INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Defensive Strategic Information Warfare: Challenges for the United States

Gregory J. Rattray

Guest Presentations, Spring 1999

Charles J. Cunningham, Kawika Daguio, Patrick M. Hughes,
Peter H. Daly, Walter Jajko, David J. Kelly, Gregory J. Rattray,
Michelle K. Van Cleave, Robert T. Marsh, Randall M. Fort

June 2000

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-63-1 **I-00-2**

Defensive Strategic Information Warfare: Challenges for the United States

Gregory J. Rattray

Major Gregory J. Rattray, USAF, is chief, defensive information warfare integration, Directorate of Intelligence, Surveillance and Reconnaissance, Headquarters, USAF, Pentagon. Immediately prior to his current assignment, he was a full-time doctoral student at the Fletcher School of Law and Diplomacy, Tufts University, receiving his Ph.D. in 1998. His previous position was at the Air Force Academy in Colorado Springs as an assistant professor of political science and deputy director of the USAF Institute for National Security Studies. He served as an intelligence officer at Headquarters Strategic Air Command, Offutt Air Force Base, Nebraska, dealing with arms control and national intelligence estimates from 1989 to 1991, and with the 18th Tactical Fighter Wing, Kadena Air Base, Okinawa, Japan, from 1987 to 1988. He is a term member of the Council on Foreign Relations and co-editor of Arms Control Towards the 21st Century, Lynne Rienner Press, 1996, as well as the author of numerous studies and articles on arms control, proliferation, and conflict in the information age. Major Rattray received a B.S. in international affairs and Military History from the Air Force Academy in 1984 and an M.P.P. from the John F. Kennedy School of Government, Harvard University, in 1986.

The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Rattray: Let me just give you a little background about where I'm coming from. I'm an Air Force officer still on active duty. I actually came to Harvard right after I graduated from the Air Force Academy, so I've been in this building, on and off, for about 15 years. I'm an intelligence officer by trade, but I also have taught at the Air Force Academy, and the Academy gave me the opportunity to come back and do a Ph.D. At that time, I decided that I would get out of the area I was in, which dealt with strategic nuclear warfare and arms control. In the early 1990s, proliferation was starting to come on the scene as an important national security concern. When I was teaching at the Air Force Academy, I picked up a book called *War and Anti-War*, by the Tofflers.[1] I cotaught a course in the spring of 1994 using that book. When I went off to get a Ph.D., I decided information warfare was really the next wave of warfare that we needed to understand better. So, that's how I ended up writing this massive tome on strategic information warfare (SIW).

I went down to the Pentagon last summer, so I've been there for about nine months. I'm the deputy chief of the Air Force's Defensive IW Division at Headquarters, Air Force. We work for the Operations Directorate. Just as we have air operations and space operations in the Air Force, we also have information operations. My job is to help the Air Force make information operations emerge as a real warfighting capability. We also work a lot with the communications and computer community, which has the technical expertise in the IW realm, particularly the cyber realm.

What you're going to see this afternoon is definitely an approved presentation that has gone through a security and policy review, but it is not the DOD's official position on these issues.

This afternoon I'm going to start by discussing what I think SIW is. I think that is the least-understood dimension of what constitutes the subject that people label as IW.

[1] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown, 1993.

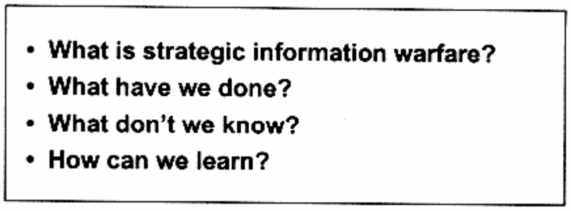
What you're going to see is primarily based on what I wrote in my dissertation.

I wrote myself a note flying up on the airplane this afternoon that when I introduced this I needed to start off with the kind of statement that I always forget until the end. That is: I will discuss a lot of things that we have yet to do or that are difficult to do, but we've made a lot of progress. One of the main things I did in my dissertation was compare SIW to the evolution of strategic air warfare from the end of World War I to the beginning of World War II, and analyzed it in decades-long timeframes. They knew at the end of World War I that they had to deal with strategic air warfare. Yet, in 1942, they were not that well equipped to do that, even though conceptually they'd been working on it for 25 years.

My starting point is the early 1990s. We're now eight or nine years into working on what I call SIW, and we've made a lot of progress. We've been proactive. We haven't suffered through what I would term a large-scale strategic information war, yet the U.S. government has issued a Presidential Decision Directive (PDD) to deal with cyber defense. Congress has even been involved by mandating that the President deal with the vulnerabilities of our critical infrastructures. We in the Pentagon spend a lot of time standing up new organizations in order to deal with some of these things. I was telling people at lunch that we've got an INFOCON (information conditions) system, similar to DEFCONs (defense conditions) and THREATCONs (threat conditions), by which we manage our protective responses to growing cyber threats. We're starting to institutionalize that system. So, while I'm going to talk a lot about limitations and potential areas for more work, I do want to start off by saying I don't think the situation is all bad, and I believe that we've done a lot that is positive. The question is how we continue to make progress most effectively

This presentation is really designed to take 40 minutes or so. This gives me a little luxury not to have to speed through these slides the way I've done it in the past. We should then have a considerable chance to discuss either things that come up in this presentation or, within reason, I'll field questions about things that I'm doing down at the Pentagon. I'm not going to get into whether the Kosovo policy is right or wrong. I don't think anybody can answer that question at this point.

I phrase this presentation in terms of answering questions, because my take on this area is that there are still important questions that are open and need to be answered, and you need to think about how to get yourself the most leverage on the answers (figure 1).



- **What is strategic information warfare?**
- **What have we done?**
- **What don't we know?**
- **How can we learn?**

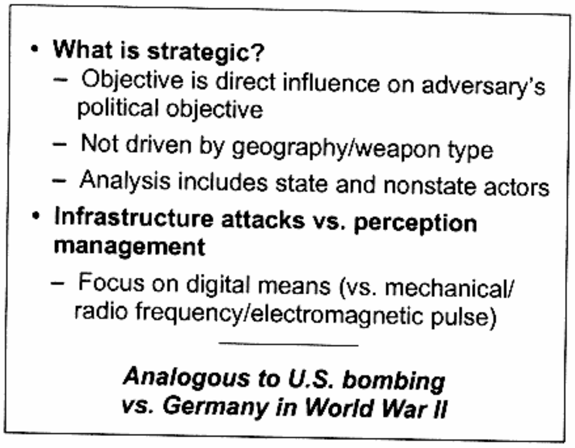
Figure 1

Overview

You'll read about IW and hear people asserting that they've discovered the answer. I advocate that if you hear people being too dogmatic about what they're saying, you ought to be skeptical right from the start, because there's not very much empirical basis to make strong assertions about IW at this point. So, I'll talk to you about what I think IW is, or at least the segment that I dealt with and continue to deal with; the types of things that we've done—how we got to 1999 in terms of the preparation of the United States to deal with an adversary's digital attacks; what things we don't know very much about, and poke at the conventional wisdom that's already grown up around this subject; and then suggest some things that we can do in terms of learning about what the reality is out there in terms of protecting our information infrastructure.

I took this course in the spring of 1996, and I sat through much of it the following two years while I was in Cambridge. IW came up a lot during the course while I was here. There were always vague definitions being discussed. I believe that the Department of Defense has a pretty firm idea now what it means by IW. If, in the second hour, we want to talk about the doctrine (i.e., the conceptual framework) that the Department of Defense uses for IW, we can do that.

What is not yet well attended to is what we mean by SIW (figure 2). We definitely believe that there are strategic, operational, and tactical levels of IW. The problem is that at the strategic level, where national policy comes into play, the Department of Defense has to fit into its role and that has yet to be well defined in terms of SIW. So, I still think it is useful to try to talk about what we mean when we say "strategic information warfare."



- **What is strategic?**
  - Objective is direct influence on adversary's political objective
  - Not driven by geography/weapon type
  - Analysis includes state and nonstate actors
- **Infrastructure attacks vs. perception management**
  - Focus on digital means (vs. mechanical/ radio frequency/electromagnetic pulse)

Analogous to U.S. bombing vs. Germany in World War II

Figure 2

Definitions and Boundaries

The applicability of this slide is actually going to atrophy over time, because when I came up in the military in the mid- to late 1980s, "strategic" meant intercontinental nuclear weapons. It was based on the type of weapon you were using—nuclear—and weapons with intercontinental range. We had lost the 19th century, Clausewitzian conception of "strategic" as activities directed at achieving your political ends, exerting direct influence on the adversary to get to the objective of why you're engaged in the conflict in the first place. SIW is not about winning on a battlefield, but rather going directly after the enemy's centers of gravity in order to win in a conflict. In air warfare, you might go after his ball-bearing plant so that he can't produce the necessary parts for tanks and artillery and airplanes, or go after his war-supporting infrastructure, or you might try to disable his power production systems so there's no electric power, and his populace gets tired of suffering and exerts pressure on the political leadership to get out of the war. That's what I mean by strategic. It's not driven by geography or weapon type. One of the very relevant new dimensions of this realm is the potential for nonstate actors actually to conduct strategic warfare because of the nature of the digital weapons you can use to disrupt the other guy's centers of gravity.

I'm pretty much going to talk about attacks on infrastructures. Just as you can physically bomb a telecommunications switch, you can jam a microwave link in a communications system. You can go in digitally. In the dissertation, I used the term "microforce." Digital attacks actually involve the use of physical energy to accomplish your goals, so I'm staying in the physical realm when I'm talking about infrastructure attacks, even if I mean bits and bytes and electrons. Flipping energy states in a microprocessor is still physical. That's one thing Professor Oettinger and I talked about a lot while I was doing this: that cyberspace tends to be painted as a virtual or nonphysical realm with completely different rules. My belief is that you've got to continue to think about it as a physical environment. You might need new types of people who understand this kind of environment, just as you need people who understand air and space and people who understand the ocean. But it's still a physical warfare environment.

What I'm not going to talk about, but which is part of the Department of Defense's IW concept, is perception management: doing things to the other guys through the media, through psychological operations, or through deception to make them believe something. Those activities are important—some people would argue more important than evolving new means for infrastructure attacks—but that's not what I'm talking about today. The analogy that I will draw on heavily is the run up to World War II, when they thought they'd be able to take down an adversary's war economies and general economies through air attacks against precise points. Does that capability exist in the information realm or the cyber realm?

As I go through this, if anybody has questions or believes that I've mischaracterized something (because I'm going to make some fairly strong assertions), please rebut me or ask questions at the time. I would prefer that this evolve as a dialogue rather than my simply telling you what my world view is and trying to interact afterwards.

I really struggled hard to find definitions from which I can move forward in terms of what information infrastructures are, and which ones are important. This slide just tries to point to sets of activities supported by information infrastructures that could provide centers of gravity for an adversary to go after (figure 3). The first four are the types of things identified in the President's Commission on Critical Infrastructure Protection (PCCIP) report, and are already heavily attended to under the critical infrastructure protection efforts in the country. I broadened the definition to include the general commercial users of infrastructures, in addition to the infrastructures themselves. As an example, if someone could crumple the information infrastructure of corporations like Dupont or Ford, engines of the American economy, I feel that would also be a center of gravity that an adversary could go after.

- **National security**
- **Vital human services**
- **Other government services**
- **Public utilities and transportation**
- **General commercial users**
- **Commercial technology producers**
- **Commercial and network service providers**

Figure 3

Key Sectors of Activity Involved in the Use and Operation of Information Infrastructures

Student: What do you mean by vital human services? Hospitals?

Rattray: Medical services, fire, police, 911; those sorts of things.

Student: You've mixed categories. National security is an entirely different concept from the six other categories. I can look at the term "other government services" and even if I cannot identify exactly what they are, I have some idea. But how about national security?

Rattray: If I put "national security establishment," would that have refined my categorical problem? Really what I'm talking about are those institutions that we in the United States call national security institutions—the Department of Defense, the intelligence community, and so on.

Student: National security institutions, rather than national security?

Rattray: Right. Because, as you say, these are identifiable organizations. This is a concept that could include protecting all these other things.

Student: The others are functions or consequences of the institutions, right?

Rattray: Right. It would be like saying "good health" instead of "vital human services," but I agree.

I like this diagram for a number of reasons (figure 4). It presents a very simplistic view of information infrastructures: the sets of players that have to work together to produce functionality for national security, for vital human services, for an organization to use an infrastructure to accomplish a purpose. When you start to peel back our national infrastructure protection efforts, you can use this diagram to point to where the efforts are going or not going.

There is a set of players that produce software or hardware, and that get together and collaborate on the establishment of standards. These are the players I'm calling the technology producers—Bay Network, Cisco, Microsoft. They create the pieces that the network and service providers or operators, such as AT&T, put together. You can obviously have an organization that performs both roles. Microsoft produces technology, but it also runs the Microsoft network, in which case the organization is conducting two sets of activities necessary for information infrastructure operations. Then you've got sets of players that use information infrastructures for productive purposes.

As we talk about this, I'm going to refer back to the idea that most of the attention right now in our infrastructure protection efforts focuses on the two bottom layers. Yet, these activities rely on products that come from the top layer and constitute the

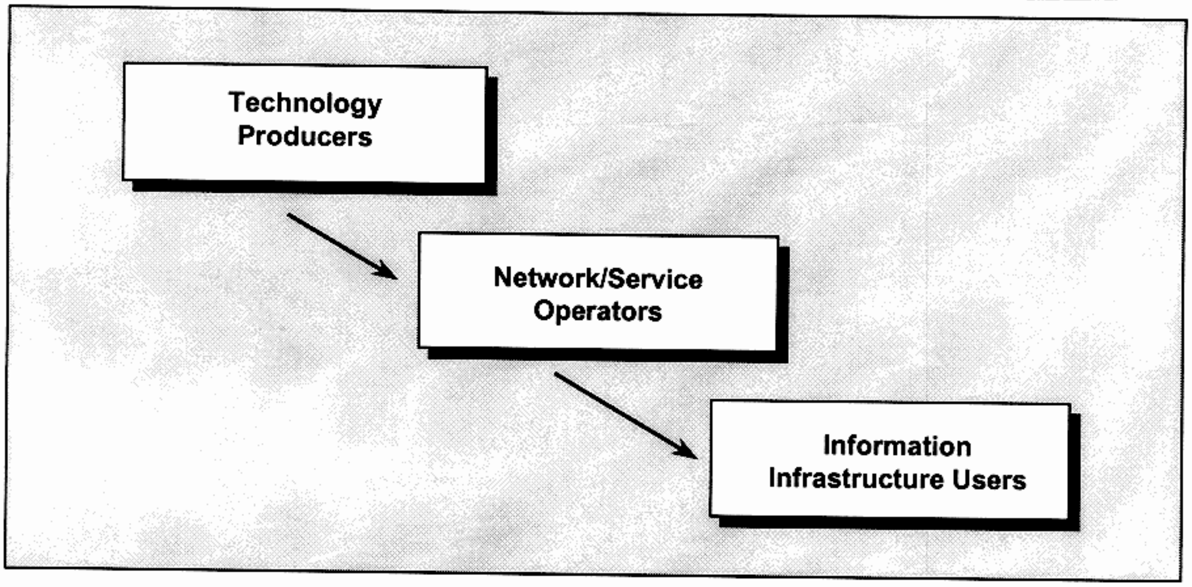


Figure 4

Components of Information Infrastructures

foundations of an information infrastructure as put together in the middle layer. If you have problems at the level of the information infrastructure use downstream, you have to go back and start to patch and fix them, whereas if you had employed technologies that didn't have a lot of vulnerabilities to start off with, you'd have less of a challenge in terms of infrastructure protection at the network/service and user levels.

Student: I was just reading an article last week about Microsoft. They actually are planning to decentralize the operation into a similar structure rather than being dictated by the operating system. So, within Microsoft they want to make fences between network operators and technology producers and customer service.

Rattray: The technology product segment has been a dominant locus of activity in Microsoft, and now they want other activities …

Student: … to be of equal size or equal weight in the company.

Rattray: My dissertation had two major themes going on at once—one about technology and how you orchestrate it for a productive purpose, and one about the nature of strategic warfare. I've just captured most of what I'm going to talk about in terms of the technology dimension. I'm going to spend the next 20 minutes or so on strategic warfare, and the key factors that allow you to conduct strategic warfare successfully. I'm not going to talk in depth about the technological orchestration that you might have read about in my dissertation.

I analyzed the evolution of strategic warfare, particularly in the 20th century, and the evolution of air warfare through different phases: the run up to World War II, as well as the inability of air power to achieve its objectives in Vietnam. A lot of people would argue we're facing the same types of challenges in Kosovo right now. I also looked at nuclear warfare. I tried to cull out the types of generic enabling conditions you would need to conduct strategic warfare successfully, so that I could go forward and analyze what you would have to be able to do if someone were actually to wage SIW (figure 5).

First, you have to have what I call offensive freedom of action. In air warfare, that meant the B-17 could get over Germany and deliver its bombs, or in nuclear warfare that the missile could make it to its target and not be intercepted by antiballistic missiles. The

- **Offensive freedom of action**
- **Significant vulnerability to attack**
- **Vulnerabilities can be targeted and attacks assessed**
- **Prospects for retaliation/escalation minimized**
- **Presence of effective command and control**

Figure 5

Enabling Conditions for Strategic Warfare

offense must actually get to its target. The targets must be vulnerable to damage by the destructive mechanism that the vehicle carries: the bombs could destroy the ball-bearing plants, the nuclear weapon could destroy a city. In these cases, it was much clearer that the weapon would actually achieve the intended result.

In the digital realm, when you send a stream of bits or you launch a virus at an organization or sets of computers, you have to know that you are going to be able to deny service, to get in, and to gain control. You have to know that the Melissa virus will cause an overload of servers because the e-mail system is flooded.

You have to be able to figure out what you're targeting. In the case of airpower, you pick key adversary systems that you can attack, and then you have to assess whether you hit them once attacked. In air warfare, battle damage assessment is a constant challenge: once you drop your bombs, can you tell if they hit their targets and if you've had your effect? Fortunately, we never had much actual experience in finding out whether we could do that in nuclear warfare. We had pretty high confidence that we could hit the things that we wanted and make sure that the results were what we expected.

But, if strategic warfare is going to be successful, particularly a cyberwar, it's not a viable way to achieve your objective if the other guy can basically respond in kind. Similarly, self-deterrence may occur if you believe he can respond with different means, whether he'll use conventional weapons or actually go to nuclear weapons, and ratchet up the damage to you. So if stepping on what used to be called the escalation ladder is more dangerous to you than it was for him, then it's not worth doing.

That definitely comes into play in cyber warfare with state adversaries who might launch attacks at other states. If the targeted state can respond with more damaging physical force, it's not clear why you would ever start to get into the cyber warfare game. The Russians have publicly declared that an attack on their nuclear command and control with IW legitimizes a nuclear response. How much of that is bluff and bluster is open to question, but this idea of escalation dominance is an important one. It's also very important in terms of nonstate actors, because if nonstate actors launch cyber attacks on us, what do we do in response? It's much more difficult to resort to kinetic physical force, so we'll have more difficulty achieving a deterrent effect.

Then you must have effective command and control. In the air and nuclear realms, that wasn't so difficult. In the cyber realm it may be more so.

This is where I came out (figure 6). It synopsizes about 100 pages of my analysis.

- **Offense can get through**
  - Depends on sophistication and preparation
- **Important vulnerabilities exist**
  - Depends on actor's goals and presence of key nodes
- **Discerning targets and damage difficult**
  - Insiders, sloppy security and time help
- **Escalation and retaliation advantages to the less technologically advanced and nonstate actors**
- **Command and control may prove a challenge**
  - Insiders tough, issues of collateral damage

Figure 6

Enabling Conditions and SIW

There are some bold assertions here. If anybody wants to disagree, we could certainly work through the validity of the assertions I make about SIW. What I tried to do in the sub-bullets is to point out mitigating conditions or the considerations that you need to take into account when I make an assertion like, "Offense can get through." My belief is that right now it is questionable whether kid hackers can get through, but that sophisticated state opponents will be able to get through. In other words, how far you get through, and what you get through to, depends on your sophistication. Whether you are detected as you try to get through the networks definitely depends on your sophistication and your level of preparation.

More time helps, in a couple of different dimensions. That is, going in slowly, as you gather intelligence about what you're going to attack and you prepare to launch an attack, makes it much more difficult for the defense to see you coming. If you had to generate a cyber capability quickly and launch an attack at an adversary in a period of weeks or months, I think that would become obvious much more easily than if you were preparing for years to get ready in case you have a conflict. That affects your ability to get through.

Important vulnerabilities exist. I'm going to talk a lot about what we know and don't know about key nodes in our infrastructures. I do believe that we are highly reliant on computers for critical warfighting functions, and that different portions of those centers of gravity in the commercial sector and the vital human services sector rely on information infrastructures so much that if they were hit by cyber attacks we could lose important societal functions and it would be very painful for us.

It does depend somewhat on what the actor is trying to achieve. The gross distinction I make here is the ability to throw hand grenades versus shoot somebody directly in the head. In the cyber realm it's a lot easier to throw hand grenades right now than it is to pinpoint your attack at something that's very damaging to your opponent without causing much collateral damage. If you're the type of actor who can achieve objectives by throwing hand grenades and causing indiscriminate pain, SIW is probably a more viable option for you right now than if you have to go in there surgically and hit very limited things because you're worried about the possibility of reprisal, or your own populace's disdain for causing widespread disruption—or death, in the case of messing up medical systems and that sort of thing.

Student: So you think strategic warfare is less controllable right now?

Rattray: I think cyber strategic warfare is not very easily controlled. There's a lot of talk out there about "The electron is the ultimate precision weapon." I think that's significantly overstating the case.

Oettinger: There is underneath that a technical point that is often overlooked because it is both subtle and difficult to discern. Let me try to make it clear by using an analogy with a highway. Just to summarize what I want to say, it has to do with the degree of coupling of the various elements of the system. If it's loosely coupled, you can target some piece, but not much may happen. If it's tightly coupled, you can target some piece and an awful lot may happen. The question of sharp targeting or predicting effects depends very significantly on this question of tight versus loose coupling.

Now, let me give you the instance. You're driving on a highway, and everybody's tailgating. That's a very tightly coupled situation. One car comes to a stop, or there's an obstacle on the road, or a terrorist has bombed the bridge, and you get six miles of a 300- or 500-car crash, and all hell breaks loose. If everybody is driving a mile apart, one car may go off the bridge, but everybody else will come to a stop and nothing will happen. It will be like somebody driving a car into a telegraph pole: it's tough for him, but you don't get maximum effects.

That happens to be an instance where this question of tightness and looseness of coupling is fairly easily discernible. In the kinds of targets that we're talking about here, it's difficult even to frame the question of whether you're dealing with something that's tightly or loosely coupled; ergo, discerning targets and damage and pinpointing and getting accurate effects becomes very difficult. A lot of the arguments over IW tend to neglect this question because it's a very hard one. In many instances, people don't even know if they should be considering it. But even among cognoscenti, it's a hard one to discuss because there is very little known and understood about what this is.

You're also dealing in a realm where the nature of the technology is changing very rapidly. So, the question of whether what is true today at noon is true tomorrow at noon or next year is itself another difficult question. It's a consideration that you should keep in the back of your mind, at least as a question. There are very few answers.

Student: Would you draw a parallel between IW and biological or chemical warfare? When the wind blows the other way, you run the risk of harming your own people, even in the laboratory.

Rattray: There's a possibility at two levels. There's definitely a possibility of unintended consequences. You think what you hit is not tightly coupled or networked to something. It turns out that it is, and you've got this cascade of unanticipated effects. I hear a lot of talk about potentially cascading into our friends, our allies, even back to ourselves, due to the existence of global network connectivity. I think that may be a little bit of a hype. Figuring out how you would hit another guy's network, and how that would blow back and cause problems in Western Europe or the United States, is difficult for me. It's possible, especially if you start to try to go after communications outside of its country. Then it quickly becomes an issue of whether you get blowback against yourself.

Student: In both Iraq and in Serbia, the systems they are using are 1960s Soviet types of equipment. Iraq is mostly a public sector country. Everything is run by the state; people cannot buy typewriters for their own use. But if it's Taiwan or any other country that is much more closely integrated into the international market, then that effect might be much stronger.

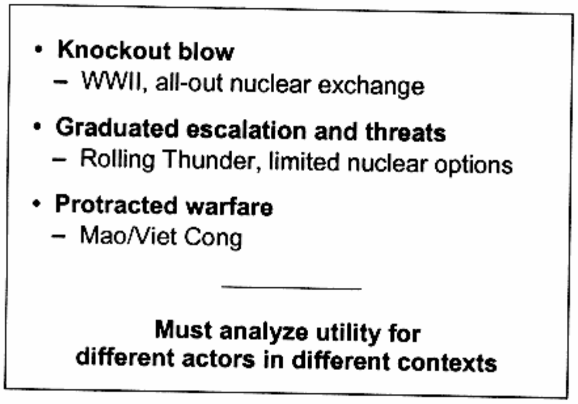
Rattray: In the reverse case, most of the people we would go after, even if they were networked with somebody else, are probably not networked with close allies of ours. If an adversary went after Fidelity, it would affect other countries. Fidelity has extranets that tie it globally into the world economy. If you denied service to Fidelity, other people would be impacted around the world. They would mostly be Western, democratic, capitalist countries, but a lot of our adversaries wouldn't particularly care that they had damaged them.

Student: The idea that I had in mind was, for example, just hypothetically speaking, that the United States hit China. Hong Kong is part of the so-called capitalist world, and it might have a repercussion on Hong Kong, which would have repercussions on such neighboring countries as Taiwan, Japan, Korea, and so forth.

Oettinger: Speculating on that is a very interesting sport, but the empirical knowledge required to put teeth into what you just said is enormously detailed. It really depends very much on the details of coupling and, even if there is coupling, on the ability to detect something happening and decouple. One of the ways you avoid an umpteen-car crash is by being alert and swerving over to the side and passing or doing something else. I cannot overemphasize the difference between in-principle speculation and empirical knowledge of specific targets and of a specific situation at the time when you hit it.

Rattray: We've gone to the bottom line of my presentation in the last 10 minutes. It's really the lack of empirical basis that we are working with today, and some frameworks for thinking through these things, that I'm going to discuss.

Among the things that I think are useful to think about is that there are different ways to conduct warfare campaigns (figure 7). Usually, when we talked about strategic warfare, especially in the U.S. context, we talked about launching a knockout blow on an adversary through an all-out nuclear exchange, or in World War II about disabling our opponent through the use of strategic warfare. We have believed, and continue to believe, that we can use strategic warfare to ratchet up the pain and show our opponents that it will get worse if they don't give in to our objectives. This is called "graduated escalation." We did this in the Vietnam War: give the enemy the opportunity to surrender; if he doesn't surrender, go ahead and hit him harder, and show him that it is not in his interest to



- **Knockout blow**
  - WWII, all-out nuclear exchange
- **Graduated escalation and threats**
  - Rolling Thunder, limited nuclear options
- **Protracted warfare**
  - Mao/Viet Cong

Must analyze utility for different actors in different contexts

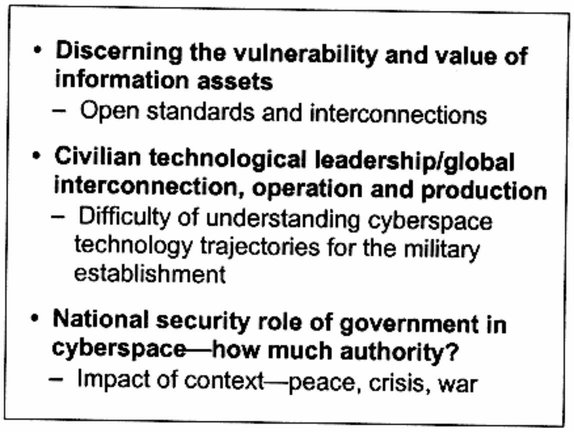
Figure 7

Potential SIW Campaign Approaches

continue this conflict. You could certainly try to do that with IW, but it probably—and I would argue maybe to an even greater degree—suffers from the difficulty this type of warfare has always had succeeding because the other guys can recover during those periods when you're letting up.

I don't think enough attention has gone to the possibility of protracted warfare, as in a guerrilla campaign or the classic Chinese approach advocated by Mao: an adversary who comes in, hits you at your weak points when it's advantageous for him, and then runs and hides over a period of several years. If we develop adversaries who take that approach to us in cyberspace, especially if they don't have a physical center of gravity that we can hit back at, this could become very threatening to us. It may be the most effective way of conducting this type of warfare against the United States. I don't think that much of the dialogue about the potential importance of SIW talks enough about IW waged in this fashion. The utility of any of these types of campaigns depends on the actors and what type of objective they're trying to achieve.

I think these are the primary challenges (figure 8). We already talked about the difficulty of discerning what the key nodes are and the value of those key nodes. The fact that we've moved more towards open standards and become highly interconnected makes this an even more difficult challenge. You don't have state-owned, centrally controlled sets of infrastructures to understand. Now these things are all linked together.



- **Discerning the vulnerability and value of information assets**
  - Open standards and interconnections
- **Civilian technological leadership/global interconnection, operation and production**
  - Difficulty of understanding cyberspace technology trajectories for the military establishment
- **National security role of government in cyberspace—how much authority?**
  - Impact of context—peace, crisis, war

Figure 8

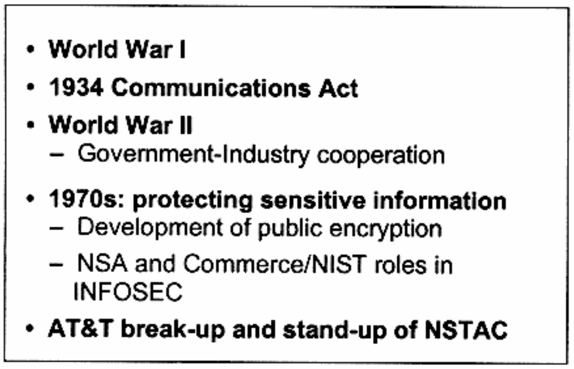
Defensive Challenges for U.S. National SIW Efforts

The leadership in this realm is in the commercial or civilian sector. In the 1950s and 1960s, the Department of Defense pretty much led the development of information technology through the nuclear programs and the space program. Now, the cutting-edge technologies are developed outside of our control and we're scrambling to catch up to implement those sorts of things.

Something that we bring up all the time, but don't have easy solutions to, is that today's technology is produced globally. I heard that most Y2K fix software is produced in India and Israel rather than in the United States. I don't want to evaluate our political relationships, but India's clearly not a place where we could definitely rule out conflicts of interest. We haven't figured out a way to estimate the risks involved in having our systems based on software largely programmed in India, and on contracting out development of commercial software, as well as defense and other government software, to those places. I'm going to talk, as we go along, about the proper role of national security and the government in managing information infrastructures, and argue that it depends on the context.

I'm going to try to do this more quickly. I'm already seeing that, just as with my dissertation, I'm being long winded and it's taking longer than I thought.

The next segment is a mostly historical section on where we've been. This slide shows the macro history with regard to telecommunications and national security (figure 9). The U.S. government has considered management of telecommunications issues as a national security issue for a long time. It didn't just happen in the 1990s with the "information age" and the advent of the Internet. We nationalized AT&T in World War I. We did it again in World War II. The 1934 Communications Act was the first major legislative framework for how the government interacted with AT&T. This act made a major point of giving the President authority to control our telecommunications systems in a national security emergency.



- **World War I**
- **1934 Communications Act**
- **World War II**
  - Government-Industry cooperation
- **1970s: protecting sensitive information**
  - Development of public encryption
  - NSA and Commerce/NIST roles in INFOSEC
- **AT&T break-up and stand-up of NSTAC**

NIST = National Institute of Standards and Technology

Figure 9

U.S. National Security and Telecommunications

In World War II, AT&T cooperated very heavily with the U.S. government. Bell Labs was a big supporter of the war effort. Microwave communications were developed during World War II. This cooperation paid benefits during AT&T's continual fight to avoid being broken up as a monopoly for the next three decades, but they eventually lost that fight.

In the 1970s, as we started to realize that we passed around important information on unclassified networks that weren't covered by encryption or developed by the government for classified information, we started to allow the development of public encryption. There was a big debate in the 1970s, which continues to this day, about the proper role of the government in regulating the ability of people to use encryption. The big debate today is about whether or not we allow the export of strong encryption.

Finally, as we've already mentioned a couple of times, in 1984 AT&T was broken up. The Department of Defense strenuously objected to that. At the time, the major concern was AT&T's role in supporting the command and control backbone for nuclear operations. Yet, despite the objections of the Department of Defense, I think it was a watershed. Commercial interests dictated that we needed to break up AT&T because everybody had to have the benefits of cheaper telecommunications services, even if it was going to cost us in terms of national security. That happened early in the Reagan Administration, when the Cold War was at a renewed level of tension. They did establish the National Security Telecommunications Advisory Committee (NSTAC), which allowed the government to communicate with all the new telecommunications providers and try to provide an orchestrated means for securing the communications the government needed during emergencies. Way back in 1984, we were trying to deal with this issue of public/private sector cooperation in terms of critical infrastructure protection. The basic point is that we've been doing this a long time. It's not a completely new challenge.

Oettinger: For any of you who want details, there is a wealth of information on every one of the bullets in that chart in the general publications of the Program on Information Resources Policy or in the records of the seminar. So, if you're interested in pursuing it further, talk to me.

Rattray: The next four or five slides take different slices of how people have treated this issue of SIW in the 1990s. Within the Department of Defense, the Persian Gulf War drove home the idea that information systems are critical to our warfighting capabilities (figure 10). In 1992, DOD actually published the first directive on IW and, subsequently, we've been scrambling around for the last eight years figuring out what IW actually means and how to implement growing capabilities to accomplish new missions.

The box that says "support to the warfighter" makes the point that most of the effort within the Department of Defense has been to support forces, like the ones flying

- **Development of the IW concept**
  - Gulf War and concept of the RMA
  - 1992 DOD directive on "Information Warfare"
  - 1993 JCS publication on "C^2 Warfare"

Support to the warfighter

- **Growing realization of defensive SIW threat**
  - Studies: DISA analysis/Defense Science Boards
  - Rome Labs 1994/Eligible Receiver 1997/Solar Sunrise 1998

Reached the top of the defense agenda

RMA = Revolution in Military Affairs

Figure 10

Department of Defense and the Emergence of the IW Idea

over Kosovo right now, who are in a physical conflict in a traditional sort of war, for instance, by bringing them better electronic warfare capabilities, or protecting their information against an adversary's attack. The locus of activity has not been on national infrastructure protection or protection of our networks at home. That has started to rise, I would argue, since about 1994 or 1995. A number of conceptual studies of our vulnerabilities started to point out that hackers could get into our telecommunications systems. If we lost those systems, we'd suffer significant disruptions.

Then we had a number of incidents. In 1994, hackers broke into an Air Force research lab up in Rome, New York. They actually jumped from there into the Korean nuclear research laboratory. At the time the actual incident was going on, it wasn't clear whether it was the South Korean or North Korean nuclear research laboratory. It became apparent very quickly that it was the South Korean one, but this generated congressional attention. It started to get the ball moving that this was an actual concern for us.

In 1997 we ran an exercise ourselves, in the Department of Defense, referred to as Eligible Receiver, where we actually constituted what we call a Red Team to play a set of adversary hackers. Without going into the details, the exercise highlighted the potential for digital attacks to disrupt large-scale military deployments and operations.

The next spring, in 1998, we suffered another major hacker incident, which is referred to as Solar Sunrise. Solar Sunrise was a series of attacks that the deputy secretary of defense called the most organized structured attacks we've seen. It was during one of our run-ups against Saddam Hussein, when we were moving forces to potentially launch more bombing strikes over there. It turned out the attackers were two teenagers in California, mentored by an Israeli 18-year old who subsequently was conscripted into the Israeli military. The court case against the two teenage hackers has actually resulted in a verdict. They had their computers taken away and they had to promise that they wouldn't use computer systems for malicious purposes. These incidents have generated a lot of interest at the highest levels of the Department of Defense.

Within the U.S. government as a whole, there is a somewhat different story. It's interesting and important in terms of who ends up with leadership for national infrastructure protection (figure 11). In 1990, after the

- **1991 NRC *Computers at Risk* and civilian analyses**
- **Oklahoma City—CIWG and FBI leadership**
- **GAO and the popular press**
- **Kyl amendment and formation of the PCCIP**
- **PDD 63 issued in May 1998**

Reached the top of the national security agenda.

CIWG = Critical Infrastructure Working Group
NRC = National Research Council

Figure 11

Rising National Concern about II Vulnerability

Internet Worm incident in 1988, the National Research Council produced a study called *Computers at Risk.*[2] If you read it again today, you'd find that study still has much to say about the importance of dealing with computer security and the problems that the government was going to have getting commercial cooperation in that realm.

What initiated the effort that we see today to protect our critical information infrastructures, interestingly, can be directly traced back to the Oklahoma City bombing. As a result of that bombing, the Department of Justice stood up something called the Critical Infrastructure Working Group. Janet Reno and then Deputy Attorney General Jamie Gorelick decided that they would add cyber threats to the physical threats in terms of understanding the terrorist threat, domestic and international, to the United States. That started what has continued to this day: a very heavy law enforcement, Department of Justice involvement in protecting our critical infrastructures.

The General Accounting Office (GAO) issued a report on this, and if you ever do a NEXIS-LEXIS search, you'll see a spate of articles in the summer and fall of 1995, when the *New York Times*, *Time*, *The Economist*, the *Boston Globe*, and the *Washington Post* all published their first big IW pieces. That obviously generated a lot of attention. Senator Sam Nunn from Georgia and Senator Jon Kyl from Arizona, who is still there, and a strong advocate of attention to this issue, wrote into the DOD Authorization Act in 1996 that the President had to provide Congress a report about what he was doing to protect our infrastructures against cyber attacks. That resulted in the PCCIP.

Oettinger: You've heard from one commissioner, Peter Daly; you'll hear from the chairman of the commission, General Marsh; and next week, you'll hear from Michelle Van Cleave, who was a principal staffer to Senator Kyl.

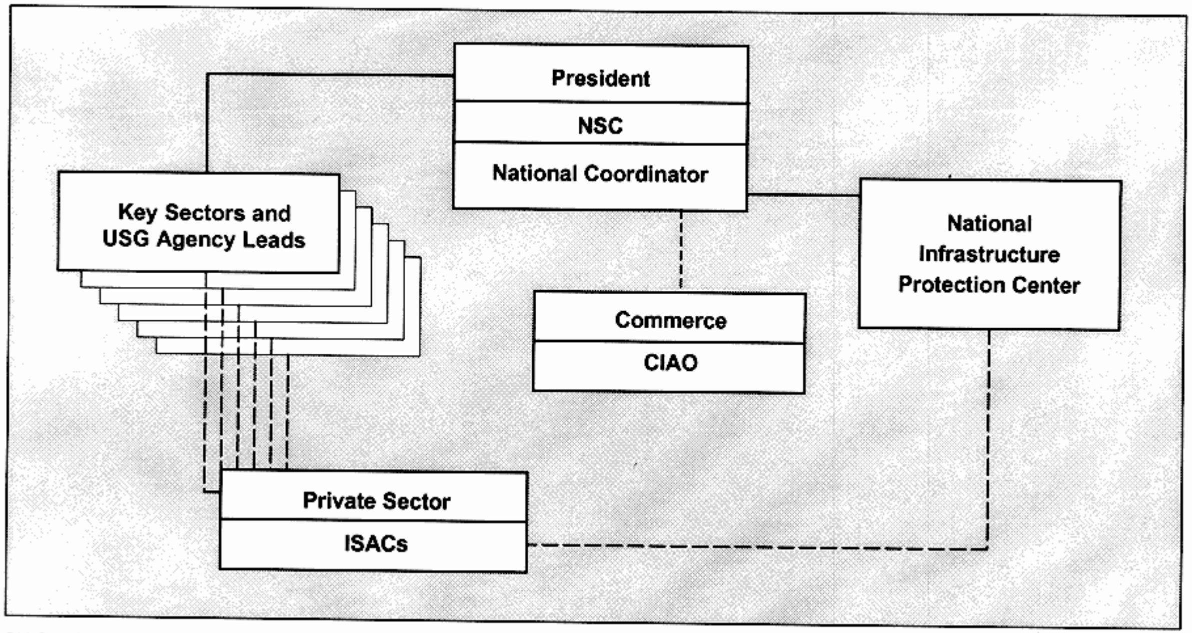
Rattray: All these things started to build momentum. The PCCIP issued its report in October 1997. Three weeks after I defended my dissertation, PDD 63 created a framework within which we're currently planning and organizing for critical infrastructure protection, very much along the lines that General Marsh and the commission's report suggested. There's now a national coordinator on the National Security Council (NSC) for security, infrastructure, and counterterrorism (figure 12). The National Infrastructure Protection Center (NIPC) is housed in the FBI building. It works for the NSC, but it's 75 percent staffed by the Department of Justice and FBI. It has the cyber crime responsibility as well as the infrastructure protection responsibility.

There's a tension between a law enforcement perspective on what you do in response to a cyber incident and a national security perspective. Law enforcement agents want to build cases against individuals to get prosecutions. Those concerned with national security want to understand the threat to the nation as a whole, and to its infrastructures. They want to gather information differently, and they conduct a dialogue between a different set of players. One of the big challenges the NIPC has is to make those two functions work together.

The PCCIP staff has migrated into the Department of Commerce as something called the CIAO, the Critical Infrastructure Assurance Office. These are the people who are supposed to be helping the private sector stand up centers for each of the critical infrastructure sectors. Since you have the report, I'm not going to go into them in detail. The information and security sector, the transportation sector, et cetera, are supposed to work with a lead government agency to get private/public cooperation. That is the key challenge here and is yet to be done, as opposed to the NIPC the President established 15 or 18 months ago. These Information Sharing and Analysis Centers are not in place and operating at this point.

At the same time that all this is going on regarding the need to attend to our cyber vulnerabilities, even within the government, we've done things that make it more difficult to protect our information infrastructures (figure 13). In the early 1990s, the Federal Communications Commission promulgated guidance to the telecommunications

[2] National Research Council, System Security Study Committee, *Computers at Risk.* Washington, DC: National Academy Press, 1990.


President
NSC
National Coordinator
Key Sectors and USG Agency Leads
National Infrastructure Protection Center
Commerce
CIAO
Private Sector
ISACs

CIAO = Critical Infrastructure Assurance Office
ISACs = Information Sharing and Analysis Centers

NSC = National Security Council
USG = U.S. government

Figure 12

PDD 63: The Current Plan for National Information Infrastructure Protection

- **FCC and open network architecture**
- **NII initiative, IITF, and global electronic commerce**
- **1996 Telecommunications Act**
- **1998 Digital Millennium Act**

No national security provisions. Unleash control and unintended consequences.

IITF = Information Infrastructure Task Force (NIST)

Figure 13

Working at Cross-Purposes: Other Government Actions

companies and subsequently the companies that provide Internet communications to dictate that they must allow anybody to hook up to their networks. The goal is to promote competition, but it also means that there's no central point where you know who's hooked up to your networks, and that your standards explicitly foster anyone's ability to enter the networks. If your mandate is protective, that increases your challenge immediately. You've basically told everybody how to get into the network so that they can hook up, and you have a much larger set of players you're trying to deal with.

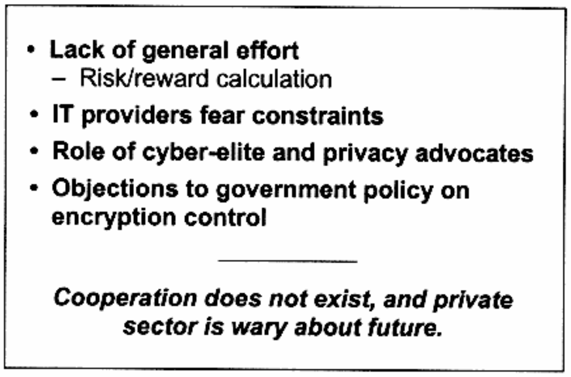
The term NII refers to the National Information Infrastructure. Are people familiar with that term? It was much more in vogue three or four years ago. When the Clinton Administration came in, they launched something called the NII Initiative to foster the use of digital technologies in all our communications—telecommunications, phone, voice—to achieve economic productivity and social good in terms of distributed learning, and other sorts of activities. Vice President Gore's "reinventing government" initiative pushed more efficient use of information systems to foster cheaper government. They had a task force to foster global electronic commerce. These things were not coordinated with the activities going on in the national security community. They were about openness, while we in the national security community were talking about the need to defend our networks. So these two trends were going in different directions at the same time.

The 1996 Telecommunications Act, which supplements the 1934 Communications Act, has redirected the Baby Bells and their relationships regarding who can compete in what markets. It does not address national security at all. The provisions of the 1934 act are still in effect, but the national security relevance of information infrastructures is different in the 1990s than it was in 1934, and we haven't decided to update the overarching legislation on our telecommunications system.

One of the first things I worked on when I got to the Pentagon was the Digital Millennium Act, and I provide it as a prime example of the disconnects I'm discussing here. I got an e-mail from the people who run our computer emergency response team, saying that they had heard from their counterparts in the civil sector that there was a provision in the Digital Millennium Act, which is the implementing legislation for the World Intellectual Property Organization, that basically stated you could not reverse engineer software. It was pretty draconian and as simply put as that. To create computer tools to protect your networks and to respond to computer incidents, you basically have to go back and deconstruct the content of the software you're trying to analyze, or, in the case of an incident response, hack back into the software that's been corrupted and figure out where the problems are. The unintended consequence of that provision was that the emergency response and protective engineering communities were screaming that all their activities were about to be made illegal by an act of Congress because any reverse engineering of software was going to become illegal.

We managed to create an effort in time because the Senate and the House versions of the bill differed enough that they had to go to a conference committee. That took six weeks, and during that time we managed to get a provision written into the legislation that allowed legitimate protective software engineering in computer emergency response activities to continue without undue burden of proof that you had good intent. The guys who wrote this act never intended to undermine infrastructure protection, yet because of the lack of attention to critical infrastructure protection, they could have had a major impact on our efforts.

I'd actually probably tone down my analysis of this at this point (figure 14). I think we're at arms length with the private sector, but the private sector has shown more attention in the last 12 to 18 months to their role in creating secure technologies, which goes back to my initial comments about technology producers. I guess I'll just make the basic point that there's a strong advocacy community out there for privacy in cyberspace. They've been in constant tension with the government about the nature of our encryption control policy. The software industry has not been happy with the U.S. government about encryption policy, because it makes it difficult for them to export their software, and they felt they've suffered commercial consequences from that. Therefore, key players in our critical infrastructure efforts have not been involved and actually are very wary of being involved with government.



- **Lack of general effort**
  - Risk/reward calculation
- **IT providers fear constraints**
- **Role of cyber-elite and privacy advocates**
- **Objections to government policy on encryption control**

Cooperation does not exist, and private sector is wary about future.

Figure 14

At Arm's Length: The Private Sector

Historically, countries, including the United States, have taken approaches all the way across this spectrum in terms of the legitimate government role in the operation of its information infrastructures (figure 15). I would say we're way out on the right now, and basically letting the private sector create infrastructures as they see fit. There are huge benefits to that economically and socially, but we pay costs in the national security realm because of that. These are public policy choices to be made.

I'll just tell you that in these past couple of weeks we've maybe seen a little bit of movement back toward the left. Microsoft is

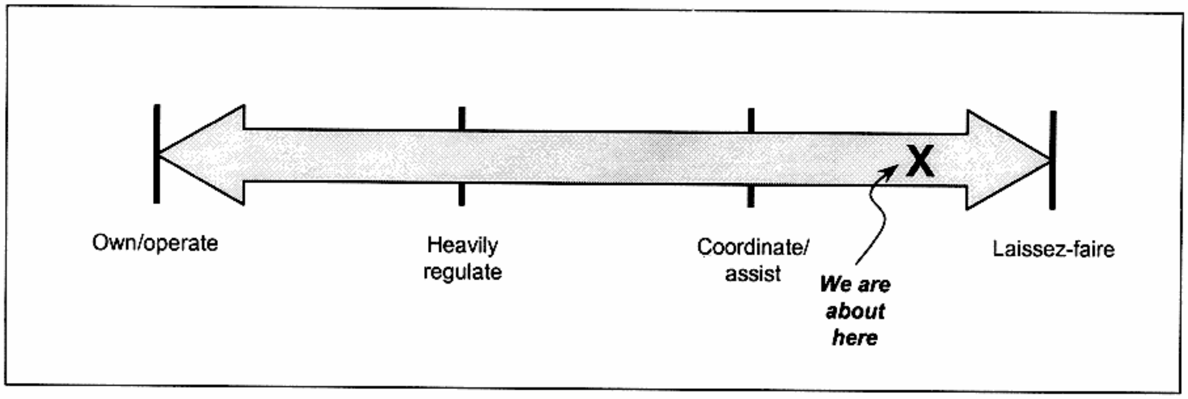


Figure 15

Approaches to the Government Role in Infrastructure Protection

obviously involved in a major antitrust litigation with the government. They're starting to show willingness to cooperate, maybe to avoid continuing the antitrust suit. When Melissa hit, they immediately detailed people to help the government solve the Melissa problem very quickly. Hopefully, they would have done that whether they were in antitrust litigation or not.

Student: I don't really understand that graph. Are you trying to make the connection that if you're far on the left, where the government would own and operate the infrastructure, there's going to be some greater infrastructure protection?

Rattray: No, not necessarily. But I would assert that most people believe that that's the case. I think there are good counterarguments that government ownership wouldn't necessarily result in better control, but historically, governments, including the U.S. government, perceive that's the case and have gone in that direction explicitly to achieve that objective.

Oettinger: Let me reverse it for a moment, because "own and operate" is perhaps not the critical element, whether it's public or private. In most countries, of course, the network infrastructures have been owned by the government, and in the United States, with its tendency to have things private, the phenomenon is the same as elsewhere. AT&T, though not a government entity, was pretty thick with the government, and so for all practical purposes we were at that end of the spectrum in the following sense: that General Kelley's counterpart at what used to be in those days the Defense Communications Agency, General Lee Paschall,[3] could always pick up the phone and call a guy named Bob Gradle at AT&T and say, "Bob, I need *X*," and Bob would pick up another phone and get it done.

Now, how would they pay for it? It didn't show up in defense appropriations. It showed up as 1/100 of one cent on your phone bill, so without any need for taxation, by virtue of the scale of the enterprise, the stuff would get paid for. There'd be no problem. So, on the financial end you were essentially even better off than owning and operating, because it didn't show up on the tax books.

Unitary control, which is the central concept, as opposed to "own and operate," meant that by virtue of a considerable amount of R&D the AT&T folks had come to understand the way you avoid overload—the equivalent of today's notion of a denial of service attack. They have what still is called the Mother's Day phenomenon: Everybody tries to call mother on Mother's Day, and the network collapses. Why? Because the way a telephone network used to be constructed, so much of the equipment is busy looking for a way to get from here to there that it's all pre-

[3] Lee Paschall, "C^{3}I and the National Military Command System," in seminar proceedings, 1980.

occupied in hunting for paths, and therefore can't accept any more calls. The more calls you make, the more it hunts, and it finally disintegrates. Simple solution: When you are in control of the whole network, you stop it at the point of origin. If there are a lot of calls to Louisiana, you filter out the Louisiana-bound calls, whether they originate in San Francisco or New York or anyplace else.

You've got to have control of the whole network to be able to do that. You've got to be able to pay for those facilities. That was duck soup in the Bell System days, prior to the break-up of the monopoly. Under current conditions, two things are happening. First of all, the computer folks who are building the Internet-type networks never heard of Mother's Day, because that's not part of their culture. So, by and large, the computer-based networks do not have overload protection facilities of this kind. Among some of my colleagues in academe, research to provide understanding of overload phenomena in computer networks is frontier stuff. It's 30- or 40-year-old stuff in the telephone world.

If you try to implement that, who's going to pay for it? There is no unitary control, and there is no agreement. There's this NSTAC that you talked about, which is a place where some of these folks can come together. The structure, both technical and economic, of that industry has changed radically and is still in the process of changing, so going from one end of that chart to the other or even moving around is a very complicated and nasty kind of a process. Anyway, the point that I want to make is that "own and operate," to my mind, stands for "unitary" as opposed to "diverse and competitive," regardless of whether it happens to be privately or publicly owned.

Student: One other point that I'm really confused about is that you have "heavily regulated" as a demarcation on that chart, and it seems that in the past the government role in heavily regulating has been contrary to infrastructure protection. I'm thinking about antitrust laws and things of that nature. Regulating industry wasn't necessarily the government's role in infrastructure protection. I can't think of an example where the government's role, or solution, has been to regulate in favor of infrastructure protection.

Oettinger: You're right: in principle, it isn't so. Your skepticism, based on just the words, is well founded. It so happens that in the United States and in most countries the pattern of heavy regulation was one that encouraged that kind of investment.

Rattray: With AT&T, part of the heavy regulation was the requirement to provide certain services in critical situations to the government.

Oettinger: Essentially, it's a little bit of a tacit trade-off: "We'll let you be a monopoly and make a little bit more profit because you're saving our ass in terms of paying for things that otherwise would be politically embarrassing if we had to pass a law each time." Telephone exchanges during that period were built, among other things, to be impervious to civil disturbance and so on, so that if the President were someplace where he needed protection, you'd whisk him off to the nearest telephone.

Rattray: But if your skepticism is based on the idea that central control would necessarily result in more robust, protectable infrastructures, that skepticism is well founded.

Now I'm going to talk about what I think we don't know, and basically ask you, as I started to in the beginning, to question conventional wisdom in the face of a dearth of real evidence about some things (figure 16).

- **Ease of attack—offensive vs. defensive advantage**
- **Key nodes, cascades and complex adaptive systems—what to hit?**
- **Network mapping—what to defend?**

Figure 16

Conventional Wisdom vs. Dearth of Real Evidence

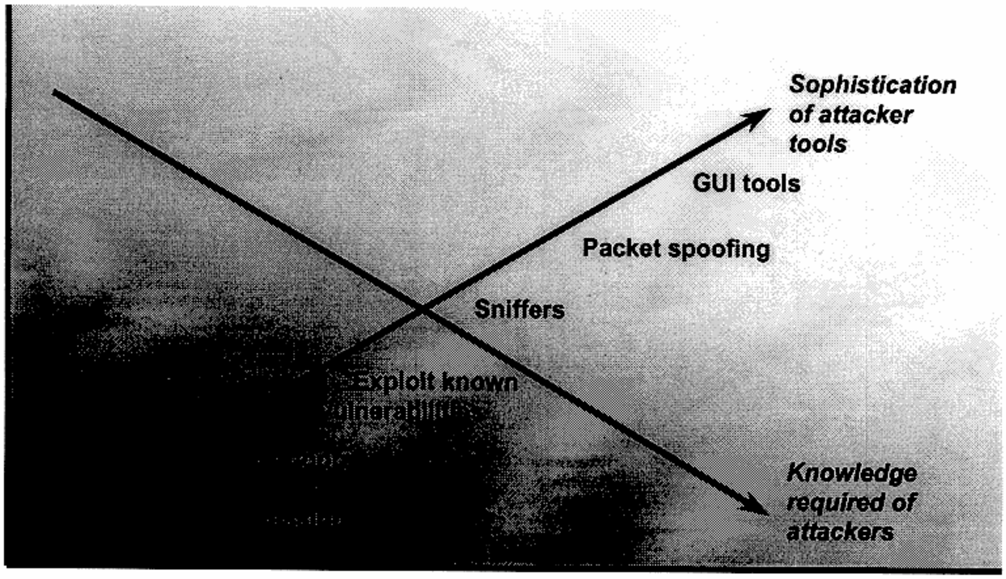


Figure 18

Tools and Required Expertise

- **Operators capable of conducting attacks**
- **Computer programmers for advanced exploits**
- **Networking engineers to analyze adversary's infrastructure**
- **Targeting experts to estimate damage**
- **Experts to assess political influence and social impact**
- **Communications experts to operate command and control**
- **Security to secure, maintain, and update plans**
- **Intelligence agents to develop insiders and access**

Figure 19

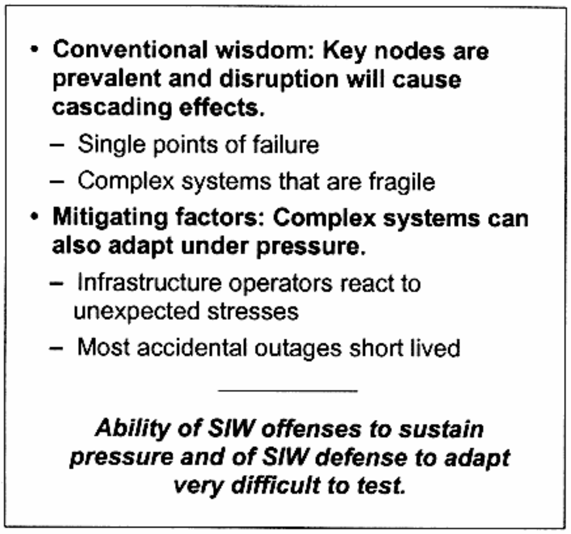
Skill Sets for Offensive SIW

to be able to conduct digital attacks, but if you want to go for key points of his infrastructure that aren't easily exploitable by known tools, you also have to have advanced programmers who can design custom tools to go after them. You have to be able to analyze what his infrastructure looks like and what damage it would cause if you launched these tools. The average hacker is not concerned about these questions, because he's not trying to damage the infrastructure or keep it down for a prolonged period of time. To conduct SIW, these are the sorts of intelligence analyses that you would have to do: activities that historically have proven very difficult to do in strategic warfare. You'd also need to be able to assess what would happen if you brought his computer networks down. Would that really cripple his economy? What would the impact on the people be? Would they immediately be fearful because they couldn't use their computers, or would they be irritated at whoever was doing it, because now they were being harassed?

You need to have people who can operate your command and control system. The point I like to make is that when we formulated nuclear plans, we spent a lot of money on very tight security, and developed ways to handle our information regarding what we would target with nuclear weapons. If you had a list of targets that you wanted to attack, you would have to put controls on your cyber targeting list similar to the nuclear targeting list. This requires manpower, infrastructure, and procedures. This is not something that you do off the cuff if you're going to launch large organized attacks.

Then there is an intelligence/counter–intelligence game going on. You want to place agents inside your adversary's key information infrastructure operations with good counterintelligence capabilities to make sure that people are not getting inside your operations. The point there is that hacking is not necessarily on the cheap if you're going to do it in a large-scale, organized fashion.

We've already talked a lot about the idea that how systems fail is critical to the belief that you can do SIW. Generally, I'd say the conventional wisdom is that there are lots of key nodes out there and that if you hit them properly, the system will fall apart (figure 20). There's a quotation from my dissertation that I want to read; I found it down at Air University in Montgomery, Alabama, in the Air Force's historical archives. This idea—and, I would argue, quintessentially American belief—that you can find a key target and that you can cripple your adversary with it has been prevalent for a long time. This was written in 1934. The author, who ended up actually as part of the team that produced the initial war plans for the U.S. Air Force in World War II, wrote about this when he was lecturing future Air Corps leaders on what we were trying to do with strategic air power.



- **Conventional wisdom: Key nodes are prevalent and disruption will cause cascading effects.**
  - Single points of failure
  - Complex systems that are fragile
- **Mitigating factors: Complex systems can also adapt under pressure.**
  - Infrastructure operators react to unexpected stresses
  - Most accidental outages short lived

Ability of SIW offenses to sustain pressure and of SIW defense to adapt very difficult to test.

Figure 20

Key Nodes, Cascades, and Complex Adaptive Systems

> The classic example of the type of specialization, and hence vulnerability, literally fell into our laps. The delivery of controllable-pitch propellers had fallen down. Inquiries showed the propeller manufacturer was not behind schedule. Actually, it was a highly specialized spring that was lacking. We found that all the springs for all the controllable-pitch propellers of that variety in the United States came from one plant, and that plant in Pittsburgh had suffered from a flood. This was a perfect and classic example. For all intents and purposes, a very large portion of the entire aircraft industry in the United States had been nullified just as effectively as if a great many airplanes had been shot up or a considerable number of factories had been hit.[4]

That practical example set the pattern in the U.S. doctrine for ideal selection of precision targets for bombardment. That was the kind of key node sought in every economy. That was what the air planners were trying to do when they formulated strategic air warfare. It's arguably what people will do when they conduct SIW. The problem is that finding those single points of failure that cause cascading effects has historically proven much more difficult than the conceptual idea that those sorts of things exist, and finding anecdotal evidence that they do.

I'm going to counter myself here a little bit. We do have single points of failure. When the satellite that Pagenet uses to control all of our digital pagers went out of orbit, 80 percent of the pagers were down in the United States. When AT&T switching software failed on Martin Luther King Day in 1991, they lost service to 40 or 60 million customers because the signaling errors in one switch cascaded into another switch.

Oettinger: Yes, but it's worse. The analysis of this gets very complicated. You said a pager. Why did the U.S. economy not collapse? First of all, because not everybody depended on pagers. Second, there's an alternative, which is to pick up a phone. It may be a little bit more costly, and not everybody

[4] Thomas H. Greer, *The Development of Air Doctrine in the Army Air Arm* 1917–1941. Washington, DC: Office of Air Force History, 1985, page 81.

who has a pager may be near a phone, but it's an alternative. In the case of the strategic bombing, there remains a controversy over the effect of U.S. and British bombing in World War II.

Rattray: He's challenging the conventional wisdom, which he did for three years with me. Complex systems can prove and have proven their ability to adapt, too. Power companies do this all the time. Ice storms come through, and people lose power. Power companies get good at putting the power grid back together. Most of these accidents, such as the Pagenet failure or the AT&T switching software failure, lasted for a period of hours. Can we live without these services for hours? Obviously we can.

What we don't know is if adversaries could keep the infrastructures down if they attacked in a structured, organized fashion, trying to inflict pain for long periods. What we're having a difficulty with is that we can't test that. We're not allowed to go out and see how people would react without electric power for two weeks. So we need to take opportunities when we have them to see how systems fail and how people react.

Oettinger: But there are lessons. Every lesson that we've seen in the real world shows that even relatively primitive societies or fairly advanced ones have a lot more resilience than we seem to assume. The whole Vietnam War history is one case in point. The classic one is the World War II bombing of the Schweinfurt ball-bearing factory, which was regarded as a great coup because we were going to cut off all the German ball-bearing supplies. The problem is the Germans went and bought ball-bearings from Sweden.

Rattray: They did a lot of other things, too. They redesigned their tanks. They had stocks of ball-bearings that we didn't know that they had.

Oettinger: The point is that it's a very difficult game, both offensive and defensive. A lot of the stuff that you read about hacking has this notion that somehow it's Superman doing something omnisciently, and it's a lot more complicated than that.

Rattray: For any given system, in many cases we don't know whether we're in a situation where if you hit a particular node it quickly disables the whole system, or if the system pushes back effectively (figure 21). We need to figure out when we get opportunities to learn. I'd say Y2K is an opportunity to kind of measure which types of systems fall into which basic categories. Therefore, the ones you've really got to be concerned about are the ones that have the fast cascade sort of characteristic, and you want to learn what types of organizations create an adaptive type of effect in terms of infrastructure.

The conventional wisdom is that the defensive effort will be prioritized based on value and vulnerability (figure 22), and that it's an easily knowable thing. According to this theory, organizations can pretty much tell you what they rely on, and its relative significance to them. That is how most of the infrastructure protection plans that I've read in the past year have been developed.

What I would argue is that, if this is what you're trying to defend, it's very hard to discern what your key nodes are, or what your centers of gravity are (figure 23). That's a Bell Labs-generated map of all the Internet routers in the United States. I think it's probably representative of global networks.

Oettinger: Is this loosely coupled or tightly coupled?

Rattray: This is the confusing thing that we're trying to defend.

Oettinger: Is that good or bad?

Rattray: On the bad side, it's obviously complex. It requires a lot of investment to understand. On the good side, you're starting to see that there are ways to depict information that start to tell you things. It's not a high-fidelity slide, but you can start to learn from it. For example, UUNET runs a large number of the backbone Internet routers and its color-coded links show through on the map. If you were going to choose an organization to attack, and if you had a color-coded

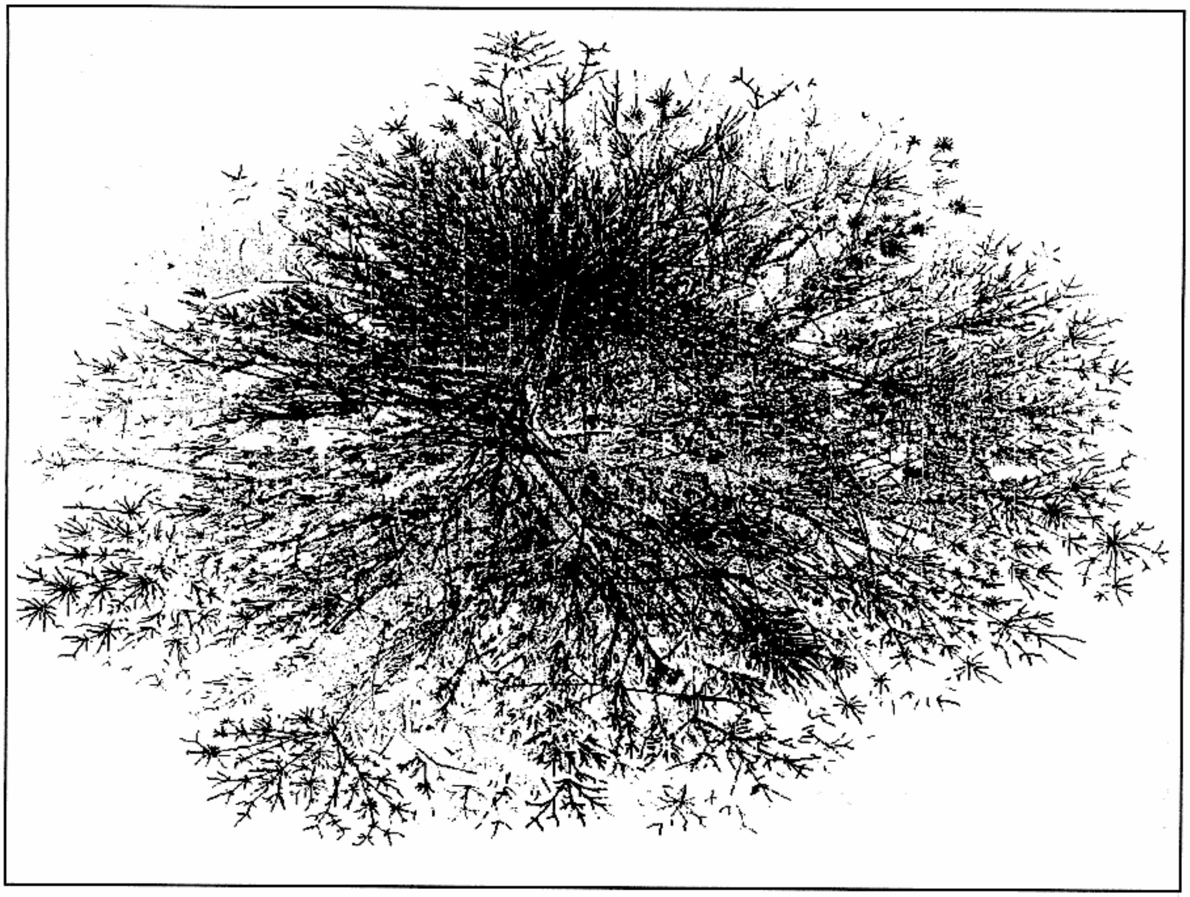


Figure 23

Late 1998 Bell Labs Map of Internet Connections

- **Negative impact of doctrinal lock-in**
- **Adaptability of defenses and infrastructure**
- **Lack of proper intelligence support**

Figure 24

Learning from History: Development of U.S. Strategic Airpower and WWII

In a realm where technology changes at a high rate, which it did in the 1920s and 1930s in aircraft engineering, you don't want to get locked too early into what you think the right answer is (figure 25). By the early 1930s, the people in the Air Force pretty much decided that unescorted, high-altitude, long-range, lightly armed bombers were the way to go after an adversary. For the rest of the 1930s, that's the type of bombers they

"Bombers will always get through"

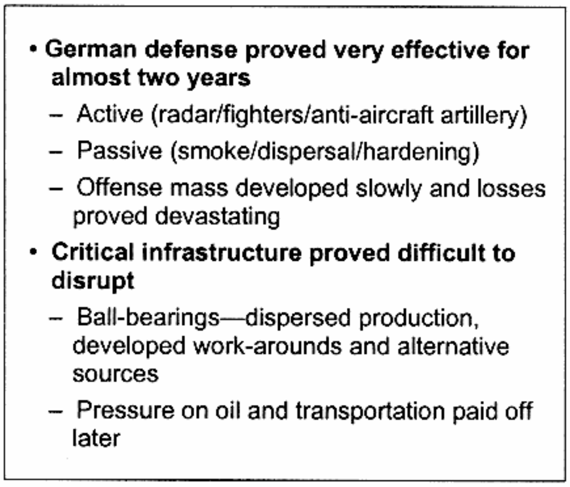
- **Reasons for early doctrinal commitment**
  - Quest for independent mission
  - Bomber pilot mafia drove doctrine as well as technology development and evaluation
  - Artificial exercises and test
- **Impacts of doctrinal focus**
  - Miss experiential lessons and new defensive technologies
  - Underdeveloped key skills and protective technologies
  - Loss of key personnel

Figure 25

Doctrinal Lock-In

built, even though radar was invented and fighters got a lot better. We went into World War II with that doctrine and with technologies that were influenced by that doctrine. They were not as effective as they could have been if we had continued to adapt and change throughout the 1930s based on technological change. That's something we don't want to do in this realm, since the key features of the information infrastructure seem to be changing on a rapid basis; not annually, but in short time cycles.

This point has been hammered home from the start of the presentation (figure 26).



- **German defense proved very effective for almost two years**
  - Active (radar/fighters/anti-aircraft artillery)
  - Passive (smoke/dispersal/hardening)
  - Offense mass developed slowly and losses proved devastating
- **Critical infrastructure proved difficult to disrupt**
  - Ball-bearings—dispersed production, developed work-arounds and alternative sources
  - Pressure on oil and transportation paid off later

Figure 26

Adaptability of Defenses and Infrastructure

It proved very difficult for those who made the doctrinal statement that I read to find those sets of targets in Germany. They didn't get the types of dire effects that make airpower a war winner in World War II. I'll read a quotation. In January of 1945, we had been bombing for two and a half years, D-Day had occurred, we had been on the continent seven months, we'd already fought the Battle of the Bulge, and we were five months away from victory. I found this in the Air Force archives; it's from General Hap Arnold, who was the commander of the U.S. Air Forces. This was Arnold's assessment in a memo to his chief planner:

> Great damage by bombing has already been inflicted on the German military installations and industry. Nevertheless, the German army and German air force continue under these circumstances to fight with an effectiveness that would have been considered impossible a few years ago. It would appear to me that new yardsticks for measuring the ultimate effect of our bombing on the German military effort must be used. We are certainly destroying German industry and facilities from one end of the country to another. Also, certainly, this destruction is not having the effect on the German war effort that we had expected and hoped—not the effect that we had all assumed would result.[5]

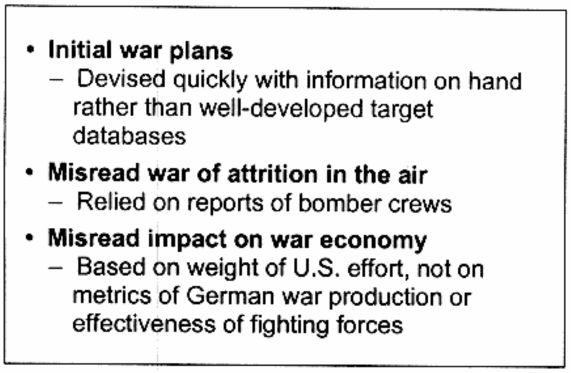
That's what I'm worried about, as a bottom line: that people think SIW is easily going to be a war winner in a conflict. It's just not going to be that way, for the same reasons that airpower was not the war winner. It caused massive damage, and inflicted massive pain. It was a contributor to the Allied victory in World War II, but it wasn't decisive.

Oettinger: We laid the basis for the German post-war *Wirtschaftswunde*r [economic miracle] by eliminating all the old plants and breaking new ground and getting them to invest and do new things.

Rattray: Maybe Y2K is to some extent doing that to us, too. It's a potential threat that all our systems will go down and force us to make wholesale changes to the system.

If you're going to conduct this type of warfare, you basically need good intelligence support (figure 27). This problem has been identified right now for our IW efforts. I've stressed throughout this whole talk that it's not only a matter of being able to get to your target; you've also got to be able to pick the right target. We didn't do that prior to World War II. We had five people in the organization in Washington responsible for the formulation of our targeting lists against Germany in 1941 and 1942. They actually picked electric systems as their top priority because the U.S. banks had made loans to the German electric power industry, so they had information on the German electric system that

[5] Air Force Historical Research Agency, file 145:81-162.



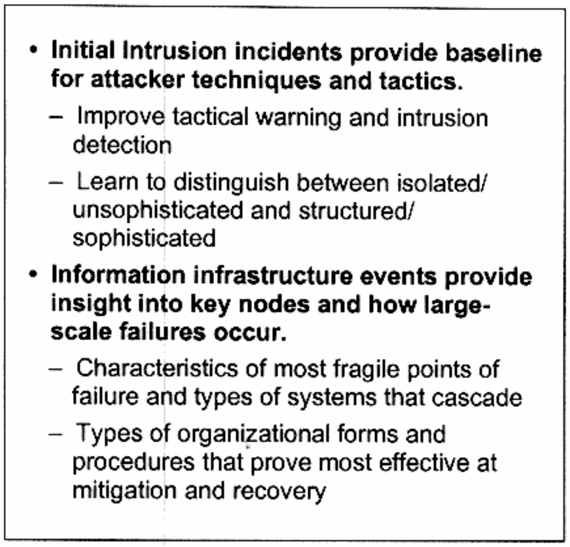
- **Initial war plans**
  - Devised quickly with information on hand rather than well-developed target databases
- **Misread war of attrition in the air**
  - Relied on reports of bomber crews
- **Misread impact on war economy**
  - Based on weight of U.S. effort, not on metrics of German war production or effectiveness of fighting forces

Figure 27

Lack of Proper Intelligence Support

allowed them to target that system. That is not the way you pick your center of gravity: through use of available limited information. You should be able to pick what you think is most significant to your enemy.

We must learn from experience, incidents, and events, as we talked about (figure 28). When we get hacked and when we have failures, we should take the opportunity to understand new lessons. One challenge that I know we have in the Air Force, and I imagine others will face, is capturing these lessons learned, because it takes effort to record them in such a way that we can draw on them as we form new policies and doctrines. We have not done a good job of that. It's expensive and we need to do more of it.

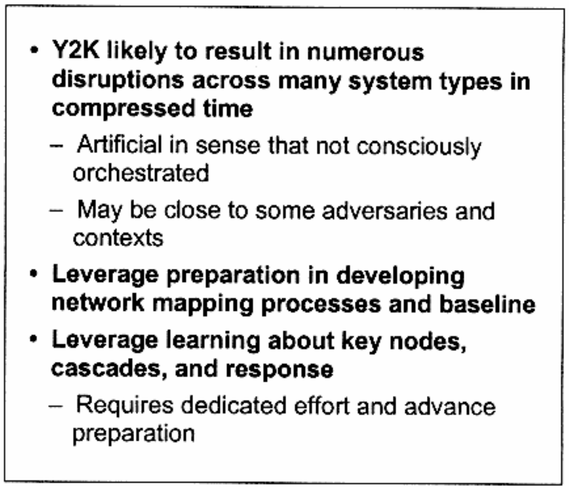


- **Initial Intrusion incidents provide baseline for attacker techniques and tactics.**
  - Improve tactical warning and intrusion detection
  - Learn to distinguish between isolated/ unsophisticated and structured/ sophisticated
- **Information infrastructure events provide insight into key nodes and how large-scale failures occur.**
  - Characteristics of most fragile points of failure and types of systems that cascade
  - Types of organizational forms and procedures that prove most effective at mitigation and recovery

Figure 28

Incidents and Events

I think Y2K already has provided a real opportunity that we don't want to lose, and it may provide even more learning when it actually happens (figure 29). The learning that we should capture now is that we've evaluated the relative significance of most of our information systems for Y2K. We had to do that to decide which ones to spend money on to make sure that they weren't Y2K flawed. We need to make sure that the process by which we did that, which involves both the people who use the systems and the technical people who support the systems, doesn't get lost. If we have a lot of problems during the Y2K onset, we will start to see which types of information systems fail dramatically, which ones actually degrade gracefully or are capable of handling the problems, and which sorts of organizations are better or worse at responding to losses of information service and at getting information systems to recover. The Air Force is trying to put an effort in place to do that kind of learning and data capture. Again, resources are an issue for us.



- **Y2K likely to result in numerous disruptions across many system types in compressed time**
  - Artificial in sense that not consciously orchestrated
  - May be close to some adversaries and contexts
- **Leverage preparation in developing network mapping processes and baseline**
- **Leverage learning about key nodes, cascades, and response**
  - Requires dedicated effort and advance preparation

Figure 29

Leverage the Year 2000

Oettinger: You did a marvelous job. He knows more about this stuff than any other human being on earth.

Rattray: But I don't know much, because none of us knows that much.

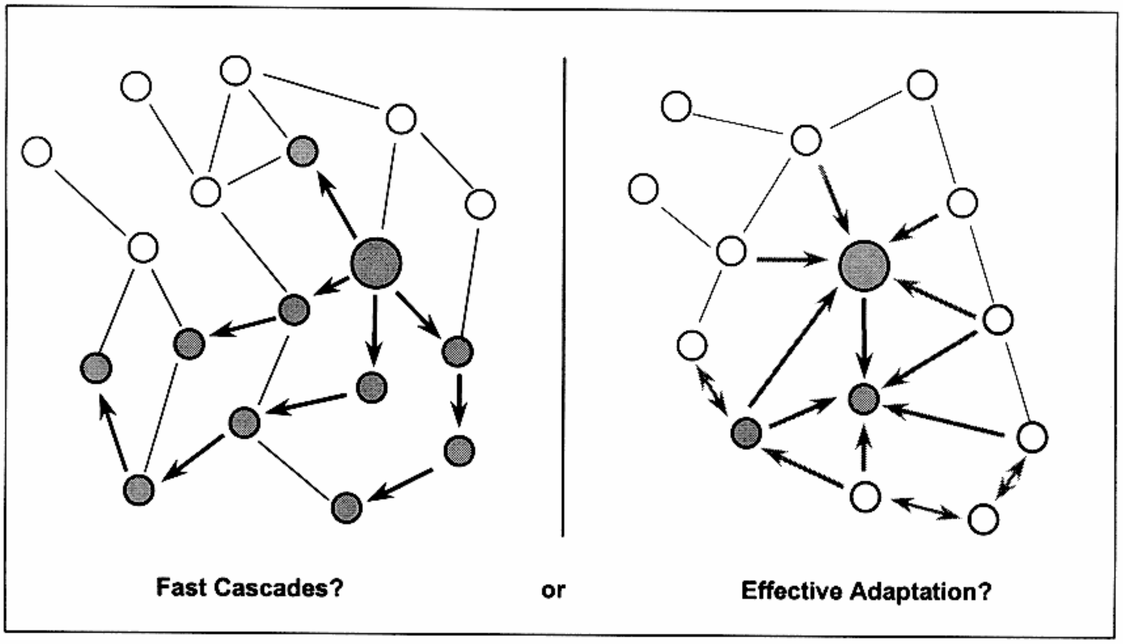


Figure 21

Cascading vs. Adaptive Effects

graph, you could start to pick out organizations to go after. The people who put this together talk about portraying this in 3-D so you can get more fidelity in depicting our networks and their connections. This is a big challenge and actually a place where a lot of intellectual creativity would be well spent in terms of how we depict what we're trying to defend.

There are challenges in terms of network mapping (figure 22). If you're going to try to evaluate what it's worthwhile to spend on defense, you don't only have to understand what's technically connected, but you'd better also understand who uses it for what purpose. Lots of vulnerabilities are distributed throughout that confused diagram I showed you (figure 23). If the software that runs all those routers has one flaw, or if somebody designed it with a purposeful bug, the attacker could theoretically bring down the whole thing at once. That's a critical node that no single person has responsibility for identifying, and that becomes difficult to force out of a process where owners of physical infrastructure are required to identify their vulnerabilities. The pace of change will require that the network map be updated almost constantly, again making it an expensive process.

I'm going to suggest a few ways we can learn. This has already been put on the table for us (figure 24). We can learn through history. This is not such a new wave of warfare that the examples we have from the past don't teach us some things about the relative significance of this task now.

- **Conventional wisdom: Defensive effort will be prioritized based on value and vulnerability.**
  - Lower-level organization will identify.
  - Higher-level organizations will allocate effort.
- **Challenges: Baseline maps are difficult to create.**
  - Must understand both technological connections and operational value.
  - Key nodes and attendant vulnerabilities may be widely diffused throughout system, not geographically localized.
  - Pace of change will require almost constant updating.

Figure 22

Network Mapping

Student: It is known that the most sophisticated agents would be developed in western societies. So are there any measures against possible attacks from the developed Western European countries or possibly Japan or other foreign countries?

Rattray: I'm not in a position to discuss specific measures and specific countries. The assumption that you have to be a technologically advanced nation to develop a sophisticated IW program I think is one that we ought to question, because the numbers of sophisticated people you need to orchestrate this could be fairly limited. There are ways to develop that sort of expertise.

I'm actually kind of leery of the concept of hackers for hire on a large scale, or a nation-state putting its national security on the line by relying on hired hackers, because there are a lot of huge risks. If those guys turn on you, you've just divulged that you're developing this capability. But the potential for leveraging a large number of experts, getting the tools together, and then not needing a lot of sophistication once you've figured out how to use them, leads me to believe that lots of different sorts of actors could get them, not just Western societies.

Oettinger: I hate to cut this off, but we have to vacate the room. Sir, once again, a small token of thanks for our large gratitude.

Rattray: Thank you.

INCSEMINAR1999

ISBN-1-879716-63-1