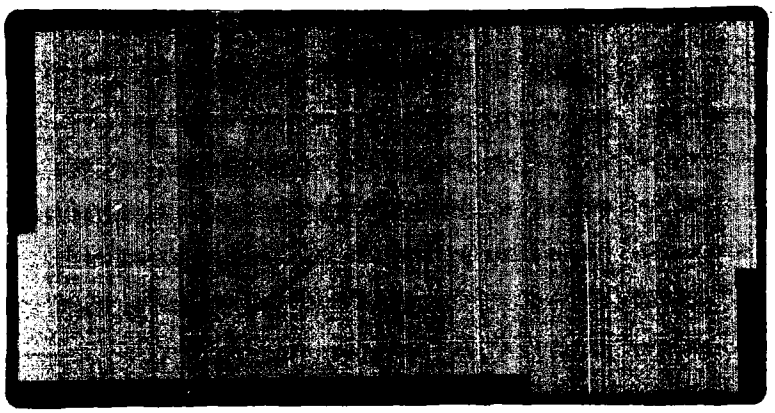

SAIC®

An Employee-Owned Company

DRAWING ON THE NUCLEAR AGE
WORKSHOP FINAL REPORT

WORKSHOP CONDUCTED
3-4 SEPTEMBER 1998

REPORT PREPARED BY
MICHAEL BROWN
ANDREW MAY

REPORT PREPARED FOR THE OFFICE OF NET ASSESSMENT,
OFFICE OF THE SECRETARY OF DEFENSE
CONTRACT NO. DASW01-95-D-0060, D.O. 19
SAIC PROJECT NO. 01-1175-04-7301-000
DOCUMENT NO. SAIC-99-6951+SAC

The Strategic Assessment Center
Science Applications International Corporation
1710 Goodridge Drive, McLean, VA 22102

DRAWING ON THE NUCLEAR AGE

Workshop conducted at the Strategic Assessment Center, SAIC, McLean, VA
September 3-4, 1998

CONTENTS

Participants 2

Executive Summary 3

Day I: September 3 9
- Introduction 9
- [redacted] Conclusions of the PCCIP 10
- Discussion 14
- [redacted] Developing a Doctrine for IW 15
- Discussion 16

Day II: September 4 35
- [redacted] Attacks on Networks 36
- Discussion 39
- Concluding Comments 42

Appendices
- [redacted] of the PCCIP ..... Appendix A
- [redacted] a Doctrine for IW ..... Appendix B
- [redacted] on Networks ..... Appendix C

ONE PAGE WITHHELD FROM RELEASE
PURSUANT TO 5 U.S.C. § 552 (b)(6)

EXECUTIVE SUMMARY

For several years, strategists have been struggling to develop a strategic framework for understanding Information Warfare. This effort has been complicated by the lack of a common conception of IW, uncertainty about the effects of attacks against the nation's information infrastructure, and vast geopolitical changes. We are faced, in short, with a new weapon (or, really, a group of weapons), the implications of which are not yet fully understood but which seem to promise a dramatic change in how we understand – and act out – armed conflict.

To lend some coherence to our conception of IW, some analysts have recommended that we look back to the development of nuclear strategy–another time in which the nation confronted a new weapon and a changing geopolitical landscape. Toward this end, the Office of Net Assessment contracted with the Strategic Assessment Center of SAIC to host a conference in which participants used nuclear strategy as a springboard to understanding the implications of the Information Warfare revolution and its implications for U.S. strategy. The conference was held at SAIC's McLean offices on September 3rd and 4th, 1998.

The participants' observations, concerns, and areas of agreement and disagreement can broadly summarized as the following:

The Strategic Use of Information Warfare

There was some disagreement as to the strategic uses of information warfare. One group believed that IW was a useful adjunct to military force. Members of this group believed it could be used to prevent or slow the deployment of military forces over seas, for example, or at the *operational* level against command and control, fire support, logistical and other kinds of information systems. A second group agreed that IW could be used in conjunction with other military methods, but thought it possible that information warfare itself could have a *strategic* impact. Participants cited several examples. In one set of instances, the adversary might use electronic attack or blackmail to slow America's response to a developing crisis, thereby seizing the initiative. A second example posited a sustained campaign of electronic attacks against elements of the banking system, communication networks, and other critical elements of the national infrastructure – all with the goal of significantly weakening U.S. self-confidence, international prestige, and economic might. Such a strategy might appeal to those actors that have as their objective the elimination of the "threat" posed by the spread of U.S. culture and Western values.

It should be noted that, in most of these instances, there are analogies to traditional uses of military force. Physical attacks on command and control systems and Lines of Communication to prevent or slow deployment are standard military techniques. Similarly, the use of physical military force to blackmail or coerce other countries and the use of military forces to erode an opponent's military and economic power are both – to a greater or lesser extent – traditional uses of military force. Yet, it should not be overlooked that the reliance on information networks as an element of national power does present adversaries with new frontiers and the potential for new kinds of assaults against the United States.

If it is true that these techniques can be used only as an *adjunct* to military force – as some of our participants claimed – it may be useful to explore the relationship between information warfare and traditional conflict. Is the use of information warfare at the theater level an inherent dimension of warfare in 21st Century? If so, what does that say about information-dependent military forces? If not, can we learn anything about the relation between IW and conventional conflict by studying the relationship between theater nuclear weapons and conventional conflict?

If, however, IW weapons can be used at the strategic level as an *alternative* to traditional military force, then they become strategic weapons in the same way that nuclear weapons were strategic – capable on influencing nations. If the effects of an IW attack were strategic in nature, we might be able to construct a framework by using the nuclear framework as a model. Some participants objected to this line of thinking by arguing that an information attack could not have consequences as devastating as those of nuclear weapons. As [redacted] noted, however, most analysts have focused on Information Warfare *attacks* rather than IW *campaigns*; it remains unclear how much damage could result from a carefully-planned and well-executed campaign of strategically linked IW assaults. Although the participants did not have time to adequately explore this issue, it is clear that drawing this distinction is crucial to any sophisticated understanding of IW and the ways in which it could be used to achieve political ends.

The Effects of Information Warfare

There was some debate over the likely effectiveness of Information Warfare. In general, the participants were in accord about the real danger posed by IW attacks: everyone agreed that networks are vulnerable to electronic and physical attack. Physical attacks could come from high explosives placed at critical nodes, or through the use of Radio Frequency weapons or High Powered Microwave. There was less agreement about the likely consequences of such attacks. To cite one illustration, there was uncertainty about how far the effects of IW attacks might spread and about the robustness of the nation's infrastructure: it is unclear whether the loss of some computers will cripple an entire network, and how the individuals using that network might

contribute to the damage by panicking. (Here, the most useful analogy is a bank failure, in which the real damage is caused by panic rather than systemic failure.) In this connection, many participants strongly recommended that the nation begin developing a method for simulating IW attacks and testing the robustness of complex systems.

This problem is complicated, the participants noted, by the extent to which networks have become a shared terrain. Because we share our networks with allies and adversaries alike, any changes we make to our own system will almost certainly affect these other users. In short, if we make the network more secure, we will also be affording protection to our adversaries; if we launch attacks that disable parts of the network, we will be affecting not just our enemy, but our allies and ourselves as well. (In this connection, [redacted] made a revealing analogy between the "blowback" of IW attacks and the inevitable spread of radioactive fallout.) Similarly, if we protect our networks and our allies do not do the same, their inaction will reduce the effectiveness of the defensive mechanisms we put in place.

In addition to the strength of the attacks themselves and the recuperability of networks, the effects of Information Warfare will also depend on the ability of society to function in the wake of attack. Although this question received less explicit attention, there was some discussion of America's resolution in the face of attempted blackmail by a nation prepared to launch a series of IW attacks against the U.S. There was general agreement that the nation would be highly unlikely to submit to a blackmailer's demands in such a situation. How long the nation might remain resolute in the face of continued attacks or a sustained power outage, or what the long-term consequences of such attacks might be, was not discussed in depth.

Attack vs. Defense

The participants spent considerable time debating how – and if – the nation could develop a viable defense against IW attacks. It was generally agreed that a meaningful defense – including one that served to place the price of attack beyond the reach of most nations – would be extremely valuable. Yet, there was among the participants little confidence that such a defense was possible, and universal agreement that it could not be implemented anytime soon. The notion that someone could identify the "key" components of the national infrastructure flies in the face of the increasing degree to which the elements of the infrastructure are interconnected and the ease of access to the entire network of networks. Even if the most critical pieces of the infrastructure could be identified, the cost to protect them would be significant. In this context, the group generally agreed that, for the time being at least, offense holds a considerable advantage over defense: companies are often reluctant to learn about, let alone resolve their vulnerabilities; offensive tools are readily available at low cost; the internet was designed for

openness and accessibility; and software is being developed so quickly that it is full of "holes," "backdoors," and other vulnerabilities.

The general feeling seems to have been that the nation's best opportunity for developing a viable defense rises from its leadership position in technological developments. As [redacted] noted, the nation will have, in the coming years, the power to shape Internet II: there are intrinsic aspects of networks that make security possible, and the nation that develops the networks of the future will have the power to make then as secure or insecure as it chooses. Such an approach, however, would change the instruments with which the United States has traditionally formulated its strategy. The State and Defense Departments, for example, might be far less important than Commerce or DARPA.

Deterrence

In the nuclear age, when the degree to which the offense dominated defense became clear, analysts developed the notion of deterrence in great detail. In the information age, however, the future prospects for deterrence are uncertain. There was among the participants a general belief that the old model of nuclear deterrence has been outgrown: most obviously, the group noted the degree to which IW lacks the sort of clear threshold characterizing nuclear warfare. Because low-level IW attacks occur almost constantly, it is extremely difficult to formulate the sort of highly threatening deterrent that predominated in the nuclear age.

Another factor complicating our understanding of deterrence, the conferees agreed, is the rise of a multi-polar – or perhaps more precisely a polycentric – global power system in which non-states share considerable power. Indeed, the decline of the bipolar cold war world and the increasing influence of transnational actors was a theme running throughout the conference. The absence of a nation state against which to retaliate makes classical notions of deterrence problematic. Moreover, transnational groups do not necessarily respond to the same cost-benefit calculations of nation states. Although there were many differences between the United States and the Soviet Union, there were a number of underlying similarities; both the U.S. and USSR were superpower nations, with organized bureaucracies, enormous land masses, sizable infrastructures, etc. These characteristics may not be shared by our adversaries in Information Warfare, and our conception of deterrence will need to be adapted accordingly.

The participants also focused on the problems posed by the fact that, to date, there has been no significant demonstration of the power of Information Warfare. Without the equivalent of Hiroshima or a test at Bikini Atoll, it is very difficult for the country to make a clear threat based on IW capabilities. Similarly, without clear evidence of the power of IW attacks, there is little

sense of urgency to develop a strong deterrent. The participants shared concern that the nation was complacent about the severity of the threat, and considered ways of increasing awareness. Although several suggestions were discussed, most participants expressed concern that no substantial action would be taken until an attack (or large-scale incident such as Y2K) demonstrated the nation's dependence on information networks.

Taking these issues into account, the participants had a difficult time developing a model for deterrence of Information Warfare. While some believed that the most appropriate analogy was criminal deterrence, others argued that this model would only work if the United States – or some other country – were willing to act as the world's policeman. Interestingly there seemed to be a willingness among participants to see the United States in such a role; not as a strategic actor, but as a policeman – a nation that could dictate solutions to other countries.

Alliances

The participants agreed that the cold-war era alliance structure was certain to change. Most agreed that, in the place of NATO-like organizations in which America's allies were essentially client-states, future alliances will be more numerous "regimes" of nations aligned on specific issues. Alliances will look less like a hub and spokes and more like a matrix, with groups of nations allied on some issues and not on others. Some participants argued that, with the decline of the nation-state, such regimes will eventually be open to NGOs. Looking back to the nuclear age, many participants cited the strains placed on alliances by the political significance accorded to nuclear weapons; some believed that focusing on such issue-specific regimes would allow us to avoid this problem in the future.

Competitive Strategies

Largely because of the decline of the bilateral cold war, there was some skepticism that our current approach to competitive strategies would be effective (and some thought that perhaps it had not been highly effective during the cold war). Most participants agreed that, even when the U.S. does engage in bilateral competition, as it may with China, it is unlikely to become the sort of structured, action-reaction cycle that characterized U.S.-Soviet relations. Further, because of the low entry cost of developing an IW capability, it may be difficult to use arms competition as a means of waging economic competition, as we did with nuclear weapons.

Despite this uncertainty, a few thoughts did emerge. As [redacted] noted, the goal in a competitive strategies framework is to force our enemies into adopting postures that we find less threatening; perhaps by developing an offensive capability we can force our likely adversaries to

divert funds toward the development of an IW defense. [redacted] suggested that we might be able to use DARPA as a strategic tool, perhaps using it to foster research in other countries into areas that we know to be dead ends. Thus, while strategic competition between the U.S. and our adversaries may not be so structured as it was during the cold war, there seems to be reason to believe that the competitive strategies approach will continue to yield valuable results.

Summing Up

Overall, there was clearly some utility in addressing the important "nuclear age" questions in an information age context. However, given other changes in the international environment (e.g. the proliferation of states and the increasing importance of non-state actors), and given the uncertainties of the effects of information attacks or campaigns, it is difficult to develop a strategic framework for information warfare. There are at least two steps that need to be taken. First, there is a clear need to understand better the implications of an information warfare campaign. Would the results be catastrophic, a mere annoyance, or somewhere in between? Would the nation be able to recover quickly or would the effects persist over months or years? This is an empirical question to which we need answers.

Absent an empirical answer to this most important question, it might be useful to conduct analyses based on assumptions: What if information warfare were proven to be as devastating as many of the pundits claim? How would we dissuade other nations from attacking? How would we attack others? How would that shape our alliance relationships? What would it do to the notion of competitive strategies? How would we avert "strategic blackmail?"

67 PAGES WITHHELD FROM RELEASE PURSUANT TO 5 U.S.C. § 552 (b)(5)