Chapter Eight

ALTERNATIVE ACTION PLANS

As discussed previously, the fashioning of an SIW action plan involves (1) gaining the best possible reading on where one is, and then, within the limits of uncertainties, (2) charting a course or pathway for a near-or long-term goal or end state (however roughly defined) through the choices made on a carefully chosen set of policy, strategy, and related issues.

With this perspective in mind and as a final presentation of potential outcomes, Table 8.1 arrays those key issues identified in Chapter Four as potentially ready for near-term decisionmaking in terms of which options for these issues favor which end states. A comprehensive examination of such alternatives—and an initial set of choices—appears to be a priority task for U.S. government and industry in forging an initial action plan in this problem area.

Some additional perspectives on the individual issues and the array of presented end states follows:

1. Locus of responsibility and authority. This issue, arrayed against the various end states, must be faced immediately. Can the SIW problem be left to the marketplace to solve, or is some fundamental government intervention required? If there is a serious SIW-related national security threat—and it appears at this time that there could be—some level of government involvement appears to be imperative. RAND's exercises to date and the report of the PCCIP argue strongly for some kind of joint responsibility. Whether on the government's side this should have a national security orientation or a law-enforcement orientation remains debatable and is likely to be very much affected by preferences for the end state (B versus C).
2. Tactical warning and alert structure. This issue is also strongly affected by the degree of the threat from nations that could mount well-coordinated and well-structured SIW attacks. As indicated in Table 8.1, a number of different warning and response models might be considered, again depending in part on the preferred asymptomatic end state. The PCCIP report, the Defense Science Board (DSB) Information Warfare report, and the results from the RAND exercises also support creating such a warning as a priority matter if there is to be any serious effort to combat the SIW problem. Creating such a system, which cannot be done without substantial government-industry cooperation, may be a critical means of fostering the government-industry cooperation that is needed across the board on this subject.

Table 8.1

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/ authority	Federal government leads; national security focus Joint leadership	Federal government leads; national security focus Joint leadership	Federal government leads; law enforcement focus Joint leadership	Industry leads
Tactical warning and alert structure	Government-led NICON model Counterterrorism model	Government-led NICON model Counterterrorism model CDC model	CDC model Industry-led model	Industry-led model
Declaratory policy (links with other military instruments)	Strong retaliation threat (SIW retaliation emphasis) Reassurance on invulnerability of key U.S. infrastructure	Moderate retaliation threat vs. non-club actors Some reassurance on invulnerability of club NIIs	No retaliation threat Reassurance on resilience of GII	Moderate retaliation threat (emphasis on economic instruments)
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 protection and coordinated alliance action	Coordinated international action and proscriptions on offensive SIW research	Coordinated R&D, with offensive R&D proscriptions and a private sector focus	Private sector focus, with proscriptions on offensive SIW R&D

3. Declaratory policy. Declaratory policy constitutes a major problem because of the profound uncertainty in perpetrator traceback and identification techniques. This issue will be affected by the outcome of the national and global encryption debate. It therefore seems unlikely that any clear and temporally stable declaratory policy statement will be achievable in the near future. The implicit (possibly made explicit) posture on this issue appears to be ambiguity about the response to SIW attack. Explicitly, this posture of ambiguity (which could also be the chosen posture even if traceback techniques improved dramatically) would likely be couched in terms that threatened retaliation with any or all the available instruments of strategic leverage, from strictly military to economic instruments.

4. International information sharing and cooperation. This issue emphasizes the challenging problem of international information sharing on defenses against SIW attack. To adequately address this issue, careful consideration must be given to the desired SIW end state. If either the U.S. Supremacy in SIW (A) or the club of SIW elites (B) end state is seen as both desirable and achievable, sharing of such information will be highly restricted. In contrast, the other two end states assume, if not demand, a high level of global cooperation.

5. Vulnerability assessments. Some means of obtaining an assessment of comprehensive infrastructure vulnerability is imperative. But as shown in Table 8.1, who should do it and how such information is distributed and integrated is a function of the preferred end state.

6. R&D investment strategy priorities. This issue is driven largely by whether the United States is interested in maintaining a strong SIW capability (end state A) and whether the United States (and/or possibly a group of like-minded nations) sees perpetrator identification possible and therefore makes direct retaliation against SIW attackers a plausible SIW posture (end state B). However, if cooperation and a focus on defense and reconstitution is viewed as preferable (C or D), there could be a proscription on offensive SIW and global coordination of R&D similar to a public health model.