Chapter One

WHAT IS STRATEGIC INFORMATION WARFARE?

INTRODUCTION

"What is 'Strategic Information Warfare?'" was also the title for the first chapter in the initial RAND publication[1] on this emerging subject. The question bears repeating. Is there a useful political-military strategic concept, which can be called Strategic Information Warfare (SIW), that can be viewed as the intersection of strategic warfare and information warfare (see Figure 1.1)?

When considering this question and concept, what exactly does the term *strategic warfare* mean today, when compared with the past? What might the character be of

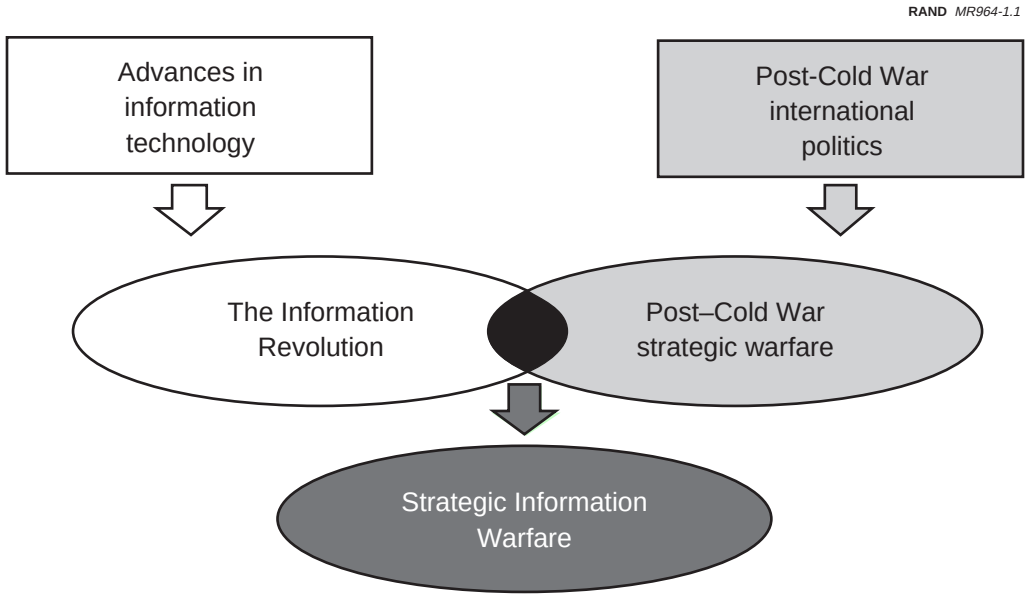

Figure 1.1—Strategic Information Warfare

[1]Roger C. Molander, A. S. Riddile, and Peter Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica, Calif.: RAND, MR-661-OSD, 1996.

strategic warfare in the future? What does the term *information warfare* mean today? What will it mean in the future? Is the concept of an intersection between strategic warfare and information warfare truly new—or has such a construct existed in the past?

A brief look at these and related questions follows, before the objective of this report, the development of a framework for facilitating near-term decisionmaking on SIW-related strategy and policy (and related) issues, is addressed.

WHAT IS STRATEGIC WARFARE?

The term *strategic warfare* is time honored. *Webster's New-Collegiate Dictionary*[2] offers the following definitions of *strategic*: "of great importance to an integrated whole" and "striking at the sources of an enemy's military, economic, or political power."

The *Concise Oxford Dictionary*[3] definitions are also noteworthy: "essential in war" and "designed to disorganize the enemy's internal economy and destroy morale."

During the Cold War, strategic warfare came to be synonymous with nuclear warfare, at least in the United States and the Soviet Union, almost to the exclusion of other potential forms of strategic warfare. But the end of the Cold War came very fast and very unexpectedly. No one in the United States or the Soviet Union (or in other countries) had given much thought to what strategic warfare would be like in the absence of the Cold War. For example, no one had considered what the character of strategic warfare might be for a global power like the United States in a multipolar world where plausible U.S. adversaries might have regional rather than global strategic objectives.

Some countries (Israel and Vietnam are good examples) had, in fact, been forced to think about strategic warfare in regional terms for many years (even though they were strongly influenced by the Cold War). Furthermore, much of the United States' major experience in-20th-century warfare outside the Cold War (that is, World War I and World War II) was largely regional strategic in character (although global in the sum of its parts). Nevertheless, the United States had not given much thought to how post–Cold War regional adversaries might seek to gain strategic leverage over the United States and its allies in a crisis or conflict, much less to how they might achieve such leverage through means other than a direct confrontation of conventional forces.

Might future regional adversaries, especially because the Persian Gulf War made conventional conflict with the United States so clearly unappealing, be highly attracted to the search for asymmetric strategies? Might they implement such strategies by exploiting weapons of mass destruction, such as nuclear, chemical, or biological weapons? Or by the selective exploitation of highly advanced conventional

---

[2]Merriam-Webster Inc., *Webster's New Collegiate Dictionary*, Springfield, Mass., 1997.

[3]*The Concise Oxford Dictionary*, Oxford: Oxford University Press, 1982, p. 1052.

forces emerging from the "Revolution in Military Affairs"? Or by the exploitation of the Information Revolution to hold at risk key national strategic assets (see Figure 1.2)? All of these strategies would appear to be distinct possibilities.

At the same time, the United States could face what might be called "global peer competitors" who would incorporate SIW as part of a broad array of strategic weapons with which to confront the United States (see Figure 1.3). When one couples the question of what is going to be in future strategic weapon arsenals (including new kinds of economic weapons) to the highly dynamic and multipolar character of the international security environment, it becomes clear why the future of strategic warfare appears to be highly uncertain in terms of both (1) the strategic objectives of prospective adversaries, and (2) the potential means for exerting strategic leverage that might be at their disposal.

WHAT IS INFORMATION WARFARE?

In contrast to strategic warfare, information warfare is a relatively new term that has found its way into the U.S. and international security lexicon only in the past few years, though the concept of the use of information in warfare is hardly new. The emergence of the term information warfare and its prominence can probably be directly tied to the Information Revolution, and to an expanding belief that this emerging revolution is so strong and potentially far-reaching that it could produce a new facet of modern warfare, or even a new kind of warfare.[4]

Through the mid-1990s, the term information warfare surged and then languished. It consistently defied clear definition, much less a consensus definition. Often, the term seemed too broad, encompassing traditional military areas, such as battlefield command and control warfare (C^2W) and other traditional forms of electronic warfare (EW), that were evolving in response to the Information Revolution, but not necessarily changing dramatically. Some of these more traditional forms of warfare had, in fact, been "driving" the Information Revolution.

Something new in the general information warfare arena was, however, gaining increasing credence: the possibility that future adversaries might exploit the tools and techniques of the Information Revolution to hold at risk (not to destruction but to large-scale or massive disruption) key national strategic assets, such as initial elements of the national military posture or the national infrastructure sectors.

The utility and the applicability of the term information warfare as a broad rubric thus became increasingly a matter of debate. In response, the DoD developed a new lexicon and typology for the broad subject of "information operations" as a more appropriate broad rubric for this general subject area, while acknowledging that in actual conflict some aspects of information operations will befit the label information warfare, if not strategic information warfare.

---

[4]Definitions of information warfare vary. An example of scholarship's relating information warfare to more traditional military challenges is included in Martin Libicki, *What is Information Warfare?* Washington, D.C.: Center for Advanced Concepts and Technology/National Defense University, 1995.

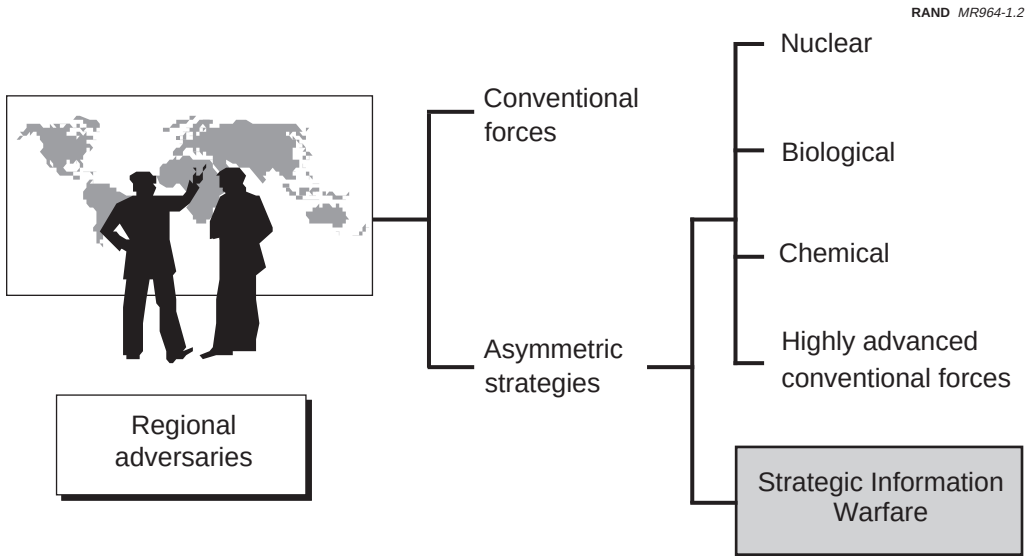

Figure 1.2—Asymmetric Strategies That Might Be Sought by Future U.S. Regional Adversaries

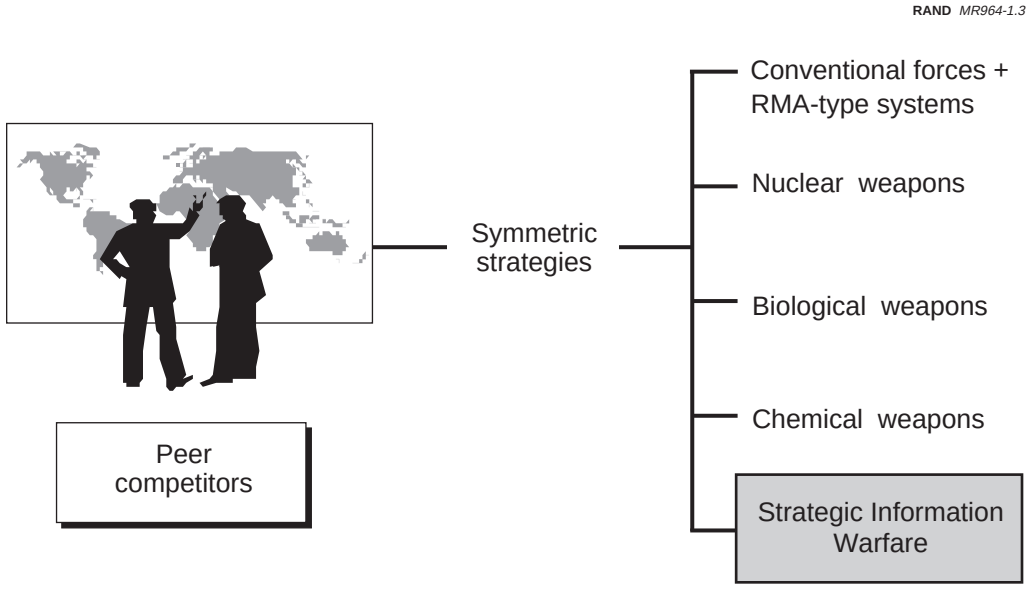

Figure 1.3—Symmetric Strategies That Might Be Presented by Future U.S. Peer Competitors

In this evolving definitional context, the use of the term strategic information warfare to describe what might be called the high end of the potential impact of the Information Revolution on warfare—a foreseeable intersection between strategic warfare and

information warfare—seems appropriate.[5] It was becoming clear that this kind of new strategic infrastructure threat could manifest itself in a future international strategic crisis or conflict involving the United States in two important ways[6, 7]:

1. A threat to U.S. national economic security. The holding at risk for massive disruption of key national infrastructure targets, to such a degree 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 that a regional adversary might use SIW attacks to deter or disrupt U.S. power projection capability. Concerns here include information warfare threats against infrastructure targets in the United States that are vital to overseas force deployment, and threats against comparable crucial infrastructure targets in allied countries. A key regional ally or coalition member under such an attack might refuse to join a coalition—or worse, quit one in the middle of a war.

The following section discusses whether there are precedents for such a strategic warfare concept, and how it might evolve in the long term?

THE HISTORY AND FUTURE OF STRATEGIC INFORMATION WARFARE

Has the concept of strategic information warfare, a strong information component of strategic warfare, existed in the past? How important has it been?

Although strategic information warfare is a relatively new term, the concept of an information component of strategic warfare is not. In fact, it may be hard to find any conflict worthy of the name strategic warfare that did not manifest some important information facet. (Sun Tzu, for example, recommended the creative use of information to achieve strategic objectives while avoiding conflict.) One could probably even note several historical instances in which fundamental changes in technology produced fundamental changes in the character of the information component of strategic warfare.

At the same time, the potential impact of the Information Revolution on strategic warfare may be unprecedented. Whereas strategic information warfare may, in the past, have played largely a subordinate role—in early times in the strategic impact of, for example, conventional armies and navies and later, likes of airplanes, rockets, and/or nuclear weapons—it might play a much greater role in strategic warfare in the wake of the Information Revolution.

---

[5]It is clear from the media and the international literature that the use of the term *information warfare* has increased considerably in both the public and the international arena, albeit increasingly as a shorthand for what is here labeled strategic information warfare.

[6]Roger C. Molander, A. S. Riddile, and Peter Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica, Calif.: RAND, MR-661-OSD, 1996.

[7]Roger C. Molander and Peter Wilson, The *Day After...in the American Strategic Infrastructure*, Santa Monica, Calif.: RAND, MR-963-OSD, 1998.

Moreover, 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 brand-new kind of information-centric strategic warfare that is worthy of consideration independent of other potential facets of strategic warfare.

Therefore, it would appear (see Figure 1.4) that SIW as the future intersection between strategic warfare and the Information Revolution might be thought of in the following terms:

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 (see Figures 1.2 and 1.3).
2. **Second-Generation.** 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 (for example, economic) and on time lines far longer (years versus days, weeks, or months) than those generally, or at least recently, ascribed to strategic warfare.[8]

As can be inferred from the above choice of terms, for established powers such as the United States, the authors tend to believe that first-generation SIW is more likely to be initially manifested. It is recognized, however, that is proposition is arguable. The United States, for example, might soon find itself in a situation in which it chose to exploit its current IT advantages and employ second-generation SIW, to prevail in a crisis that otherwise would have led to troop deployments and almost certainly to high numbers of casualties. See Appendix A for examples of a first-generation and a second-generation scenario.

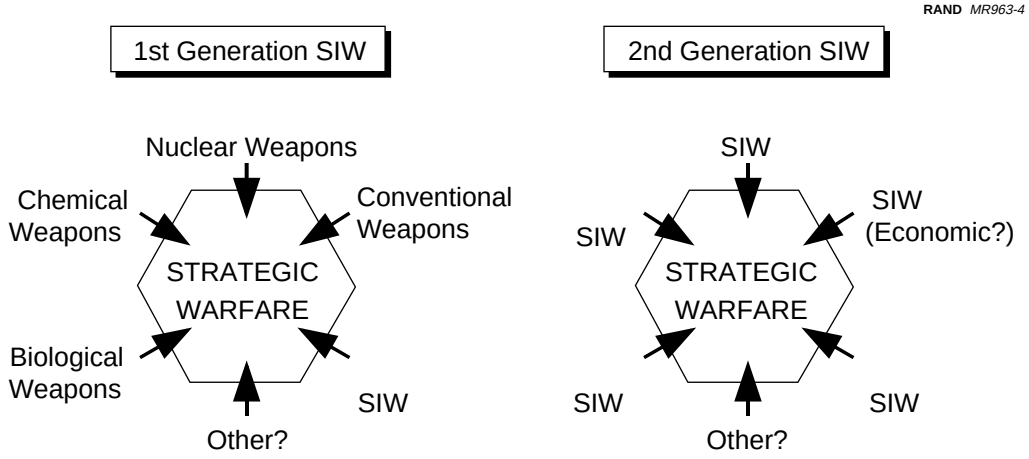

Figure 1.4—Two Concepts of Strategic Information Warfare

[8]See Ronfeldt and Arquilla, 1997, forthcoming.

For less-developed nations, which may not possess any other strategic weapons, second-generation SIW may be the first to appear. Second-generation SIW use by or against lesser powers might follow close on the heels of the demonstration of first-generation SIW.

Work to date has been able to identify a wide range of plausible examples of first-generation SIW. Most of these are rooted in the holding at risk for massive disruption of key infrastructures as part of a "combined arms" operation that includes the use of traditional military instruments of war. While the plausibility of such scenarios can be fairly well established, and there is great utility in their examination, it is far too early to discuss the probability of any such scenarios occurring according to any particular timetable.[9]

The authors found second-generation SIW scenarios more difficult to formulate. Not surprisingly, strategy and policy issues associated with such warfare are at this stage very difficult to conceptualize.

In light of this situation, this effort focused on the development of a decisionmaking framework for those problems associated with first-generation SIW concepts and their impact on established powers such as the United States (while also presenting at least one example of second-generation SIW in the next chapter).

Any substantial effort at this time to develop strategy and policy decisionmaking frameworks to address the types of problems manifest in second-generation SIW concepts for established powers such as the United States was viewed as premature, and best left to follow a more thorough examination of first-generation SIW concepts. There is, of course, a distinct possibility (if not the hope) that the approach to formulating first-generation SIW decisionmaking frameworks will prove to be highly useful in formulating comparable second-generation SIW frameworks.

---

[9]See Roger C. Molander, A. S. Riddile, and Peter Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica, Calif.: RAND, MR-661-OSD, 1996, and Roger Molander and Peter Wilson, The *Day After...in the American Strategic Infrastructure*, Santa Monica, Calif.: RAND, MR-963-OSD, 1998, for examples of two first-generation SIW exercise scenarios.