WHAT IS STRATEGIC INFORMATION WARFARE?

In the future, the possibility exists that adversaries might exploit the tools and techniques of the Information Revolution to hold at risk (not for destruction, but for large-scale or massive disruption) key national strategic assets such as elements of various key national infrastructure sectors, such as energy, telecommunications, transportation, and finance). This potential danger constitutes the principal aspect of the Strategic Information Warfare (SIW) environment addressed in this report.

Both regional adversaries and peer competitors may find SIW tools and techniques useful in challenging the United States, its allies, and/or its interests. SIW weapons may find their highest utility in the near-term in “asymmetric” strategies employed by regional adversaries (see Figure S.1). Such adversaries might seek to avoid directly challenging U.S. conventional battlefield superiority through a more indirect attack (or threat) involving some combination of nuclear, chemical, biological, highly advanced conventional, and SIW instruments.

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

1. **a threat to U.S. national economic security.** Key national infrastructure targets could be at risk to such massive disruption that a successful 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.

2. **a threat against the U.S. national military strategy.** The possibility exists 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 vital to overseas force deployment, and comparable targets in allied countries. A key ally or coalition member under such an attack might refuse to join a coalition—or worse, quit a coalition 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 information 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. In the past, SIW may have played largely a subordinate role in strategic warfare—in early times in the strategic impact of conventional armies and navies, and later through airplanes, rockets, or nuclear weapons. However, SIW 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 new kind of information-centered strategic warfare based on completely different time lines, and worth consideration independent of other potential facets of strategic warfare such as those portrayed in Figure S.1.

SIW thus might be conceptualized in the following terms (see Figure S.2):

1. **First-Generation SIW**. SIW as one of several components of future strategic warfare, broadly conceptualized as being orchestrated through a number of strategic warfare instruments (as indicated in Figure S.1).

2. **Second-Generation SIW**. SIW as a free-standing, fundamentally new type of strategic warfare spawned by the Information Revolution, possibly implemented in newly prominent strategic warfare arenas (for example, economic) and on time lines (for example, years versus days, weeks, or months) than those generally, or at least recently, ascribed to strategic warfare.

For established powers such as the United States, the authors tend to believe that first-generation SIW is the more likely form of strategic warfare to be initially mani-
fested. This proposition, is however, arguable. The United States, for example, might find itself in a situation in the near future in which it chooses to exploit its current information technology (IT) advantages and employ second-generation SIW to prevail in a crisis that otherwise would have led to troop deployments and almost certain high numbers of 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.

THE NEED FOR NEW DECISIONMAKING FRAMEWORKS

According to the project description for this study, “The goal of this project is to formulate a common DoD strategy and policy framework for addressing the challenge of strategic information warfare.” But what is a strategy and policy decisionmaking framework? A decisionmaking framework is likely to be a series of relatively simple steps, or a process, that presents the strategy, policy, and related issues that need to be addressed in some particular arena in a logical architecture, and along a logical path in a manner that facilitates decisionmaking on those issues.

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

In some situations, an older decisionmaking framework may have been tested for its applicability to the needs of the subject problem area and been 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**

The history of the carrying out of the above-mentioned tasks can be characterized as an initial search for a single, temporally stable framework to serve the stated function for SIW that soon concluded 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” and opposed to just another “strategic warfare wannabe”—would have to be dynamic, and capable of responding to ongoing changes in both the international security and IT environments. The correct construct would have to be (1) an evolving series of frameworks, recognizing and accepting the evolution-like “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 primary objective in this conceptualization of the SIW decisionmaking framework problem is that the initial formulation of the framework be one that can evolve in response to changes in its environment. It needs to have evolutionary potential, rather than being a temporary expedient that got decisionmaking going, but did not have much utility thereafter.

Because there is no precursor framework in the SIW area, the initial version of the framework will attract attention from stakeholders interested in the future of the Information Revolution and from the media. The process of designing an associated inaugural first-generation SIW decisionmaking framework—a process that constitutes the framework—can therefore be divided into the following distinct steps (see Figure S.3):

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

2. **Key strategy and policy issues.** Identify those key strategy and policy issues (and such other issues as organizational issues) germane to the first-generation SIW problem (that is, issues for which near-term decisionmaking could influence the key dimensions of the SIW environment identified above).
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 light of the above-mentioned 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 mentioned key dimensions of the first-generation SIW environment.

5. **Alternative action plans.** Array the key SIW strategy and policy issues against each of the alternative end states, and conceptualize action plans for moving toward one or more of these end states.

Any such framework will have to be continually tested and evaluated against emerging contingencies. It should be recognized, however, that it may be hard to achieve a sustained high level of comfort concerning the viability of any framework until the related IT and international security environments are less dynamic. Further details on the five steps shown in Figure S.3 are provided below.

**KEY DIMENSIONS OF THE SIW ENVIRONMENT**

As previously 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 influenced in some favorable direction by well-conceived strategy and policy decisionmaking. These dimensions (see Table S.1) thus constitute the basic factors in the SIW setting that influence attainable objectives relating to SIW,
and the relationships between purposeful action by nations (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. Thus, it is clear that some sequencing in taking up these issues nationally and internationally is appropriate. The key strategy and policy issues identified in this study can therefore be roughly characterized in terms of three categories:

“Low-Hanging Fruit.” Those issues that could be moved to closure nationally (and, in some cases, internationally) without undue difficulty once suitable processes are identified or established. Issues in this category (with sample alternatives) are

- **Locus of responsibility and 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 (for example, Department of Justice leadership)
  - Joint international government leadership with a national security focus
  - Joint international government leadership with a law-enforcement focus
  - International industry leadership with government support.

<table>
<thead>
<tr>
<th>Defining Features</th>
<th>Consequences</th>
<th>Key Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry cost low</td>
<td>May be many actors in the SIW battlespace</td>
<td>Number of offensive SIW players</td>
</tr>
<tr>
<td>Strategic intelligence on threat unavailable</td>
<td>Identity and capabilities of potential adversaries may be unclear</td>
<td>Number of offensive SIW players</td>
</tr>
<tr>
<td>Tactical warning difficult</td>
<td>May not know attack is under way</td>
<td>Tactical warning capability</td>
</tr>
<tr>
<td>Attack assessment difficult</td>
<td>May not know perpetrator or targets</td>
<td>Attack assessment capability, including perpetrator identity</td>
</tr>
<tr>
<td>Damage assessment difficult</td>
<td>May not know full implications of the attack</td>
<td>Damage assessment capability</td>
</tr>
<tr>
<td>Traditional boundaries blurred</td>
<td>May not know who has various responsibilities before, during, or after attack</td>
<td>N/A</td>
</tr>
<tr>
<td>Weapon effects uncertain</td>
<td>Both attacker and defender may be uncertain about weapon effects</td>
<td>Uncertainty in weapon effects</td>
</tr>
<tr>
<td>Infrastructure vulnerabilities uncertain but suspect</td>
<td>U.S. homeland may not be a sanctuary; vulnerable partners could make sustaining coalitions more difficult</td>
<td>Degree of SIW vulnerability</td>
</tr>
</tbody>
</table>
• **Tactical warning, attack assessment, and emergency response.** How should the United States (and the world), including 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 (called a National Infrastructure Condition [NICON] model)
  — A government-led law-enforcement-oriented model (called a counterterrorism model)
  — A Centers for Disease Control and Prevention (CDC) 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 (these could include for example, DoD-led) assessment of U.S. vulnerabilities
  — A joint public and private sector effort involving the United States and other key nations (for example, G-7 and/or potential SIW peer competitors)
  — An international public-private partnership, such as the CDC and the World Health Organization (WHO)
  — An industry-led and government-assisted assessment.

• **Declaratory policy on SIW use.** What should U.S. government declaratory policy be on the use of SIW and the relationship between the use of SIW and 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, possibly including economically oriented SIW means, in response to such an attack
  — Complete ambiguity as to how the United States would respond to such an attack.

**Tough Issues to Be Faced Now**

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

• **Research and development (R&D) investment strategy.** What investment strategy should the United States pursue for (1) monitoring, perpetrator identifica-

---

1 The G-7 is the name applied to the seven largest industrial democracies (United States, Canada, France, Germany, Great Britain, Italy, and Japan) which meet annually at the level of chiefs of state.
tion, and perpetrator “trackback” techniques, (2) attack assessment techniques, (3) defense and reconstitution techniques, and (4) damage assessment techniques?

— A government-led national security-oriented model (called a National Infrastructure Condition (NICON) model
— No significant international SIW cooperation
— Limited international cooperation focused on defensive techniques (such as the G-7 model)
— Broad international cooperation organized through existing multinational security arrangements (for example, the NATO model)
— Broad international cooperation organized through global arrangements (such as the 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? To extended defense?

— National security-oriented network protection goals
— Coordinated defensive R&D with allies
— International proscriptions on offensive SIW R&D
— Private sector or market-driven focus.

**Deferred Issues**

Issues that are not yet ready, for example, because of technical uncertainties to be taken to closure, or, worse, issues that are taken to closure prematurely, possibly producing “bad” strategy or policy decisions that would be hard to undo. Issues in this category include

• **Intragovernmental and intergovernmental cooperation on politically sensitive privacy issues.** This subject 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 providing a minimal level of communications access and services to critical governmental and societal user communities) is at all feasible from both a technical and cost standpoint.
• **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 encryption-related goals and strategies.
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. The notion that an action plan for addressing SIW vulnerabilities requires that tradeoffs be made among different factors is central to the unprecedented uncertainties of the cyberspace environment. The next section addresses defensive and offensive SIW issues that are significant to SIW action plans and policy implementation.

CURRENT STATE OF FIRST-GENERATION SIW

A macro assessment 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, at present and for the foreseeable future.

Principal SIW assessment issues from the U.S. perspective are

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

To address this issue, 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, has the most potential to be an offensive SIW “superpower.” Any lesser assessment of U.S. SIW potential compared with the SIW potential of other nations would be judged as laughable by those nations that are just beginning to speculate about the significance that SIW instruments may have in future conflicts. But how far has this 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 U.S. has well-developed and successful offensive command and control warfare (C2W), electronic warfare (EW), and other information warfare (IW) capabilities (for example, SOCOM is a master of psychological operations (psyops), and the military services develop and operate electronic warfare systems, as manifested in the large-scale use of C2W and the suppression of enemy air defenses in the Persian Gulf War), but these can hardly be characterized as “strategic” in the sense of this report. 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 mis-
sions 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 purposes, 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. Although some U.S. SIW offensive capability exists, its full potential is politically and militarily sensitive.

Beyond being a leading contender in augmenting its existing arsenal with offensive SIW capabilities, the United States, by virtue of its political, economic, and technological position 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 that are very dependent on information systems. It is geographically protected and currently has the world's most formidable conventional military capabilities. If the United States were to be defeated or thwarted militarily in the near future, it will probably 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 spectrum of threats and scenarios. 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 (such as storms and earthquakes), human errors (in software and control), and other purposeful mischief (such as hobbyist hackers and 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, nor do any appear to have been strategic in 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 attempt has been made yet?

Although a great deal of uncertainty surrounds the future vulnerability of information infrastructures, a number of trends can be observed that seem to point toward an expanded dependence on 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 payment systems (called cyberpayment), and plans for the delivery of critical services (such as telemedicine and government communications) over the GII all present potential targets for an SIW attack.

The defensive SIW assessment thus involves an assessment of information infrastructure vulnerability, threat potential, and vulnerability consequences. However, these assessments also have their problems. Existing information infrastructure systems are complex, dynamic, flexible, and interdependent. They are also public and private, and military and commercial. Some (such as those used in banking) have
been “hardened” by design because of the potential risk and cost of compromise. Others have evolved in a more benign environment with functions not related to threat (for example, cost, accessibility, and interoperability).

Standard risk assessment methodologies (fault-tree analyses, simulations, and red teams) have uncertain applicability and future analysis potential because information systems are very complex and threats can be very diabolical. Information security responsibilities are decentralized, and specific system vulnerabilities that are discovered are very sensitive and tightly controlled (for 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 them are “reasonable”). If known problems are hidden but not fixed, threats can be monitored and contingency plans developed, but associated risks may be impossible to measure in terms of direct (immediate) loss potential (such as human lives, repair and replacement costs, and opportunity costs while equipment is down).

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

1. **Number of offensive SIW players**: Unknown (but probably between 0 and a few).
2. **Tactical warning** (Is an attack under way?) and **attack assessment** (TW/KA) (If so, (by whom, how big, and at what?): The 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 IW is only one element of the conflict (but could be large if the perpetrator so desires).
3. **Damage assessment** (size and scope of damage): Significant damage will speak for itself; most critical damage assessment issues concern the potential for, and the 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 is concerning offensive and defensive SIW capabilities, people with informed opinions tend to fall into one of two 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 past 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 ensure appropriate defense mechanisms i.e., that there will never be such a thing as strategic information warfare. Determining the correct view between these two positions is less important than how we should proceed, given current (and 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 expressed in terms of the previously mentioned key dimensions of the first-generation SIW environment. Note the criterion “plausible and potentially desirable,” which eliminates possible end states such as a very large number of nations with “major-league” offensive SIW capabilities 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, an initial array of possible alternative first-generation SIW asymptotic end states might be

- **A U.S. supremacy in offensive and defensive SIW.** The United States overwhelmingly dominates the SIW environment because it possesses
  - The world’s best offensive SIW tools and techniques, capable of penetrating any other country’s SIW defenses
  - Highly effective SIW defenses and reconstitution and recovery capabilities, which it selectively shares with allies, effectively reducing the vulnerability of potential SIW targets in the United States (such as key U.S. infrastructures) to strategically insignificant levels
  - Traceback capabilities that result in a very high level of confidence in perpetrator identification capabilities, 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 group of highly competent SIW nations (5-10) emerges, with the United States almost certainly the most competent of the group. Mutual deterrence of SIW use is the common goal among club members. This handful of SIW “major leaguers” collaborates with each other to
  - constrain the spread of major-league SIW capability to other nations and non-nation actors
  - de-emphasize SIW and establish a norm of no first use of SIW
  - 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 fielding very high quality SIW defenses, the vulnerability of key potential SIW targets (including 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
— High-quality traceback capabilities (and/or a commitment to provide “whodunit?” traceback information in the event of a serious SIW attack).

— High-quality TW/AA) capabilities.

— Establishment of an SIW “arms control” regime along the lines of the BW and CW arms control regimes that establish international information operation norms, standards, legal restrictions, and enforcement mechanisms. Like currency counterfeiting, software piracy, and other threats to world economic order, SIW is something responsible states do not do. SIW rogues are dealt with as the U.N. dealt with Saddam Hussein: 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 is fast because
  — the natural strength of diversity in the globalization and standardization of cyberspace reduces overall vulnerability to SIW attack to moderate levels.
  — global cooperation provides high-quality damage assessment tools.
  — market-reinforced (“good neighbor”) cooperation insures rapid 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 can be applied to concrete decisions affecting many areas of public policy. For government actions designed to address SIW vulnerabilities, the framework provides a step-by-step process 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 thus involves

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

Table S.2 provides a sample set of alternative action plans for navigating toward the four end states mentioned above. The plans are based on decisions on those SIW issues in the “Low-Hanging Fruit” and “Tough Issues” categories (see the Key Strategy and Policy Issues Section). Note that, in some instances, more than one alternative is compatible with the indicated end state. (A more detailed description of some of the more cryptic entries in Table S.2 is provided in the body of this report.)

**CONCLUSIONS**

The strategy and policy decisionmaking framework and process, an evolving series of frameworks described above, appears to offer a useful means of organizing thinking
about the emerging SIW problem and achieving an inaugural action plan in this arena. It should therefore contribute to the ongoing effort to identify those 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. The issue of the appropriate forum(s) for such an undertaking also remains to be resolved.
### Table S.2

**Alternative Action Plans**

<table>
<thead>
<tr>
<th>Key Strategy and Policy Issues</th>
<th>Competition</th>
<th>Mixed (Competition and Cooperation)</th>
<th>Cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td><strong>Locus of Responsibility/Authority</strong></td>
<td>U.S. Supremacy in SIW</td>
<td>Club of SIW Elites</td>
<td>Global “Defense Dominance” in SIW</td>
</tr>
<tr>
<td><strong>Tactical Warning and Alert Structure</strong></td>
<td>Federal government leads; national security focus</td>
<td>Federal government leads; national security focus</td>
<td>Federal government leads; law enforcement focus</td>
</tr>
<tr>
<td></td>
<td>Joint leadership</td>
<td>Joint leadership</td>
<td>Joint leadership</td>
</tr>
<tr>
<td><strong>Declaratory Policy (Links with other Military Instruments)</strong></td>
<td>Strong retaliation threat (SIW retaliation emphasis); Reassurance on invulnerability of key infrastructure</td>
<td>Moderate retaliation threat vs. nonclub actors; Some reassurance on invulnerability of club infrastructures</td>
<td>No retaliation threat; Reassurance on resilience of GII</td>
</tr>
<tr>
<td><strong>International Information Sharing and Cooperation</strong></td>
<td>SIW programs compartmentalized</td>
<td>High degree of cooperation within club (G-7/FATF model)</td>
<td>High degree of cooperation institutional links through NATO, FATF, etc.</td>
</tr>
<tr>
<td><strong>R&amp;D/Investment Strategy Priorities</strong></td>
<td>National security-oriented protection goals</td>
<td>Coordinated defensive R&amp;D with Allies</td>
<td>Coordinate defensive R&amp;D with allies</td>
</tr>
<tr>
<td></td>
<td>Some coordinated defensive R&amp;D with Allies</td>
<td>Some proscriptions on offensive SIW R&amp;D</td>
<td>Proscriptions on offensive SIW R&amp;D</td>
</tr>
</tbody>
</table>