabilities.
4. **Alternative First-Generation SIW “End States.”** In the light of the above-cited first-generation SIW contexts and scenarios, craft a set of (plausible and potentially desirable) alternative first-generation SIW “end states”—expressed in terms of the above key dimensions of the first-generation SIW environment.
5. **Alternative Action Plans.** Array the key SIW strategy and policy issues against each of these alternative end states and conceptualize action plans for moving toward one or more of these end states.

Clearly, any such framework will need continual testing and evaluation against emerging contingencies. It should be recognized, however, that it may be hard to achieve a sustained high comfort level with respect to the viability of any framework until the related information technology and international security environments are less dynamic. Further elaboration on each of the five steps in Figure 9.3 is provided below.

It is anticipated that a second-generation SIW framework would have generic steps similar in character to those presented for first-generation SIW, but no attempt has been made to craft such a framework, not least because of the highly uncertain character of a second-generation SIW campaign.

Key Dimensions of the SIW Environment

As noted, the key dimensions of the SIW environment are obtained by identifying the defining features of the SIW environment and asking which of these can be potentially shaped or influenced in some favorable direction by well-conceived strategy and policy decisionmaking. These dimensions (see Table 9.1) thus constitute the

Table 9.1
From Defining Features to Key Dimensions of the SIW Environment

Defining Features	Consequences
Entry cost low	May be many actors in the SIW battlespace
Strategic intelligence on threat unavailable	Identity and capabilities of potential adversaries may be unclear
Tactical warning difficult	May not know attack is under way
Attack assessment difficult	May not know perpetrator or targets
Damage assessment difficult	May not know full implications of the attack
Traditional boundaries blurred	May not know who has various responsibilities before, during, or after an attack
Weapon effects uncertain	Both attacker and defender may be uncertain as to weapon effects
Infrastructure vulnerabilities uncertain but suspect	U.S. homeland may not be a sanctuary; vulnerable partners could make sustaining coalitions more difficult

basic factors in the SIW setting that influence attainable objectives relating to SIW and the relationships between purposive action by states (and other actors) and changes in the shape of the SIW environment itself.

Key Strategy and Policy Issues

SIW presents a broad and complex spectrum of issues and challenges to existing decisionmaking processes. As a consequence, it is clear that some sequencing is appropriate in taking up these issues nationally and internationally. To this end, the key strategy and policy issues identified in this chapter can be roughly characterized in terms of three categories:

1. **Low-Hanging Fruit.** This category encompasses issues that could be moved to closure nationally (and, in some cases, possibly internationally) without undue difficulty once suitable processes are identified or established. Issues that lie in this category (with illustrative alternatives) are
 - **Locus of Responsibility/Authority.** Who should have the lead responsibility—government (and, if so, who within the government?) and/or industry (and, if so, who within the key infrastructures)—in the U.S. national response to the SIW threat?

- federal government leadership with a national security focus
- federal government leadership with a law-enforcement focus (e.g., Department of Justice leadership)
- joint international government leadership—national security focus
- joint international government leadership—law-enforcement focus
- international industry leadership—government support.
- **Tactical Warning, Attack Assessment, and Emergency Response.** How should the United States (and the planet)—its governments and its industry—organize to develop and implement capabilities and procedures to sense and respond to SIW threats?
 - a government-led, national security-oriented model—labeled a National Infrastructure Condition (NICON) model
 - a government-led, law enforcement-oriented model—labeled a counterterrorism model
 - a Centers for Disease Control (CDC) and Prevention model
 - an industry-led model.
- **Vulnerability Assessments.** By what means and mechanisms of government and industry cooperation should a vulnerability assessment of key U.S. national infrastructures be undertaken?
 - a government-led (e.g., Department of Defense-led) assessment of U.S. vulnerabilities
 - a joint public-private sector effort involving the United States and other key nations (e.g., G-7 and/or potential SIW peer competitors)
 - an international public-private partnership along the lines of the U.S. CDC or the United Nations World Health Organization (WHO)
 - an industry-led and government-assisted assessment.

- **Declaratory Policy on SIW Use.** What should the U.S. government declaratory policy be on the use of SIW and the relationship between the use of SIW and the use of other strategic military and economic instruments?
 - retaliation principally in kind for any SIW attack
 - retaliation principally by non-SIW military means in response to such an attack
 - retaliation by economic means, including possibly economically oriented SIW means, in response to such an attack
 - complete ambiguity as to how the United States would respond to such an attack.

- 2. **Tough Issues to Be Faced Now.** These are urgent but contentious issues related to the inaugural charting of long-term SIW-related national goals and strategy. Examples of these issues (with alternatives) include:
 - **R&D Investment Strategy.** Many experts on SIW believe that there is going to be some R&D needed in this area that industry will not do. Handling this R&D (not least because offensive and defensive R&D in this domain is so intertwined) will be tricky. What investment strategy should the U.S. pursue with respect to the likes of monitoring, identification, and traceback techniques; attack assessment techniques; defense and reconstitution techniques; and damage assessment techniques?
 - no significant international SIW cooperation
 - limited international cooperation focused on defensive techniques (e.g., G-7 model)
 - broad international cooperation organized through existing multinational security arrangements (e.g., NATO model)
 - broad international cooperation organized through global arrangements (e.g., WHO model)
 - broad voluntary international cooperation.

- **International Information Sharing and Cooperation.** What principles should guide international collaboration (in particular with allies and coalition partners) in the SIW domain? Is there an SIW parallel to extended deterrence? extended defense?
 - national security-oriented network protection goals
 - coordinated defensive R&D with allies
 - international proscriptions on offensive SIW R&D
 - private-sector, market-driven focus.
- 3. **Deferred Issues.** These issues, for one reason or another (e.g., technical uncertainties), are not yet ready to be taken to closure—or, worse, that taking them to closure prematurely might produce “bad” strategy or policy decisions that would be hard to undo. Issues in this category include
 - **Intra- and Intergovernmental Cooperation on Politically Sensitive Privacy Issues.** This subject clearly needs to be included in any discussion of SIW, but more detail is needed on how privacy rights would be protected under specific strategies and policies.
 - **Minimum Essential Information Infrastructure (MEII).** More analytical and conceptual work is needed to determine whether the MEII concept (a system, or more precisely, a process that can produce the wherewithal to provide some minimal level of communications access and services to critical governmental and societal user communities) is at all feasible from both the technical and cost standpoints.
 - **Encryption Policy.** SIW is just one of the many issue areas that need to be brought to the table when the United States and the international community chart long-term goals and strategies related to encryption.

Each of these areas requires sensitive treatment. In turn, each of them overlaps with other elements of a comprehensive approach to addressing SIW policy concerns. This notion, that an action plan for addressing SIW vulnerabilities requires that trade-offs be made among and between different factors, is central to the unprecedented uncertainties of the cyberspace environment. The next sec-

tion addresses defensive and offensive SIW issues that have significance for SIW action plans and policy implementation.

Current State of First-Generation SIW

Clearly, a macroassessment of the current state of first-generation SIW in terms of absolute and relative offensive and defensive SIW capabilities of the United States and other nations (or other parties) would be difficult to do even at a classified level. The current dynamic character of the information revolution and the embryonic character of SIW as a potential political-military instrument both argue for caution in making such an assessment—classified or unclassified—now and for the foreseeable future.

The following are the principal SIW assessment issues from the U.S. perspective:

1. the extent to which hostile SIW powers already exist and the degree to which they can seriously harm the United States with SIW attacks
2. the extent of current U.S. offensive SIW capability vis-à-vis other states (foe, neutral, or friend)—whether overt or covert—in preventive, preemptive, or retaliatory SIW actions.

To address these issues, the difficult task of evaluating offensive and defensive SIW capabilities must be broached.

The United States, as the global leader in the development and exploitation of information systems, surely has the potential to be an offensive SIW “superpower” if any nation does. Any lesser assessment of U.S. SIW potential vis-à-vis that of others would be judged as laughable by nations that are just beginning to speculate about the significance that SIW instruments may have in future conflicts. The United States, not least because of its global military and economic role, is also likely, at this stage, to have more precise information on the basic architecture and key nodes of a potential adversary’s strategic infrastructures—a vital factor in a conceptual SIW campaign (where decisionmakers are bound to ask challenging questions about collateral effects). How far has the inherent U.S. SIW potential been exploited? How fast could it be exploited if the United States

were to make a strong national commitment to the urgent development of offensive SIW capabilities?

On the offensive side, the current U.S. experience with information operations is as a supporting but relatively low-profile element of U.S. military strategy and doctrine. The United States has well-developed and successful offensive command and control, electronic, and other information warfare capabilities (e.g., U.S. Southern Command is a master of psychological operations, and the military services develop and operate electronic warfare systems—manifest in the large-scale use of command and control warfare and the suppression of enemy air defenses in the Persian Gulf War), but these could hardly be characterized as “strategic” in the sense of this chapter. Offensive first-generation SIW, which by definition has the potential to hold at risk a country’s central nervous system (its critical infrastructure networks), is a much more-sensitive undertaking than are “information operations” as supporting missions in conventional warfare. It is one thing to target military leadership, communications, and radar; it is quite another to target public utilities that, among other things, provide power to hospitals.

The sensitivities of our friends and allies and the political-military capital that might accrue to possible adversaries from an increasingly open emphasis on U.S. offensive SIW initiatives have largely kept more definitive information on these capabilities from being revealed. While some U.S. SIW offensive capability clearly exists, its full potential is politically and militarily sensitive. A full debate on the role of offensive SIW in U.S. national security strategy would likely have to deal with strong arguments from U.S. information systems and infrastructure equipment suppliers that a U.S. strategic emphasis on—and possible demonstration of—such a capability could profoundly and adversely affect their overseas sales.

Beyond being a leading contender to augment its existing arsenal with offensive SIW capabilities, the United States, again by virtue of its role in the world, is also a natural target for SIW attack. The United States leads the world in the development and application of information technologies and has a complex society and economy critically dependent on information systems. It is geographically protected and currently has the world’s most formidable conventional military capabilities. If the United States is to be defeated or thwarted militarily in the near future, it will most likely be because of

the successful use of an “asymmetric” strategy by an enemy seeking to avoid a direct military confrontation.

The first logical step in understanding SIW defensive implications is to conduct a review of potential U.S. vulnerabilities to conceivable SIW attacks across a broad threat and scenario spectrum. Unfortunately (or fortunately), we have very little real-world experience on which to base such an assessment. There have been a number of natural events (storms, earthquakes), human errors (software, control), and purposeful mischief (hobbyist hackers, criminals) that suggest that things can go wrong in various national infrastructures, occasionally on an impressive scale. But none of these past events has been “strategic” in its impact, and none appears to have been strategic in its intent.

One obvious problem with this paucity of defensive SIW-related experience is in relating cause and effect: Have we escaped SIW attacks because certain undetected attempts were not successful or because no one has tried yet?

While a great deal of uncertainty surrounds the future vulnerability of information infrastructures, it can be observed that a number of trends seem to point toward an expanded dependence on inherently less-secure networking concepts. In particular, the widespread adoption of open network standards and technologies means that the industries and applications delivered via cyberspace may become more vulnerable to single-point failures. The growth of electronic commerce, the prospective expansion of electronic stored value (Cyberpayment) payment systems, and plans for the delivery of critical services (e.g., telemedicine, government communications) over the global information infrastructure all present potential targets for an SIW attack.

The defensive SIW assessment thus comes down to an assessment of information-infrastructure vulnerability, threat potential, and vulnerability consequences. These assessments also have problems. Existing information infrastructure systems are complex, dynamic, flexible, and interdependent. They are public and private, military and commercial. Some (e.g., banking) have been “hardened” by design because of the potential risk and cost of compromise. Others have evolved in a more benign environment with nonthreat forcing functions (e.g., cost, accessibility, and interoperability).

Standard risk assessment methodologies (fault-tree analyses, simulations, red teams) have uncertain applicability and future analysis potential because information systems are very complex and because threats can be very diabolical. Information security responsibilities are decentralized, and specific system vulnerabilities that are discovered are very sensitive and tightly held (for obvious very good reasons).

Undiscovered risks may continue to be the greatest concern. This suggests that continuing vigilance is required so that known problems can be fixed as they are discovered (if costs to fix are “reasonable”). If known problems are hidden but not fixed, threats can be monitored and contingency plans can be developed, but associated risks may be impossible to measure in terms of direct (immediate) loss potential (human lives, repair and replacement costs, opportunity costs while equipment is down, etc.).

With the above caveats properly lowering expectations about the precision achievable, a preliminary assessment of the current state of first-generation SIW in terms of the key dimensions listed above is as follows:

1. **Number of Offensive SIW Players:** *Unknown* (but probably between 0 and a few)
2. **Tactical Warning** (Is attack under way?) and **Attack Assessment** (By whom, how big, and what?): Issues are uncertainty in perpetrator identity and the potential value and timeliness of warning indicators; all are *unknown* but perpetrator uncertainties will likely be small in first-generation SIW in which information warfare is only one element of the conflict (but it could be *large* if the perpetrator desires)
3. **Damage Assessment** (size and scope of damage): Significant damage will speak for itself; most critical damage-assessment issues are related to the potential for, and implications of, further damage
4. **Uncertainty in Weapons Effects:** Large
5. **Degree of SIW Vulnerability:** *Unknown* (but there are worrisome trends and real concerns).

Although we do not know with confidence what the current situation with respect to offensive and defensive SIW capabilities is, people with informed *opinions* tend to fall into one of two polar groups: (1) those who see the historical glitches in information infrastructures as indicative of potential vulnerabilities that could be exploited by future adversaries, possibly with significant strategic advantage and (2) those who see this experience as strong evidence that the exploitable effects of whatever vulnerabilities might exist would be relatively modest and that the systems are evolving in a Darwinian mode that will continue to assure appropriate defense mechanisms—that there is no such thing as SIW. Determining the correct view between these two positions is less important than how we should proceed given current (and likely future) uncertainties.

Alternative First-Generation SIW End States

The fourth step in the SIW framework design process is the crafting of a set of *plausible and potentially desirable* alternative first-generation SIW asymptotic end states—taking into account the nature of the first-generation SIW threats that have been identified and expressed in terms of the previously cited key dimensions of the first-generation SIW environment. Note the criterion “plausible and potentially desirable,” which eliminates such possible end states as a very large number of nations with major-league offensive SIW capability alongside generally poor defensive SIW capabilities.

This end state–crafting process is in effect likely to be an aggregation of assessments of the impact and possible future evolution (shaped or not shaped by related targeted strategy and policy decisions) of a set of threats identified in various SIW scenarios—expressed to the degree possible in terms of the key dimensions.

On the basis of the above approach, the following might be an initial array of possible alternative first-generation SIW asymptotic end states:

U.S. Supremacy in Offensive and Defensive SIW. The United States overwhelmingly dominates the SIW environment by virtue of possessing

1. far and away the world’s best offensive SIW tools and techniques, capable of penetrating any other country’s SIW defenses

2. highly effective SIW defenses and reconstitution and recovery capabilities that effectively reduce the vulnerability of potential SIW targets in the United States (e.g., key U.S. infrastructures) to strategically insignificant levels—capabilities that it *selectively* shares with allies
3. traceback capabilities that give very high confidence of perpetrator identification—whereas no other nation has traceback capabilities good enough to identify the United States as the source if it launches SIW attacks.

Club of SIW Elites. Through a combination of technical capability and resource allocation, an international condominium of a handful of highly competent SIW nations emerges (e.g., on the order of 5 to 10) with the United States almost certain to be the most competent of the group. Mutual deterrence of SIW use is the norm among club members. This handful of SIW “major leaguers” collaborates with each other to some degree to

1. constrain the spread of major-league SIW capability to other nation-states and nonstate actors
2. de-emphasize SIW and establish a norm of no first use of SIW
3. set international technical standards for cyberspace that help to perpetuate the exclusivity of the club.

Global “Defense Dominance” in SIW. As a consequence of broad global cooperation in the fielding of very high quality SIW defenses, the vulnerability of key potential SIW targets (e.g., key infrastructures) in most nations is reduced to strategically insignificant levels. This end state is further bolstered in some measure by international cooperation in the global dissemination of

1. high-quality traceback capabilities (and/or a commitment to provide “Whodunit?” traceback information in the event of a serious SIW attack)
2. high-quality tactical warning and attack assessment capabilities.

This end state would also be bolstered by establishment of an SIW “arms control” regime, along the lines of the biological and chemical weapon arms-control regimes, which would establish international information operation norms, standards, legal restrictions, and

enforcement mechanisms. Like currency counterfeiting, software piracy, and other threats to world economic order, SIW becomes something responsible states do not do. SIW rogues are dealt with as the UN dealt with Saddam: Deny them their goals and punish them.

Market-Based Diversity. The extent of damage or disruption achievable in an SIW attack is modest, and reconstitution and recovery are fast as a consequence of

1. the natural strength of diversity in the globalization and standardization of cyberspace reducing overall vulnerability to SIW attack to moderate levels
2. global cooperation in providing high-quality damage assessment tools
3. market-reinforced (“good neighbor”) cooperation on reconstitution and recovery.

Alternative Action Plans

The fifth step is applying the methodology to develop alternative action plans. The analytical and conceptual framework described here has application to concrete decisions affecting many areas of public policy. In the context of government actions designed to address SIW vulnerabilities, the framework provides a step-by-step means of addressing the relationship between strategy and policy questions in the SIW domain and the net—or relative—impact of different policy choices on achieving overall SIW-related strategic objectives.

The process of developing a set of alternative action plans is thus one of

1. choosing a set of illustrative alternative SIW end states
2. coming to judgment on a selected set of key SIW strategy, policy, and related issues (such as cited above) with an eye to moving in the direction of a specified end state.

Table 9.2 provides an illustrative set of alternative action plans for navigating toward the four illustrative end states cited above, based on decisions on those SIW issues in the “Low-Hanging Fruit” and

Table 9.2
Alternative Action Plans

	Competition	Mixed (Competition and Cooperation)	Cooperation	
	A	B	C	D
Key strategy and policy issues	U.S. Supremacy in SIW	Club of SIW elites	Global “defense dominance” in SIW	Market-based diversity
Locus of responsibility and authority	Federal government leads	Federal government leads	Federal government leads	Industry leads
	National security focus	National security focus	Law enforcement focus	
	Joint leadership	Joint leadership	Joint leadership	
Tactical warning and alert structure	Government-led NICON model	Government-led NICON model	CDC model	Industry-led model
	Counterterrorism model	Counterterrorism model CDC model	Industry-led model	
Declaratory policy (links with other military instruments)	Strong retaliation threat (SIW retaliation emphasis)	Moderate retaliation threat v.s nonclub actors	No retaliation threat	Moderate retaliation threat (emphasis on economic instruments)
	Reassurance on invulnerability of key infrastructure	Some reassurance on invulnerability of club infrastructures	Reassurance on resilience of GII	

Table 9.2—Continued

	Competition	Mixed (Competition and Cooperation)	Cooperation	
	A	B	C	D
International information sharing and cooperation	SIW programs compartmentalized	High degree of cooperation within club (G-7/FATF model)	High degree of cooperation Institutional links through NATO, FATF, etc.	High degree of voluntary cooperation
Vulnerability assessments	Government-led (NICON organizational model)	Government-led (G-7/FATF model)	Public/private U.S. (WHO Model)	Public/private U.S. (CDC Model)
R&d/investment strategy priorities	National security-oriented protection goals	Coordinate defensive R&D with allies	Coordinate defensive R&D with allies	Proscriptions on offensive SIW R&D
	Some coordinated defensive R&D with allies	Some proscriptions on offensive SIW R&D	Proscriptions on offensive SIW R&D	Private-sector focus

“Tough Issues” categories (see above). Note that, in some instances, more than one issue alternative is compatible with the indicated end state. (More detailed descriptions of some of the more cryptic entries in Table 9.2 are provided in Molander, Wilson, Mussington, and Mesic, 1998.)

CONCLUSIONS

The above-described strategy and policy decisionmaking framework and process—an evolving series of frameworks—would appear to offer a useful means of organizing thinking about the emerging SIW problem and achieving an inaugural action plan in this arena. As such, it should contribute to the ongoing effort to identify the SIW-related issues on which decisions need to be made at this time in the United States and the appropriate forum(s) in which to take up these issues.

This framework and process, though oriented to U.S. national decisionmaking, should also contribute to preparations for the imperative and even more challenging international decisionmaking process on this subject, for which the issue of the appropriate forum(s) for such an undertaking also remains to be resolved.

REFERENCES

- Arquilla, J., and D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997.
- Libicki, M., *What Is Information Warfare?* Washington, D.C.: National Defense University, Institute for National Strategic Studies, ACIS Paper 3, 1995. Available at <http://www.ndu.edu/inss/actpubs/act003/a003cont.html> (last accessed February 18, 1999).
- Molander, R., and P. Wilson, *The Day After . . . in the American Strategic Infrastructure*, Santa Monica, Calif.: RAND, MR-963-OSD, forthcoming.
- Molander, R., P. Wilson, D. Mussington, and R. Mesic, *Strategic Information Warfare Rising*, Santa Monica, Calif.: RAND, MR-964-OSD, 1998.

PCCIP—see President's Commission on Critical Infrastructure Protection.

President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Washington, D.C., 1997. Also available at http://www.pccip.gov/report_index.html (last accessed February 18, 1999).

Thompson, K., "Reflections on Trusting Trust," *Communications of the ACM*, Vol. 27, No. 8, August 1984. Reprinted in L. Hoffman, ed., *Rogue Programs: Viruses, Worms, and Trojan Horses*. New York: Van Nostrand Reinhold, 1990.