INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Information War: Ready for Prime Time?

Martin C. Libicki

Guest Presentations, Spring 1996

James R. Clapper, Jr; Mark M. Lowenthal; Richard T. Reynolds;
Julie J.C.H. Ryan; Arthur K. Cebrowski; John M. McConnell;
Albert J. Edmonds; Martin C. Libicki; Robert A. Rosenberg

January 1997

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 1-879716-39-9 **I-97-1**

Information War: Ready for Prime Time?

Martin C. Libicki

Dr. Martin C. Libicki has been a Senior Research Fellow at the Institute for National Strategic Studies, Advanced Concepts and Technologies (National Defense University), since 1986. His present field of interest is the relationship between information technology and national security. In that context he has written Information Technology Standards: Quest for the Common Byte, *and* The Mesh and the Net: Speculations on National Security in an Age of Free Silicon. *The latter extends the work on technological forecasting done for Project 2025, undertaken for the Vice Chairman of the Joint Chiefs of Staff. His other work includes* What Is Information Warfare?, *and "Dominant Battlespace Knowledge and Its Consequences" in the NDU book* Dominant Battlespace Knowledge. *Dr. Libicki's earlier monographs include "What Makes Industries Strategic," and "Industrial Strength Defense, Phase II Analysis." His prior employment includes three years on the Navy staff as program sponsor for industrial preparedness and three years as a policy analyst for the General Accounting Office's Energy and Minerals Division. Dr. Libicki received a B.S. in mathematics from the Massachusetts Institute of Technology, an M.A. in city planning from the University of California, Berkeley, and a Ph.D. from Berkeley, writing on industrial economics.*

Oettinger: I won't go into an elaborate repetition of the biographical details on today's speaker, which you've seen, but I want to point out that he's one of the most prolific authors among any of the visitors we've had so far. He's the author of *The Mesh and the Net*; a rather explicit title, "Dominant Battlespace Knowledge—The Winning Edge," ...

Libicki: I was not responsible for the subtitle.

Oettinger: ... and "Standards: The Rough Road to the Common Byte." There is a longer version of that called *Information Technology Standards, A Quest for the Common Byte*, which is commercially published. He also wrote "What is Information Warfare?" The four small ones that I've pointed out are NDU publications, and they are freebies. So, for any of you who are interested in following up on our speaker's words today in greater depth than is possible in the seminar, you can get these four publications, which are yours for the asking, by writing to National Defense University in care of the Publications Directorate. *Information Technology Standards* is a publication of Digital Press, and I'll advertise that because he doesn't get royalties on it, but the Program on Information Resources Policy may. It's an expenditure well worth making.

With that, I'll turn it over to Martin, who has indicated that he is interruptible *ad lib*. What have you done?

Libicki: The other way of getting it is just to pull it off the Web by going to my home page (http://www.ndu.edu/ndu/inss/staff/libicki.html) and working from there.

I took a very similar briefing before the Defense Science Board in January of this year, and before I got up to speak, after trying to ascertain what they really wanted me to talk about, I went to the assistant to the task force's chairman and said, "Look, I'm going to get up in front of these distinguished people (this was a Defense Science Board on defensive information warfare), and I'm going to say, 'The sky is not falling.' Now you're going to get a lot of people, I'm sure, who are going to stand up and say, 'The sky is falling. This is an enormous problem we've got to do something about, and if we don't do something about it, the Republic is in peril.' Have you got anybody else who's going to stand up there and say that the sky isn't falling? I'll be curious to see whom you've got." He said, "Nope. You're the only one who's going to get up there and say the sky isn't falling."

But my best surprise came at the end of the discussion, when the chairman, Duane Andrews,* said, in effect, "We owe it to ourselves, as the Defense Science Board, to hear a wide range of opinions. And having heard yours, we are satisfied that we have, in fact, accomplished this." Basically, what he said is, "Now that we've heard from the nut case, we can go on and do what we were going to do in the first place."

I am known among those people who know me at all as the curmudgeon of information warfare, or IW. Despite the glory to which that concept has risen in the Pentagon, my sense is that IW does not really exist as an integrated discipline. Instead, it is a collection of things having to do with information and warfare, some of which are easier to do now than they were 5 or 10 years ago, some of which are harder to do now than they were 10 years ago, many of which basically depend on the eternal constituents of the human mind and, therefore, don't change in any fundamental way. To take a lot of things that were formerly disparate and glorify them under the notion of "information warfare," to put them under the rubric of the Third Wave (you folks are familiar with the *oeuvres* of Heidi and Alvin Toffler) is a gross disservice to thought. One of the things I'd like to do is try to spend some time puncturing that balloon. I am told, by the way, that I'm not entirely successful in this. The Pentagon is going on with its myths, which are the subject of my first slide, but I do what I can.

First myth: information warfare is a coherent something, in the sense that naval or other types of warfare are coherent somethings (figure 1). I do not believe this is the case, and as I go through, I will talk about various aspects of information warfare, some of which are strongly related and some of which are weakly related.

A myth, by the way, does not necessarily mean something that is false, but something that is widely believed and becomes a totem of a particular culture.

- **It is a coherent something.**
- **It will become increasingly important.**
- **It will dominate all other forms of warfare.**
- **It is the new strategic arena of conflict.**

Figure 1

Myths

Myth number two is that IW will become increasingly important to how warfare is conducted. Some aspects will become increasingly important, but others will become less important. It will definitely not dominate all other forms of warfare—which will remain the ugly business of killing people and destroying things. Information warfare is not going to change that aspect very much; it will mediate some of the ways in which people carry out warfare, but it will not itself supplant them. Therefore, I do not think it's a new strategic arena of conflict. Warfare in the 21st century will have a lot of familiar elements to it. It will not be a bunch of people at their keyboards zapping each other across the Internet.

Student: Let me ask you one thing. I was at breakfast this morning with Congressman [Jack] Reed (D-RI), and he was talking about info warfare and he said the term, and then he stopped himself, and he said, "Oops! New name: information security." Has it changed within the D.C. Beltway?

Oettinger: Security is a subset.

Student: Yes, I know that, but the way he had said it, it was like, "Well, the more politically correct way to say it now is info security." I didn't know if that was his term or that was something generally used.

Student: Did he say assurance or security?

* Duane Andrews, ASDC^{3}I 1989–1992.

Student: No, he said security.

Libicki: INFOSEC is an old term.

Student: No, it was not used in the context of INFOSEC, but it was as an alternate to info warfare.

Student: It probably has to do with whatever legislation is pending at the moment.

Libicki: There's that tendency.

DOD's official definition of IW (figure 2) is basically something to the effect that all operations designed to degrade, destroy, da, da, da, dee, the enemy's network systems, information, information systems, and enhance, protect, da, da, da, da, our own information systems, et cetera, is information warfare. I think they spent 6 months wrangling with it and actually got the word "systems" or "networks" into the definition. If any of you have been familiar with the Pentagon, none of that wrangling will seem very strange.

In MOP (memorandum of policy)-30, the Joint Chiefs of Staff has defined a version of information warfare under the rubric of command and control warfare. I think it's electronic warfare, destruction, operational deception, operation security, and unit-level psychological operations. It's basically a grab bag of things that we've always done.

MOP-30 is a lot of roles and missions and what is this and what is that. Whenever people talk about doctrine, and you actually read a doctrine publication, it's about who gets to do what to whom. "This is your responsibility, that's your responsibility." Like many such doctrines, of course, it reflects the results of a long bureaucratic battle. They're halfway right, because you can talk about information warfare not only in terms of the military context of warfare but also in terms of civilian context. The people who get most excited about information warfare don't spend their time talking about radar jamming, even though that's actually a very important component of information warfare, but they spend a lot of their time talking about the Internet and CNN.

- **By official definition**
- **By MOP-30**
- **As the struggle for command and control**
- **By parts**

Figure 2

Defining Information Warfare

The third way you can define information warfare is as the struggle for command and control. That was offered to me by Don Starry, a developer of the DOD's Air/Land doctrine. I found that a very nice definition, until I thought about it for five minutes and remembered the classic land battle, in which two armies go at each other. One wins and the other panics and runs, and that defined victory. If you had a coherent army at the end of the day and he didn't, you were the winner. What that meant was that the other guy had lost command and control of his armed forces. Thus, to define information warfare as a struggle for command and control is excessive. Part of the problem with these definitions is that they tend to get excessive, because, in fact, there's no form of warfare that does not, somehow or other, subsume information.

The other road to excess comes from overdefining warfare as any competition. If Toyota, which is a Japanese firm, advertises its cars against Ford Motor Company, which is an American firm, advertising is information; competition is warfare; and, therefore, advertising is information warfare. That kind of definition takes in pretty much everything.

Oettinger: If I may interject something here, Martin, something I wrestled with a great deal in the general economy was the notion that this is an information age. I teach a course called "The Information Age," but that's advertising; that's information warfare for the souls of the students. Every age has been an age of information. So what is the difference today? I throw this out to see whether you would agree that it applies in this realm. The difference is that we're more information intensive than before, for one very simple reason: that information goods and services have gotten cheap relative to other, say, energy-intensive or materials-intensive, goods. Therefore, there's a tendency to use more of the cheaper thing. And so, I think I can defend the notion that relative to earlier economies, our economies today are more information intensive, and I think that's, in that realm, a more accurate view. Does that make sense to you in this realm?

Libicki: Yes. That's the Hegelian notion: changes in quantity are changes in quality.

Oettinger: Maybe.

Libicki: Consider the *kanban* system for parts manufacture. Toyota invented it without computers whatsoever. They had these little cards that went around and when you used a part, this little card went back through the supply chain and told you to order more parts.

When American manufacturers went to the *kanban* system they computerized it. Far more bits are needed to make the American *kanban* system work as well as the Japanese *kanban* system, because only the Japanese *kanban* system presupposes a set of industrial relationships dating back from feudal times. Therefore, in order to get it to work as well, Americans had to throw a lot of bits at the problem.

If bits become cheap enough, might the path that basically says, "Throw as many bits as possible at the problem and eventually the economies will be on our side" end up better than a path that relies on sociological and unrepeatable foundations? I don't know. One issue that arises when automating an armed service is that you have to spend a lot attention on the man-machine interface. This is particularly true for artificial intelligence, if such a thing ever exists. It's one thing to have a system do something. It's another thing to get the person to get the machine to do something the way the person wants the machine to do it or the way the person wants to do it.

What I have done in *What Is Information Warfare* is basically take a look at information warfare in terms of seven component forms of warfare (figure 3), which takes up the first hour of this lecture. The next 30 minutes come from a paper called "Defending the United States in Cyberspace" (a chapter in *Cyberspace* by Al Campen et al., which is also on the Web).

- **Command and control warfare**
- **Information-based warfare**
- **Electronic warfare**
- **Psychological warfare**
- **Hacker warfare**
- **Economic information warfare**
- **Cyber warfare**

Science fiction

Figure 3

Forms of Information Warfare

Let me go back to the various forms of information warfare (figure 3). You've got command and control warfare. The basic definition is dropping bombs on the other guy's headquarters and on his communication chains. It turns out that some aspects of that have been a very, very old form of warfare.

Information-based warfare, which I will not go into at great length, because that's really a two-hour lecture all its own, is basically Admiral Owens' system of systems.* How do we systematically collect information on the other guy, and how does the other guy keep himself from being systematically collected against?

Electronic warfare is very familiar stuff.

Psychological warfare I define as a use of information to change the mindset, the opinions, the attitudes, the beliefs of the other person. The term "psychological war-

* See, for example, William A. Owens, "The Three Revolutions in Military Affairs," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1995*. Cambridge, MA: Program on Information Resources Policy, Harvard University, January 1996.

fare" is often used to talk about anything that in fact changes somebody else's mind. Perhaps the most effective form of psychological warfare we conducted in the Gulf was dropping bombs on the Iraqi troops for 40 days and 40 nights. It made them so fearful that by the time we invaded, they were ready to surrender to CNN or even to our unmanned airborne vehicles. Now, to include B-52s under psychological warfare and thus information warfare is a stretch, but, in fact, they had a very strong psychological impact on the people who were on the receiving end of all that ordnance. When I talk about psychological warfare I shall limit myself to the use of information to change the other person's mind. Remember Napoleon's aphorism, "In warfare, the moral is to material as three is to one." It's old stuff.

Hacker warfare is basically what Winn Schwartau talks about.* Goya's painting, "The Sleep of Reason Produces Monsters," occurs to me in this section. Since I'm going to be spending a lot of time talking about this, I'm not going into detail right now.

Economic information warfare and cyber warfare are mostly in the realm of science fiction at this point because it would take even the advanced U.S. society a lot of evolution before we had the computer networks and dependence on computer networks that would allow these forms of warfare to be effective.

A basic truism about information warfare is that its effectiveness is very, very sensitive to what the other guy has: if the other guy does not have computers, you cannot take down his computers. If the other guy does not have media, you cannot get on CNN and do anything. The construction of the other person's information infrastructure has a very, very distinct impact on which of these things succeeds. If a person insists on being primitive, there is not a whole lot you can do with information warfare, because there isn't any handle you could grasp at, except to a certain extent.

Let us say we had a rogue country and wanted to cut them off from information—thus from global communications. Whether or not you can do that, the impact of that action depends very strongly on how they're wired into the rest of the economy.

Cyber warfare is really a kind of grab bag of miscellany. Did anybody ever see Sandra Bullock in "The Net," or read William Gibson's *Neuromancer*? That's what I mean by science fiction.

Oettinger: It's taken seriously. I had a student at dinner last night ask me whether "The Net" was an accurate portrayal of the future. She was fearful.

Libicki: You remember the story, right? Absolutely nobody in the world could identify her because of the lifestyle she led and, oh by the way, her mother had Alzheimer's. They really had to work at that plot.

Command and control warfare is something we did very successfully in the Gulf (figure 3). We were able to disable, to a large extent, Saddam Hussein's command apparatus, and we were able also to a large extent to keep Baghdad from talking to the field. The combination of those two actions immobilized what was actually not going to be a terribly mobile army to begin with, but essentially made them sitting ducks for our subsequent operations, notably, our air attacks and our ground attacks.

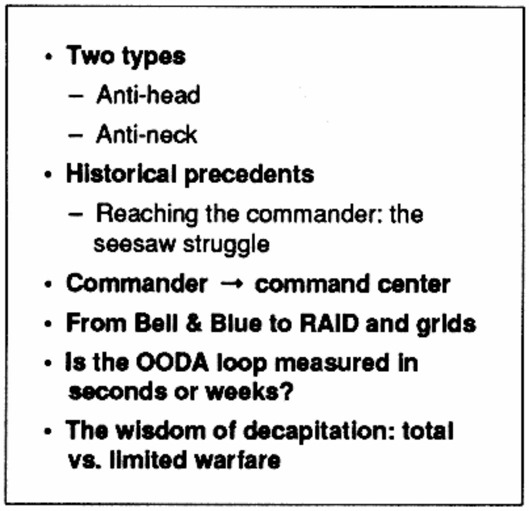
In almost all planning for information warfare, command and control warfare is, I'm certain, an element in the Pentagon. But this also illustrates another aspect of information warfare not terribly well commented upon by its advocates. Command and control warfare, like other forms of IW, is highly opportunistic, and because it is highly opportunistic, you can't necessarily count on its working. A prudent commander will try various forms of information warfare, and he will exploit the successes as best as he can. But if he is prudent, he will not predicate his campaign upon these successes actually happening.

That's very important to remember because that differentiates IW from a lot of other warfare. That is, if you send a tank battalion into another tank battalion, you

* See Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunders Mouth Press, 1993.

have some sort of idea of what you're trying to achieve, some sort of idea of the likelihood you have of achieving it, and some sort of way of building on those gains, if you have them. If you drop a bomb on a target, you have some sort of likelihood that it will hit and some sort of likelihood that hit will matter. I would argue that, in information warfare, you're dealing with a lot more imponderables. So, yes, you should build it into your campaign, but you should also be prepared for very few good opportunities to come up, and you'll have to go back to doing everything else you had to do in the first place.

Command and control warfare has historical precedents (figure 4). Gunning after the other side's commander has been a tried and true method of warfare anywhere from the ancient Greeks, who were always after the commander, to stories in the Bible, to the game of medieval warfare, which was called "capture the king and see how big a ransom you can get," to the fact that there were sharpshooters in the age of the rifles. Admiral Nelson, for instance, was killed that way during the battle of Trafalgar. There were a number of Civil War sharpshooters whose specialty was going after the other side's generals. Therefore, how you did command and control, by the way, was very strongly predicated on where you could safely afford to stand in a particular battle. Wellington had a number of horses shot out from under him at Waterloo.



- **Two types**
  - Anti-head
  - Anti-neck
- **Historical precedents**
  - Reaching the commander: the seesaw struggle
- **Commander → command center**
- **From Bell & Blue to RAID and grids**
- **Is the OODA loop measured in seconds or weeks?**
- **The wisdom of decapitation: total vs. limited warfare**

Figure 4

Command and Control Warfare

The practicality of C^2W has been a seesaw struggle because of the relationship between the range of the firepower and one's ability to command from a particular vantage point. In World War I, at least in the Western lines, a commander with a telegraph could stay far back from the lines and run the war that way, and there were very few instruments you could shoot from that range that would get you to the commander. Then someone went out and invented something called the airplane, and all of a sudden, all those commanders were back in reach again. In fact, one of the ways that we hit the Japanese navy in World War II was to shoot down Admiral Yamamoto's command plane.

In our last three battles, we tried to find the other guy's commander. We tried to go after Saddam Hussein, Noriega, and Aidid. By the way, our record was poor. We got Noriega, but only a week after we occupied the entire country. We never did find Saddam Hussein, and we never did find Mohammed Farah Aidid, although CNN seemed to have no problem. A lot of advocates of information warfare talk about this bloodless decapitation. It's not easy to do.

What has been the change wrought by the computer? One of the themes of this book has basically been: okay, we know all about information warfare before the age of the computer. Now, what is the delta that we get with the computer? What's new here?

In my opinion, the biggest difference in C^2W is the change from the commander to the command center. A command center tends to be large and distinct, and hitting it can create considerable damage. The more U.S. forces automate, the more important our command centers become, and the more other forces automate, the more important their command centers are going to become. So the notion of going after a command center is that if you miss the commander and still hit his computer or network, you've done yourself a pretty good piece of work.

What we did in the Gulf War may be extremely hard to replicate in the future because of the nature of computer technology.

What was Saddam Hussein's computer architecture, by and large? It was centralized phone switches and pretty much centralized information systems—that is, Ma Bell and IBM. What is happening with computers is a lot more dispersion and distribution of information, so that there is no longer one core that you can hit. It is possible, technically, to take valuable information and replicate it a thousand times. It is possible to build a cellular grid without any core whatsoever, just a bunch of switches, and the switches can be portable, so if you're really sophisticated you can knock out a bunch of switches, but the rest of the switches can reconstitute a system.

I'm not saying that every Third World country can do so. But my hunch on information technology is that if you've got good mathematical skills and you're willing to learn the stuff, you can learn this stuff. Per capita, I think, Americans know information technology better than others, but I don't think the lead is so wide in all cases, and to assume that other people won't pick it up is foolish. Therefore, the technology allows you to go to cellular grids and use a redundant array of inexpensive disks and other forms of distributed information replication so that there is no longer one single target to hit.

For instance, what do we do in command centers? We get the commanders together to have a conference. Wouldn't it be nice if you could hit all these guys around the conference table at once? If you go to video conferencing over cellular telephony, you never have to put these people in the same room at all. Now, that may not necessarily be the best way to hold a meeting, but if you're under a heavy attack, that may not be a bad second best way to do it.

One of the purposes stated for C^2W is to attack the other guy's decision-making cycle. If you could figure out how the other guy makes his decisions, and you can at least slow it down, you could have a demonstrable effect. You don't necessarily, according to this theory, have to destroy it.

All this theory relates to the OODA (observe-orient-decide-act) loop. There is a large school of thought in the Pentagon that finds the superiority of American forces and the contribution of information technology in our ability to make decisions a lot faster than the other guy can. We can now get inside his cycle. That comes from John Boyd's* theory of air power, and it comes from making decisions at, basically, synaptic speeds, which is to say fractions of seconds, and being able to maneuver an aircraft in terms of firing positions. But somehow this specialized application has become the *leitmotif* of a large percentage of the Pentagon.

There are other ways of looking at the OODA loop. In 1973, during the Arab-Israeli War, the Israelis were very surprised by Egypt's use of Sagger antitank missiles. I don't know whether the Israelis didn't know that Saggers existed, didn't think the Egyptians could handle them, or didn't know how effective they were, but whatever it was, the Israelis lost a lot of tanks. It looked bad for a while, but the Israelis are pretty smart warriors, and it took them a couple of weeks to figure out how to defeat Egyptians armed with Saggers, and it had something to do with using mortars or combined arms or artillery or whatever, but whatever it was ...

Student: Having been involved in that, I know there is a little bit more to it than that. But you're right.

Libicki: They were able to figure it out, to go from "I observe that we are having a real problem" to being able to act on a solution over a two-week period, and since it was a four-week war, two weeks, in fact, was good enough. The Israelis were able to drive the Egyptians beyond the Suez Canal.

By contrast, the Iraqis never really did figure out how we picked apart their air defense system, and we did a very good job doing that because their OODA cycle was actually a good deal slower than six weeks, which was how long it took us to win there. OODA loops are not always measured in seconds. Maybe the important ones are measured in weeks, and they're not functions of computers, but they're

* Col. John Boyd, USAF, a pilot and combat theorist in the so-called Military Reform Movement of the late 1970s.

functions of individuals using their own wetware (brains). That's something to keep in mind.

Last item. Is it always wise to decapitate the other side?

Student: No.

Libicki: Good. I'm glad we got an answer to that question real quick. The answer is sometimes yes and sometimes no. At Appomattox, the Union wanted Lee to surrender all his troops. Had Lee chosen an alternative path, or had he not been available to surrender his troops, there might have been many years of guerrilla warfare to come. By the same token, if you're fighting a nuclear war, and you're fighting an enemy who's using negative control over his forces, if you decapitate the other side, you may not be able to stop a nuclear war. Until you know how the other side is wired, you may want to rethink your decapitation theories to a large extent.

There is one other aspect I want to bring into this as well, related to future prospects for intelligence. In World War II it took roughly 2,500 bombs to hit a point target because, at the altitudes we were flying, we were so inaccurate. By the Vietnam War, even before precision munitions, bomb guidance systems became a lot more accurate, so it only took about 120 bombs to hit the same target point. In 1972, the U.S. troops introduced the Walleye missile, and we use one of the many descendants of the Walleye missile, the laser-guided bomb, to prove pretty adequately that if you have air control, one bomb would be sufficient to take out a target.

Somebody has offered that the same ratio is going to continue with information warfare: that, in fact, we can choose which of the 50 targets to hit and thus continue on that downslope. But what people seem to forget is how much intelligence—and I mean not brain power, but intel—needs to be collected to determine precisely what that target is.

We basically have three ways of collecting intelligence in the armed forces. One way is to use sensors to collect bits from the battlefield as ELINT or PHOTINT, et cetera; we're getting better at that. The second way is to pick up signals intelligence (SIGINT), which we're going to get worse at as people use cryptography, although I'll get to that in a minute. The third way is human intelligence (HUMINT), in which we're probably not going to get any better or any worse because of the computer revolution, because we're still dealing with the same wetware.

The kind of intelligence that it takes to determine who's making what decision is almost all HUMINT and SIGINT. We're not going to get any better at that, so we may have the tools to strike that 1 out of 50 nodes, but we probably will not be any better at getting the intelligence to identify that 1 out of every 50 nodes. That's another overall generalization about information warfare: to do it correctly requires a lot of intelligence about the other guy's information architecture, and if you don't have that intelligence, a lot of what you're doing is a shot in the dark.

I tend to wax more enthusiastic about this information- or intelligence-based warfare than I do about information warfare in general (figure 5). One of the effects of the information revolution is that the cost of collecting a bit is going down with every given year. As the cost of collecting a bit goes down, the same amount of resources can get you more and more bits. The net result is that on the modern battlefield we can see better and better, and that's going to make some profound changes in warfare.

What did we formerly ask intelligence to do? We said, "Okay, we're fighting a battle. I want you to tell me where the other guy's tank columns are, and try to give me

- **To the system of systems**
- **From intelligence to operations**
- **Attacking a system of systems**
  - Directly
  - Maskirovka
- **An instrumented peasantry?**

Figure 5

Intelligence-Based Warfare

a guess as to where he's going to come at me." We are now getting close to the point (I don't know if we're there yet) where we're going to ask the intelligence assets not to tell us where the other guy's tank column is, but to tell us where every single tank is, because we now have weapons that we can get on top of every single tank. That kind of processing power, combined with that kind of weapons, will change the nature of certain types of conventional warfare very seriously. But it also means that J-2 and J-3, not to mention J-6, have all got to be working together, not the ways that they are now currently stovepiped.

Now, the other guy who is being seen is probably not going to be very happy about that turn of events, and he's going to be spending a lot his time trying to degrade that system of systems. There are essentially two ways of degrading it. One is to attack the sensors directly. To a certain extent, we depend on a lot of very vulnerable sensors. The AWACS (Airborne Warning and Control System) and the JSTARS (Joint Surveillance Target Attack Radar System) are extremely capable tools, but they all use active energy to do their jobs, which means they all radiate like Christmas trees, which means that they're almost impossible to hide against an adversary with weapons that are long enough to get at them. Since each one of those aircraft costs somewhere between $250 million and $500 million, a strategy of going after that aircraft in conventional warfare is probably an intelligent one. Therefore, the United States will probably end up having to go, sooner or later (and I hope it's sooner), to an information architecture that uses a lot of smaller sensors rather than a few large sensors.

The other way is through basically *maskirovka*—pretending that you are something that you are not. I don't want to get too deeply into this because it's again another discussion. A tank tends to look like a tank. You may try to camouflage a tank, you may try to hide it in leaves, but, in fact, there are so many things that a tank does that say "tank" that they're extremely difficult things to hide. If, however, you take a 23-millimeter Bushmaster and you mount it on a pickup truck, then for most sensors it's going to look like a pickup truck. If you've got a war in which you can replace tanks by pickup trucks, which you can't always, you're going to be able to confuse this system or at least force it to work a good deal harder, because we either have to target every single pickup truck, or we have to go with a lot more close-in forces to be able to determine which are the pickup trucks and which are the ones with the Bushmasters on them.

The slide mentions an instrumented peasantry. This is sort of my East Asian fantasy for the kind of wars we're going to fight. A middle-income Asian city has many households with hardly enough protein to eat, but they find a way of buying a lot of cheap Japanese consumer goods. One of these consumer goods is video cameras. Take a city like Bangkok, which will soon approach 10 million people, and is a middle-income city. Perhaps a million households will soon have video cameras. Imagine how many of them are going to have cellular telephones. Imagine how many of them are going to have GPS receivers, which are now coming in pagers. Imagine trying to conduct a military operation in that kind of environment and stay hidden. It's not an easy thing to do. It's not going to be only our system of systems; it's going to be other people's systems, and there's going to be this warm electronic glow out there.

I don't want to get any deeper into that because that is really another lecture. I would point out that people who talk about information warfare tend to forget to include this form of information warfare, but in many cases, this is going to be the most effective form we've got.

Electronic warfare, jamming, and interception, all that sort of stuff (figure 6), is quite historic. This is World War II. This is Battle of Britain. We're getting better. We're going digital. We can do frequency hopping, et cetera, but essentially, it's the same parameters. One's ability to jam the other guy has to do with the square of the distance of the signal in communications or, with radar, the fourth power of the distance of the signal, and the extent to which you use all the bandwidth in the signal. Pretty much the only interesting form of

- **Forms**
  - Anti-communications
  - Anti-radar
  - Cryptography
- **Fates**
  - Power
  - Precision
  - Population
  - Towards unbreakable codes

Figure 6
Electronic Warfare

electronic warfare to come on has been the more efficient use of spread spectrum and other code division multiple access (CDMA) technologies. My hunch is that jamming is a matter of power, position, population, and bandwidth.

The ability to generate electronic power from chemicals isn't going up all that fast. Our ability to do digital communications is going up very fast, and since the cost of electronics is going down, our ability to proliferate these things is going up somewhat fast. My conclusion is that over time, even though this has historically been a seesaw battle, I would have to put my money on the bits getting through one way or the other. Now, in a heavy electronic warfare environment, you have to do a lot more processing to make sure you've got the right bits going through. But I don't see that as an insurmountable problem.

Finally I'm going to mention cryptography. My hunch is—and not having received any classified piece of information on this topic, I can speak freely in total ignorance—that the day of unbreakable cryptography is upon us. The cost of making a code of a certain level of difficulty unbreakable is going down much faster than the cost of cracking the code at a certain level of difficulty. If I make a key length long enough, I can make sure that for all practical purposes it won't be broken. Now, there is a technology that people are talking about called quantum computing, which will at least allow you to break certain types of codes fairly easily, but no one's proved that you can actually make one of these quantum computers yet, so I'm not going to worry about it.

Oettinger: You should, though. There are proposals going to the National Science Foundation and ARPA and so on, and it's beginning to look as though maybe it isn't as wild and woolly as one thought six months ago.

Libicki: Two factors suggest that it's probably going to be about 20 years before we worry about it. One is simply that that's how long it takes for authentically new technology to get to engineering. The other method has to do with error correction. These quantum computers are analog systems. All systems tend to drift. A digital system will also drift, but it's always corrected with every cycle, so you always get back to a zero or a one. There is a small chance that you'll end up with a zero when your computer should have given you a one, but it's an extremely small chance, and nobody even bothers thinking about it now.

Oettinger: On the contrary, one thinks about it a great deal, but it's under control.

Libicki: It's under control. Okay, *I* just don't think about it; other people think about it. The quantum computing problem may be a more difficult problem in terms of error correction than any other analog computer, and my hunch is it will take a long time to crack that.

Student: It may. I don't mean to take the lecture from you, but let me just show another part to you here. That's great for high-level systems. We are the first military around the world to have gone to enciphered and encoded systems almost across the board, and from ship to ship or airplane to airplane that's not really hard to do. Going from soldier to soldier, or tank to tank, or in the middle of Bangkok and all that sort of stuff is very, very difficult to do. You run into a cost problem to diffuse systems at that low a level. You run into a problem of actually distributing codes even if you distribute electronically at that level, and what reality is showing us is that the advent of digital technology is not manifesting itself in codes going everywhere, but in Mohammed Farah Aidid running around with a cellular telephone, which makes him, in fact, very easy to follow.

So when we start talking about the lead that we have, or the advantage that we have over people, it is that we actually have an electronic society, and as much as we want to talk about Malaysia, or the Middle East, or the Ethiopians, they are not electronic societies. They tend to latch on to one of these things and diffuse it and use it extensively, where it's child's play for us now, in a sense.

Libicki: Yes, but then what happens when, 10 or 15 years from now, every cellular telephone has cryptography built into it, and, in fact, it's harder to turn it off than it is to turn it on?

Student: Oh, yes, you're right. The other side of that is that it would be very easy to break by the time that happens.

Libicki: I don't think so.

Student: We get into funny areas here. I just wanted to point out that there's more to this than meets the eye. That is my whole point here.

Oettinger: Maybe you're initiating a discussion about measures and countermeasures.

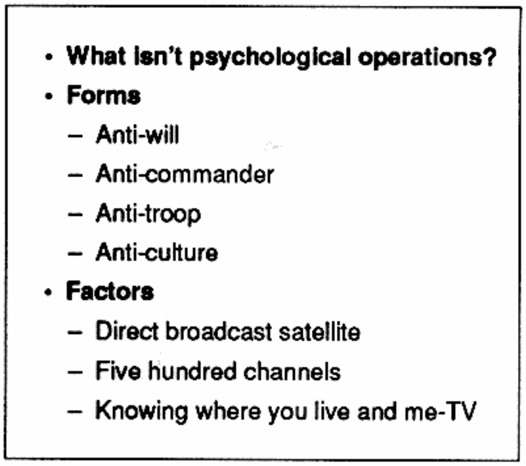
Student: Yes, tit for tat, who knows what it's going to be.

Oettinger: It's hard to tell how that would come out.

Libicki: What was it that Damon Runyon said? "The race does not always go to the swiftest, nor the battle to the strongest, but that's the way to bet."

Student: Absolutely.

Libicki: Let me talk about psychological operations (figure 7). As I mentioned, if it's badly defined, you have everything in psychological operations. There are basically four types, or people talk about four types. The first one is a sort of CNN effect. How do you organize the line that your country, your forces, et cetera, are putting out in such a way as to influence the populace of the other country? The classic case, getting back to our good friend Mohammed Farah Aidid,* is that when they had the fire fight in Mogadishu, and were dragging the body across the streets, they were convincing the American public that we no longer wanted to be in Somalia.



- **What isn't psychological operations?**
- **Forms**
  - Anti-will
  - Anti-commander
  - Anti-troop
  - Anti-culture
- **Factors**
  - Direct broadcast satellite
  - Five hundred channels
  - Knowing where you live and me-TV

Figure 7

Psychological Operations

A few weeks later, we had signed an accord with the leaders of Haiti. The people in Haiti, having watched CNN, and seen the effect of Somalia, rioted when the *U.S.S. Harlan County* came to drop off the peacekeepers, because they had seen how a small amount of opposition, magnified through CNN, in fact was able to manipulate U.S. will. That's a very important fact of psychological operations.

Anti-commander. One of the most important forms of information warfare is to make the other guy's command leadership think you are going to do things you aren't going to do. The deception that Allied forces pulled off against Hitler during the Normandy invasion to convince him that we were going to Calais, when we were in

* Died, August 1996, of violence, in Mogadishu.

fact going to Normandy, is a classic of information warfare. We did something similar to the Japanese by convincing them that we posed a threat to them from the Aleutians. In the Gulf War, we convinced the Iraqis we were going to have a seaborne invasion of Kuwait, and we also led them to think that we were going to use air in a much different way than we ended up using air. This is a classic form of information warfare. It's always going to be with us, and always ought to be with us in terms of being good warriors.

Anti-troop involves the dropping of leaflets and a lot of other more sophisticated objects. Again, it's a classic form of psychological warfare.

I mention anti-culture, even though it's something that nobody in the United States really understands unless they've recently been or talked overseas. But once you get outside the good old 50 states, there is this notion that America's going to conquer the world by selling it blue jeans and Madonna records and Kentucky Fried Chicken, and we're going to homogenize and destroy everybody else's culture, so take it for what you will.

Most of the basics of psychological operations originate in the human mind, originate in human nature, have not changed radically since Thucydides, and are not going to change radically from here on out, because they basically have to do with the three messages of warfare: If you're nice to us, we'll be nice to you; if you're not nice to us, we'll be nasty to you; and God is on our side. Everything is just sort of a variation of those three messages. It depends how you play that.

Let me talk a little bit about what may change. The first thing is direct broadcast satellites. We're getting to the point where we have the capability, as does the Disney Channel, of getting any message to somebody with a direct broadcast satellite connection, and that basically means that you can now start talking to the other side. Right now we talk to the other side through CNN, but in the future we're going to be able to talk to the other side directly. I think that's going to have an effect. I'm not quite sure exactly what that effect is.

The question that one may legitimately ask is: Does the United States have a national edge at psychological operations? I would have to say we have a big plus and a big minus. The big plus is that we really do understand the media. We've been awash in that stuff for half a century. We export political consultants; we don't import them. In that sense, I think we understand what you can do with the media.

On the other hand, I would have to argue that Americans are probably among the most parochial of people on God's green earth. We don't learn foreign languages. We don't learn foreign cultures. We even tend to assume that there are no foreign cultures; it's just Americans who eat funny food and wear funny clothes. Most people in the world—Europe is an example—are forced to learn about other cultures, are forced to be internationalized from the get-go, and the result is that I think in many ways foreigners have a better understanding of Americans than Americans have of foreigners. One of the great secrets, by the way, of the United States is that in world terms we're definitely an outlier. Did you ever go to a sociology class? Europe is the norm. The United States is off somewhere on another tangent. Anyway, enough of that.

Oettinger: Wait a minute, before you go on. Even that is not new. Maybe it is on a global scale, but in World War II, you could hear Hitler in France and England and Churchill in Germany, and so the directness of the communication was there. It's a little bit like the arguments over strategic bombing. It isn't exactly clear what the effects were. There were effects, but 50 years later, we're still arguing over what difference it made. It just seems to me that direct broadcast satellite line is more a higher-up among the things that are eternal. The scales are changing.

Student: The media change. We had direct broadcast radio in World War II. They had a radio receiver instead of a DBS.

Libicki: Could those guys really reach the American mainland?

Oettinger: No, but I think ...

Student: That's true, you couldn't go transcontinental.

Oettinger: If you short-waved it, you could, of course. You could tune in, not all that reliably, but if you had a short-wave receiver, you could hear any damn thing you wanted.

Libicki: The proliferation of channels, in many ways, is going to make life a lot more difficult. If you've got a world in which fly-fishermen are tuning into their fly-fishing channels and chess enthusiasts are tuning into their chess channel, et cetera, it's going to be more difficult to craft a message that will appeal to everybody in your own country or in different countries. We are eventually going to something that's called Me-TV, "eventually" being a term of art, which is to say that people are going to be able to start putting together their own menu selections, either through their software agents or through some sort of information broker or whatever. That basically says that the day of the mass media is rapidly drifting away.

Did you ever get one of these cards that actually had your name on it and it had some sort of facts about you and how much you like to do this and how much you like to do that? They've already established that technology in the world of mass mailing. In terms of the world of the media, that's coming. I wonder if there's going to be a way to reach soldiers on the other side actually by name; whether we will, in fact, have that kind of information. If we do, it's also going to change the nature of psychological operations a lot.

Student: I'd like to know some of the funny interactions you get between the different types of operations you're talking about. For example, the community of psychological operations has to do with manipulating the other guy's OODA loop. You've got to stay out of this OODA loop. If your insight is stifled, then your psychological operations don't have time to take effect before you're already acting. So you could have instances where you're cutting yourself off from these different avenues.

Libicki: One of the classic issues coming out of Iraq was: Do we blow up the TV tower or do we put propaganda on the TV tower? Yes, you've got to look at these issues.

I'm going to switch gears here and spend about the next half hour or so talking about hacker warfare (figure 8). Other than Tony, are any of you people here computer folks? None?

Oettinger: Are you a nerd?

Libicki: Anybody ever done any programming?

Student: BASIC on punch cards. I'm that old.

Student: FORTRAN.

Libicki: Let me just sort of go into that. There is a large group of people among the information warfare enthusiasts who make statements to the effect that attacks on information systems, particularly attacks on domestic information systems, are going to be the way people go to war. Or if it's not the way people are going to go to war, it's going to be an important component of overall national strategy.

- **Reasons for vulnerability**
  - Dependence on computers
  - Open networks
  - Open operating systems
  - New innovations
- **Ordinary attacks (greed, spite, spying, services)**
- **Extraordinary attacks (disruption and corruption)**
- **Military vs. civilian attacks**

Figure 8

Hacker Warfare: Foundations

Somebody I know, who shall remain nameless, talks about all this military stuff we have as the Maginot Line, which is the old technology, when the new technology really has everything to do with hacker warfare. This is total nonsense. I don't think that these things apply. If you all agree, that cuts my lecture down by 30 minutes, but just in case you get into an argument with somebody who doesn't agree with me, let me just go through this. The reason I don't think so is because I think the amount of harm you can do that way is relatively small, particularly if you're going against a well-prepared system. Thus, I think we do a disservice to ourselves if we panic prematurely.

A lot of people who go into this panic about computers don't really understand how computers work and what computers do. A service that shall remain nameless spent a lot of money thinking about how you could broadcast viruses; how you could somehow spray computer viruses into other people's computer systems. Somehow you sort of inject these viruses into the atmosphere and they end up in other people's computers. The problem is that a lot of people who talk glibly about computers don't understand them terribly well. If we had computer people here, I would say, "myself included," but now I can say it safely without that.

Why are people more worried about this? I would say the overall vulnerability basis of American society to hacker warfare has got to be rising. We are becoming increasingly dependent on computers. When was the last time you got money from a bank, and did you see a human face when you did it? That's only the tip of the iceberg. Our computers are becoming increasingly networked, not only through the Internet, but also through modem pools and to each other, which means that people can get access to computers in ways they couldn't get access to them before.

Open operating systems. The mainframe was meant to house the company jewels, and you could only access it through certain, prespecified, narrow ways. We are going to much more open systems now. MVS and VMS (those are IBM's and DEC's operating systems) had security elements built into them very consciously because of the way computers were understood. UNIX was developed at a university, where information sharing is the norm.

Oettinger: UNIX was developed at Bell Labs.

Libicki: I mean the Berkeley UNIX. And, in fact, the culture (at Bell Labs) is essentially an academic one.

Oettinger: The guy who did it at Bell Labs was one of our students.

Libicki: Now, what did I do when I started this lecture by listing my Web home page? I put down information that will allow you to get information that is in my computer system, because I'm from an academic environment. I want this information to spread. However, the Department of Defense is not an academic environment, by and large. We don't want information to spread, but we find ourselves using computers that were built on that assumption. If you take a look at the personal computer, it started off as a hobby kit. The notion of a hobby kit was that an amateur should be able to get at every single thing on that computer. So we've got personal computers that don't generally have the safeguards that we're used to in more sophisticated computers. They let anybody write any piece of information in any part of the computer. We haven't got rid of that legacy.

Finally, just in case you thought you'd solved all your old security problems, people are inventing absolutely new security problems for you to deal with. For instance, there's something called objects over networks. An object is a piece of data and a piece of code that can manipulate it. If you pick up somebody's object, how do you know it isn't a virus? If you use a macro, many of the Microsoft macros (and I don't think they're the only guilty ones) are capable of launching a virus into your system. Many Web browsers are capable of picking up a virus and putting it into your system. Neat innovations are coming through, but they sometimes have a little downside. So people are right to worry about this.

Now having said that, let me spend the rest of the time talking about the opposite point. There are a lot of nasty things you can do with computers, and there are a lot of them out there. Most people who run computer systems are aware of them, particularly people who run computer systems in which there is real money on the line.

I would identify six basic nasty things you can do with computers. You can steal money. You can steal services. You can spy on people. You can make people's lives miserable. You can cause computer systems to malfunction. And you can cause computer systems to function with incorrect information.

I divide these things into two forms of attack, one of which I call ordinary attacks, and one which I call extraordinary attacks. Let me talk about extraordinary attacks first.

Why would somebody want to take down the power grid of Massachusetts? You would have to have a really big reason to go to that kind of effort. Either you don't like the state of Massachusetts for some reason, or you're trying to cause the state of Massachusetts to suffer, or you're trying to cause the United States to suffer, et cetera. Most acts of large disruption or corruption presume an opponent, and if they're complicated enough, they presume a well-heeled and, perhaps, organized opponent.

However, ordinary attacks do not presume an opponent. They generally depend on human emotions that are ever present in the human condition, for instance, greed. In a world of absolute peace, you will have greed, and therefore, you will have people who will try to steal from banks. You will have people who will try to make telephone calls that they are not paying for. Intelligence is ever present, so you will have people who want to get other people's information. Spite is ever present in the human condition.

Now, why am I going through this litany? Because with any form of risk in this world, we take precautions against this. We take what's called an optimal amount of precaution if we understand the risk correctly. That is to say, a car that is so safe that you couldn't possibly get killed in it wouldn't go more than 20 miles an hour, and the doors would be immensely thick. We don't build our cars that way. We put in some safety features and not other safety features because we optimize. By the same token, if you're running a funds transfer institutional mechanism, or better yet, a cellular telephone system, you accept a certain amount of loss. People have tried to put security features in cellular telephone systems only to find they were too complicated for users to use and scared a lot of them away. So the cellular phone people are willing to accept the state where about one out of every 14 calls isn't paid for.

Oettinger: We just lost $500 worth of purloined calls that showed up on our bill, but the supplier absorbs it. To them it's a small fish in a large pool of risk. If we have a pliable instrument to carry around, we remain happy customers, and a loss that would be intolerable for us is not a big deal in their pool.

Libicki: And, in fact, the cost to the phone company of $500 worth of calls is much less than $500. Crooks don't need billing and servicing, for instance, trivially speaking. But if you're managing a funds transfer system, and you lose $1 out of every $14, you're not going to be in business for very long, so people optimize at different levels. What people cannot optimize against is an attack that has no history, or an attack that is caused by extraordinary events.

Before I got into this game, I used to be in industrial mobilization. One of the issues in industrial mobilization is: If there's always a chance that we may need five times as many missiles today as we did yesterday, why doesn't private enterprise itself build the extra capacity? The answer is: Because the chances that we'll actually need the extra missiles are so low that it doesn't pay these guys. They will build their capacity to what the normal day-to-day requirement for the item is, and the government, if it wants the extra capacity, will have to pay for it.

By the same token, if you are talking about attacks that either have no history or are extremely rare, it is difficult to convince people to put in an adequate amount of protection against them. All I'm saying is, concentrate on ordinary attacks and don't worry about the extraordinary ones.

Oettinger: Let me lay some groundwork for you on that because I don't want too much to flow before your point about culture and ordinariness is lost. Recognizing greed. In the old days, a bank's standard practice was that everybody, from the vice president and the president down to the lowliest teller, had to take a vacation, and your failure to take a vacation was an indication that maybe you were a bit unsavory. Now, why insistence on vacation? Because everybody knew, first of all, that anybody in a bank could be greedy. Second, defalcations, one way or another, were time sensitive, and in two weeks, any kited check would have cleared or anything else would have shown up someplace. So they were forced to take their vacations. You essentially put a firewall between them and the large-scale effects of greed.

The computer culture never understood that. Programmers are not forced to take vacations. It took quite a while to get to an understanding that if you're programming banking systems, maybe you need to have, for example, programs from which programmers take vacations so that some other guy can audit the damn thing, and you now require a conspiracy of two programmers, et cetera. It isn't that these are occult things that have no precedents. The culture point that you made is a very good one.

Libicki: I'm going to be spending my time talking about attacks on civilian systems, but I do want to make the point that if we get into a war, I would expect that the other guy will, in fact, try to attack our military systems, and therefore it is incumbent upon the Department of Defense to put in the requisite amount of security in these systems. Whether they attack civilian systems is a different issue, but I think the motive for their attacking military systems is fairly clear cut.

Essentially we're talking about four types of attack. One (and this is well beloved by the paranoids and people at the National Security Agency) is the notion that we may have corrupted components. There is a reason why that's the only government agency that casts its own silicon chips. They do not trust the commercial market to do it, because either they're paranoid, or they've figured out that the risks of anything going bad are so great that they can't afford to trust anybody. There's a hypothetical story that there's an information warfare attack because some guy in Malaysia has been paid off by the Mujaheddin and he changes the mask on one of the chips and all of a sudden every single new personal computer has this chip defect in it, and they all go down at the same time. It sounds like a fantasy to me. I hope it sounds like a fantasy to everybody else. There's a certain amount of that in weapons systems, which is to say, I would not be surprised if some of the weapons systems sold by the U.S. and other Western countries have some fail-safe circuits in them. But that's far different from suggesting that every personal computer has those sorts of circuits in them.

The most common form of computer corruption is going to be by an insider, not an outsider, because the insider understands the system, understands the nuances of the system, and has privileges on the system that the outsider does not have, so that if you're trying to protect your system, notions such as getting your programmers to take vacations, making sure that you hire trusted people, and making sure that only a certain few users can bring down the system are valid.

However, if you're trying to attack the United States, and you want to do it by recruiting insiders, you've got your work cut out for you. The reason is as follows: you've got to recruit a certain number of insiders. Some of them are always going to go bad on you. Maybe they get these pangs of remorse and run to the FBI. At that point, you've been discovered, and the efficacy of your operation goes down very sharply because people go on the lookout for these things, security goes up, perhaps you get caught, et cetera. That is to say, random computer crime is likely to be by an insider, but systematic computer crime by using insiders is much, much harder to do.

So, the dominating image of a hacker attack, basically, is one done by outsiders. Some friend from—name your Asian country—calls in, gets on the Internet, gets into a bank system, steals lots of money, takes down the phone system, takes down the power system, et cetera.

A large number of computer systems make a distinction between users and superusers. The user gets services from the computer. The superuser can change a lot of the parameters of a computer. Most security systems tend to prevent illicit people from becoming users, but they should also pay attention keeping users from being superusers. The rule on this thing is: Any sufficiently large system will have a bad apple on it, and that probability will approach one as the system gets larger. If any user can crash your system, chances are you haven't made the correct distinctions, and your system will go down.

Oettinger: Again, this is a cultural theme. Nobody would think of positive control of nuclear weapons without dual keys, et cetera. I cannot imagine, in the computer culture these days, the notion of dual keys being very clever. It just has not occurred. And so, when people are talking about hacker warfare it's because they're dealing with sloppy systems. It isn't that the techniques are unknown. If you really want to protect the computer system, you could sharply reduce that probability by doing things that are familiar to anybody who's worked with nukes: some form of positive control, duplicate keys, et cetera.

Libicki: Vigilance is really a word that gets right down here. Let me talk about more primitive defenses. One of the reasons I tend to be relatively skeptical about hacker warfare is the notion that I believe that a virtual system can be protected much better than a real system can, in many respects. If you all remember, several years ago somebody dropped a mortar round on Number 10 Downing Street. What's to prevent somebody from driving a bomb-laden van up in front of the New York Stock Exchange and setting it off? However, I don't know if you noticed that the second largest computer exchange in the world is located in—what town? Rockville, Maryland. See, you haven't heard. It's NASDAQ. NASDAQ is a virtual system, and if it's replicated sufficiently (I don't know if it is, but it could be, and not very expensively), it could, in fact, be an extremely difficult system to take down, because what you can do to guard computers is a lot different, and in many ways a lot more tractable, than what you can do to guard physical items.

Oettinger: Actually, the New York Stock Exchange is more virtual than you might think. I was involved in the automation of the Stock Exchange originally, and it was a strange thing. Because of the value of the seats on the Exchange, they needed to maintain a presence in New York, but they couldn't afford to put all the damn computers in there, so many of the operations are in New Jersey.

Libicki: This is just an illustration.

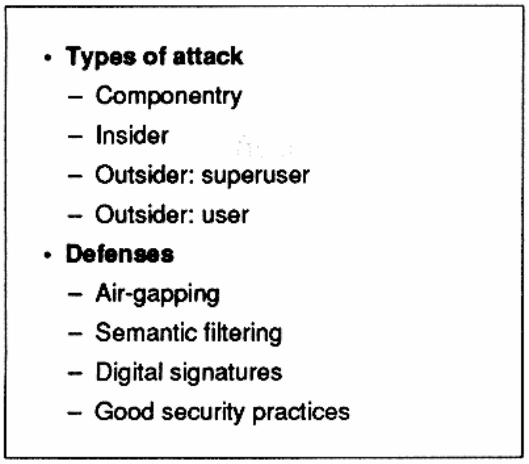
Oettinger: I know, but it illustrates that things are not always as they seem. So the notion of bringing down the New York Stock Exchange is kind of fanciful itself.

Libicki: Tom Clancy notwithstanding.

Oettinger: Tom Clancy notwithstanding.

Libicki: There is one rule I'd like to state about hacker warfare (figure 9); in fact it's so important, I'm going to write it down: There is no such thing as forced entry in cyberspace. If you've gotten into somebody's computer system, it's because the computer system was designed to let people into it. The computer system may not be terribly well designed, so it gets the wrong people into it, but, in fact, the computer system that is not designed to get anybody into it will not have a cyber attack, almost trivially.

Who saw the movie "War Games," from 1983? There was the notion of the nuclear command and control computer actually having a modem pool on it. Now, I admit that we have things like SCADA (supervisory control and data acquisition) systems in electric utilities so that you can



- **Types of attack**
  - Componentry
  - Insider
  - Outsider: superuser
  - Outsider: user
- **Defenses**
  - Air-gapping
  - Semantic filtering
  - Digital signatures
  - Good security practices

Figure 9

Hacker Warfare: Attacks and Defenses

diagnose electric utility equipment from your own home, and that's very convenient. However, the inconvenience of forcing people to go to the office to launch a nuclear attack, I would argue, is relatively small compared to the risks you would have by putting the nuclear command and control system on the Internet. That may be facetious, but in fact, that is how we protect most computer security systems in the DOD. We've air-gapped them. In the future, I would say that there are going to be more negatives than positives on this thing, but it does suggest that if a computer system is sufficiently sensitive, you can always resort to that notion.

Student: Back up, though. Isn't the problem that we're losing the air-gapping and now we're trying to build in the automated firewalls, for example, the DOD InteLink (it's the Web-like interface used in CIA's Intranet), the Top Secret Internet system? But the problem is that nowadays, on a single desk, the guy can also have Internet access through his computer, and so you're now getting into software, and no longer is the air-gapping occurring.

Libicki: That's true. All I'm suggesting is that if you really were worried about that, that's one solution. It's a trivial solution. But, in fact, it's still used a lot.

The next thing is what I call semantic filtering. It's very difficult, despite "Terminator II," to get into an ATM machine and actually reprogram the bank's machines from that. The reason is that the ATM machine only accepts certain codes. Everything else is an error message. You can design computer systems that basically accept data as input and nothing else, if you want to badly enough. As long as you know how to treat every single piece of data, or every combination of data, and know what it does, which is close to checkable if not checkable, then you have a reasonably good level of security.

Another practice is called digital signatures, which is a little more high tech, but we may see it become ubiquitous in about 10 or 20 years. That's a technology that can be used to force everybody to sign every single message in the computer, so that it is associated with a particular individual and there is a guarantee that the message the individual says he sent is in fact the one he sent. I don't want to get into the technology. There are some really nifty technologies, and I think that one's pretty nifty.

Oettinger: By the way, there is also a lot of that being worked on by the private sector, because the protection of intellectual property rights is worth a hell of a lot more to them than we are, at the moment, willing to put into national security issues. Again, from one point of view, that may be annoying because these are civilians and they have better technology than the military or the folks at Fort Meade. But from the point of view of security, folks who have to worry about this are worrying about it. It isn't that somehow the hackers are out there with nobody paying any attention.

Libicki: Yes. Finally, the last one is good security practices. By the way, they're going to have to do a lot of work on firewalls before they're actually good security practices, because a lot of them, it turns out, are fairly leaky. All I'm suggesting is that if you are determined enough to defend the computer system, you can do a good job.

Oettinger: Including having common sense. I may have told you guys this story about my early experience in a major bank, where there was this elaborate interlock and so on to the computer room, identification, et cetera. I'll date this by pointing out that what they did, however, was to take their day's use of punched cards and put them in the trash out in the back alley. You've got to be consistent about security practices.

Libicki: This chart is fairly self explanatory (figure 10). These are the two main parameters you set when you do security choices. You either maintain tight or loose user access, and if you don't spend the money on security, you end up with relatively gross filters. If you spend money on security, you can put in relatively fine filters. It's a fairly simple notion: air-gapping can make systems difficult to use. Not paying any attention to security can let them remain vulnerable, but, in fact, if you spend the money you can get the good guys in and the bad guys out with a higher degree of precision.

This is where I give you an honest answer to the question: How vulnerable is the national information infrastructure (figure 11)? I don't know, and I don't know if anybody else knows.

What kind of statistics do we have on the NII? The first statistic is that there are roughly a million break-ins on the Internet every year. How did I come up with that conclusion? Sort of by reverse division. DISA did an experiment in which they basically used common hacker tools and tried to break into systems, and they found out that only 1 out of every 400 successful break-ins was reported. CERT, the Computer Emergency Response Team at Carnegie Mellon University, reported 2,500 break-ins in 1994. Just to use a rough rule of thumb, if you divide 2,500 by 1 out of 400, you come up with about a million break-ins.

- **No one knows how vulnerable the U.S. is.**
- **Damage estimates are wildly speculative.**
- **The Internet is not a good model of mission-critical systems.**
- **Hacking parameters does not necessarily crash the system.**
- **It is difficult to wipe out distributed memory.**

Figure 11

Hacker Warfare: Vulnerabilities

What does that prove? That proves that most Internet systems are leaky as sieves, frankly. But I would also offer to you that we have not gotten to the point (with a few glaring exceptions) where the nation's mission-critical systems are, in fact, on the Internet. Not to slur my old alma mater, but I came out of Berkeley in the 1970s, as did Berkeley UNIX come out of Berkeley in the 1970s. Computer security, security, Berkeley; those are words that have a hard time going around together. But the broader fact of the matter is that the environment in which the Internet was built was a sharing and a trusting environment. A lot of the

	Less Sophisticated	**More Sophisticated**
Tighter Access	Systems are difficult to use.	Users can get in with effort but no hackers can.
Looser Access	Systems remain vulnerable.	Users can get in easily but most hackers cannot.

Figure 10

Hacker Warfare: Security Choices

problems in the Internet are not problems in the protocols, but they're actually problems in the specific implementations, which people have a hard time working out.

In 1988, Robert Morris—a Harvard graduate, I was told earlier—disabled a large percentage of the Internet ...

Oettinger: While he was at Cornell.

Libicki: He disabled a large number of computers on the Internet because he was able to exploit a hole in a UNIX program called sendmail. In 1994, a teenage hacker from England got into Rome Laboratory. Oh, gosh, a government laboratory! An Air Force laboratory! He was using the same exact hole. And in 1996, a hacker got into Los Alamos computers using the same exact hole.

These are fixable problems but, by and large, they have not yet been fixed. I will illustrate one of the reasons they haven't been fixed relative to our National Defense University.

What are the two bad things that people can do to the National Defense University's computers? They can shut them down, and they can steal information from them. Right? Well, if they shut the NDU network, it will be hard to distinguish from all the other times that the network goes down on its own. (By the way, I recently visited the Air University. It turns out their computer system goes down even more than ours does.) The second thing is: What happens if they steal information from my machine? They will just get information that I generate; you know: "Please review this and send it back to me with your comments." But that's the academic environment, and a lot of office environments have similarly low stealable value of their systems or are similarly undependable.

As the Internet starts being used for commerce (and to my mind it's not clear that in fact the Internet will see that kind of big use—it may or it may not), people will think seriously about security, and people will put security in.

Oettinger: I'll give you a calibration on that. My colleague, Debora Spar, a professor at the Harvard Business School, has just finished a paper on that very subject, some of which will be published in the *Harvard Business Review* and some of which our program will be publishing in a larger version.* So the fact that faculty at the Harvard Business School are beginning to think about these issues of securing systems for commerce when there is actual value on them gives you a sense that this is profitable. In fact, her thesis is that the most money to be made in this area is in providing security services.

Libicki: Well, you make it interesting. The market for anti-viral software is about $3 billion a year. If there were no anti-viral software, would viruses, in fact, cause $3 billion a year in damage?

Oettinger: Probably not, I'd say.

Libicki: Damage estimates are wildly speculative. Winn Schwartau wrote that the cost of computer crime in the United States is somewhere between a $100 billion and $300 billion a year. Yes, billions! The FBI's estimate, which I think is more credible, is somewhere between a $500 million and about $5 billion, and I tend to believe it's on the low end. For instance, we hear the story that banks are always covering up their computer crime. But the fact is that if it's more than $10,000, and a bank is covering it up and not reporting it to the FBI, the bank has committed a federal offense. The laws on our books force this sort of reporting.

Hacking parameters does not necessarily crash the system. Because I can steal information from a system doesn't necessarily mean I can take it down. Because I can alter the way a single phone message goes through the system does not necessarily mean that I can crash the entire phone system. There are various nasty things you can

* Debora Spar, *Cyberrules: Problems and Prospects for On-Line Commerce*, Incidental Paper. Cambridge, MA: Program on Information Resources Policy, Harvard University, in press. See also Debora Spar and Jeffrey J. Bussgang, "Ruling the Net," *Harvard Business Review*, May-June 1996.

do to computers. Being able to do one of them does not necessarily mean that you can do all of them.

Tom Clancy's *Debt of Honor* has a story about wiping out a day's transactions on the New York Stock Exchange. I started thinking about that story for a minute. I said, "Okay. I'm going to buy a share of stock." I call my broker, who calls the other side's broker, and we exchange a share of stock. How many computers have been informed of this trade? My computer, the other side's computer, his broker's computer, the other guy's computer, the Exchange's computer, and probably a half a dozen other computers in the first place.

There are ways to archive data. There are ways to distribute memory. If you have to, you can do it, and then, if worst comes to worst, you can reconstruct it. A paper printout is a very valuable piece of information, and if you don't like tons of paper, because we all love our forests, you can have a CD-ROM. Mastering a CD-ROM is relatively cheap. If you want unerasable memory, you can have it. So there are lots of ways of fixing the system if you want to fix the system.

Now I'll get to an original anecdote because it fits in here. There's a story written down about what happens if Iraq takes out 20 million accounts in the United States. Wouldn't we be forced to do something ugly with Iraq? I asked myself the question, "What happened to the money?" What is a bank deposit? A bank deposit is a loan to a bank. If the bank does not have any memory of this loan anymore, it does not necessarily follow that it no longer owes you the money. If you believe this, I would like to borrow some money from you, because my memory isn't as good as it used to be. The bank is responsible for remembering that it has borrowed money from you. So, the money hasn't disappeared if it hasn't been transferred out of your account.

However, what if Iraq actually took the money, so in the morning you wake up and 20 million Americans have nothing, and Iraq has $50 billion? All I can say is, "It's nice work if you can get it," because if I really knew how to steal $50 billion, I wouldn't have to be an enemy of the United States in order to do it. In fact, I'd just as soon not be an enemy of the United States. I'd just as soon be the Mafia or something that has no physical presence to be hit. You don't have to presuppose an enemy to presuppose that kind of computer crime. Have you ever heard of the scenario in *Time Magazine* called "The Day After"? It was notorious stuff in terms of what the hackers could do. I'm told it was only a decision-making exercise. I wonder what the value of a decision-making exercise is?

Oettinger: Wait a minute. Don't go too fast. You glossed over: What about an information Pearl Harbor? If you'll come to it, don't let me derail you. I'll just ask the question and hang fire.

Libicki: Basically, if you have to think through the problem from the strategic point of view (figure 12), and you wanted to hurt the United States, the notion is that you have to do it all at once, because if you do it in small increments, you will get people to consider security a much more serious problem than they do now. If you get people to consider it a problem, they will put defenses up against intrusions and, therefore, it's not going to be the problem it was. If you hit Chicago with a nuclear weapon, and the next day you hit L.A., L.A. is going to be damaged as much as if you didn't hit Chicago. But if I rob Citibank of $10 million one day, and I tried to do it again the next year, it's going to be a lot harder for me to do that, simply because

- **It is not a problem until it is a problem in which case it soon ceases to be a problem.**
- **How disruptive to society?**
- **How disruptive to the military?**
- **Is it worth annoying someone you have not weakened?**
- **If just anyone can dissuade the U.S., then everyone can.**

Figure 12

Hacker Warfare: Strategic Considerations

they have put the defenses in place. That means that if you're going to be effective, you have to do it all at once.

Now, doing it all at once is not so easy because you probably need a time of prior preparation, which is to say you want actually to put the bad code in the system and then trigger it simultaneously at some point. Prior preparation always runs the risk of being caught through all sorts of random methods. So there is that factor to consider.

The next question is: How disruptive would it be to society? That's an awfully difficult one to answer. For instance, let's say you took down the phone system of this country. If you could restore the phone system in a day, the amount of disruption would be relatively small. People may not buy goods over the telephone one day, but that doesn't necessarily mean they will lose the desire for these goods entirely. They will go ahead and buy them the next day—not always, but to a large extent.

Suppose I turned off all the power. I don't know how many of you have ever lived in PEPCO's (Potomac Electric Power Company) service area. Last year we had power outages once every two weeks. I was always having to reset all my digital equipment. So, if an information terrorist creates one of these power outages, do you think it's going to affect my life all that much?

My experience with PEPCO is: With a wet snow, power lines go down, and I know that if the power lines go down, because we're in an all-electric house, we're going to be cold. So, my first reaction to the notion of a large wet snow would be to get a lot firewood into the house. It turns out we didn't have it. It was not a year of wet snow. It was a year of dry snow, so the power lines never went down. But this is the nature of the disruption.

I think Professor Martin Shubik of Yale did a study of financial systems and their vulnerabilities. One of the things he discovered was that Ireland went without banks for nine months, and people managed to adjust. We really don't know how disruptive a digital Pearl Harbor attack would be to society. But my hunch is that it is a very easy number to overestimate, and, in fact, compared to natural and economic phenomena, it may be fairly small. The Northeastern snowstorm, during the first week in January, cost the Northeast roughly (I used to know this number) about $10 billion worth of losses in goods and services. That's a lot of money. But did we necessarily surrender to anybody as a result of it? If Iraq had caused that kind of snowstorm, would we necessarily not do things in a foreign policy context because of that? Does anybody know what the real cost of a small recession is to the economy? That stuff is measured in hundreds of billions of dollars, compared to which even a digital Pearl Harbor would be small.

One of the reasons that I don't think it's a particularly good weapon is because what you end up doing is annoying somebody you haven't weakened. Why do militaries generally wage war on other militaries rather than civilians? Is it because they're nice guys? No. It's because they want to wage war on the part of the enemy that can, in fact, do them the most harm.

Student: You are just jumping into and across so many issues that I cannot keep up. First off, I've been hearing you say that these threats are without sufficiency, but you acknowledge that there are potential threats. Then you come back and say: "Hey, if we're interested in solutions, the solutions are there." The acknowledgment is, then, that there is a threat. The acknowledgment is also that there is a solution, but it is also an acknowledgment that nobody is using those solutions. A couple of points ago, you said, "Well, this hole that Morris used is the same hole as so-and-so used, and the same hole that everybody uses."

So, basically, we're going to acknowledge that there's a threat. Now you just said, "The reason the military exists is to get at the bad guys." You had an organization in Japan that killed some people with some sarin gas. Whom is it that you're going to attack there? What country are you going to attack? Or what terrorist organization is it that you're going to send the military after? So there's also this ability for somebody to have an impact. They don't have to put together a pipe bomb; they don't have to put together even a gas from a chemical manufacturing plant, but they could cause some relatively significant disruption. It may not be significant, necessarily, on a world scale, but they can cause a significant enough disruption that it is going to have an impact on people. And who, exactly, is going to chase this person down, and how?

Libicki: You're asking a lot of good questions that I was about to get to, but there's a distinction between state action and terrorist action. Let me get to this statement and then get back to the terrorism business.

Consider this apocryphal story: In 1966, a young Vietnamese computer hacker goes to Ho Chi Minh and says, "Ho Chi Minh, your war in Vietnam isn't going so well. I've got this great idea. I'm going to get my hackers into the United States, and I'm going to take out the entire U.S. national telephone system, and then Americans will know not to mess with North Vietnam." Ho Chi Minh scratches his wispy beard, and he promptly sends this young hacker off to political reeducation camp, not to mention computer reeducation camp. Why did he do this? Because the nature of the message that Ho Chi Minh was trying to send was, "Don't screw in our back yard. We're not an enemy of the United States. We're an enemy of the puppet regime in South Vietnam. By supporting these guys and going to war against us, you force us to go war against you. But we are not inherently an enemy of the United States. We are not attacking the United States. Our cause is just and we have lots of friends in the United States who'll stand up and protest U.S. policy in Vietnam." Once North Vietnam takes down the U.S. telephone system, they have changed the nature of the argument and eviscerated the anti-war movement, and they've changed the nature of what we consider acceptable and not acceptable actions against North Vietnam (e.g., our self-imposed constraints on bombing them). I would argue that a rational North Vietnam, even if it could take down the telephone system, might hesitate at doing so, precisely because it would alter the nature of the message they send and create the possibility for retaliation.

Having said that, getting to the terrorism business, we have a lot of opponents out there who don't seem to be rational. If you take a look at the Arab-Israeli conflict and what has led to what, a lot of 14-year-old kids throwing stones and risking death has led to peace negotiations. Hamas blowing up buses has led to gates between Israel and the occupied territories. So the question about the efficacy of terrorism is a very difficult one that I will not answer here, but I will acknowledge that terrorists, in fact, could do things that to states are not rational. The question that implies is, what is the size of the threat?

Student: Just really quickly, states can act irrationally, too. A country could put together a big attack that they shouldn't have launched because they're going to provoke a massive U.S. retaliation, but they don't get the equation quite right in the president's head, and they go ahead and launch it anyway. We still have to deal with the consequences of their having done that.

Libicki: Conceding you're correct, that would still say that there's a distinction between irrationality and stupidity.

Student: Saddam Hussein is stupid, but he's not irrational.

Student: What you're saying is that it's so clear we will respond that it's stupid. But I don't think it's that clear.

Libicki: No. I'm not saying it's so clear. What I'm basically saying is there are risk factors that you have to take into account when you do that, which may deter many rational enemies. I'm making a somewhat weaker statement.

Now, when you're talking about terrorism, you basically have to talk about what is the probability of an event. We have lots of terrorist events in the United States. They certainly have a lot them in Europe, and we have a pattern. What we see in Europe, for instance, which has seen a lot of physical terrorist attacks, are very few computer crashes of the sort that people talk about. So we have a sort of a background level against which to say, "This is the appropriate level of security, given the nature of the threat." Now, it might be that five years from now, the level of the terrorist threat might lead to increasing countermeasures.

Student: Or perhaps Pearl Harbor is not a good analogy because you played it to a nation state. But I would say that if you accept some of the opportunities, and indeed some of the threats you've acknowledged here, these are problems. These are vulnerabilities that we have (I won't call them threats) and if those vulnerabilities really exist, and people, just because they don't perceive that there is anybody who is going to take advantage of them, therefore aren't engaged in trying to protect against anything other than just the ordinary attack, they're not engaged to protect against the extraordinary attacks. Then those vulnerabilities are there.

Libicki: Those vulnerabilities are there, and it's just a question of relative ranking.

Student: We talked about how much it costs for somebody to play on that field. You're the one who then started off with your very first point when you said that there are more bits thrown at this because bits are cheap. So, if bits are cheap, and more people can play in this game, then I've got more people who can get involved in extraordinary types of attacks against us.

Oettinger: I think we've heard Martin say some other things as well, and I think this is important because the cost of bits is not the only thing involved, and this is a truism across the computer world. Mainly, the bits themselves—the computers and so on—are the cheapest part of the whole thing. The expensive parts are, first of all, the software, and then second, the rest of the environment in which all of this is built. What would be important to net out (and this is why I interjected myself here, because I'd like to hear your reactions) is that, yes, those vulnerabilities are there, but in order to exploit them, you also need the corrupt insider, you need this or that and so on. I'm having difficulty in your talk, as well as in others, in getting a sense of what would be the aggregate of things that somebody would need to do in order to mount an attack of a certain scale, and can one even arrive at a rough judgment of relative costs and so on. Bits are cheap, but I can't get my office system to work with just bits. The PCs are the cheapest part, and then I've got all that labor and so on. That's in a benign environment where I'm in charge, and I'm trying to get something done. So I need something more than what you've given us, Martin, to arrive at a kind of conclusion.

Student: You need that vulnerability study first before you can do that.

Libicki: Let me see if I can address your question without actually knowing the answer.

Oettinger: At least it will help us with process.

Libicki: What would it take for me, or me and my friends, as it were, to take down a large portion of the United States and disrupt it? How would I go about doing so? I would probably try to use outside attack as much as possible, because I don't want to be discovered beforehand, unless I happen to start off with some insiders to begin with. I would want to try to get as much intelligence as I could, and that intelligence collection is not going to be trivial. That is to say, I want to know how systems work. I want to know what their vulnerabilities are, and I want to know what the fallback positions are so I can attack those systems that are most vulnerable and have the fewest fallback positions. Then I'd want to spend a good deal of time concocting a way to enter a system and plant something into that system and then not be caught. I'd want to spend a lot of time making sure that I wasn't caught so I wasn't going to alarm people.

My sense is that the intelligence and testing portions will, in fact, take a lot of people. They have to take a lot of the right kind of people, because a single mistake has a relatively high cost in an operation like that. That would be my best guess as to what it would take for that kind of disruption. Then it would end up being a statistical notion of how many systems I go after until the probability that I'm discovered exceeds 50 percent.

Student: If we could back up again, how much of that could be done online? I'm not a UNIX whiz by any stretch of the imagination. If I have 500 terrorists in an unspecified Middle East country, and I send them through two years of a training program, now I've got the first terrorist hacker brigade. Now we're going to start collecting intelligence for the next six months, and after than, we'll spend six more months putting in timed viruses. Can we do all that intelligence collection online by hacking systems? Or do you physically have to go and find out, "This is an IBM 6050 system that they've got here, and the power system and the New York Stock Exchange have something else."

Libicki: The most important intelligence is going to be on shoe leather— knowing the people, knowing the organization, knowing the systems, knowing the relationship between the people and the systems, knowing where the backups are, and knowing what the backups do. You're going to have to recruit a lot of people who look, feel, and smell like the rest of us, if you know what I mean.

Oettinger: Let me give you slightly less here. You could do a lot of it online, but where you would get to mostly is you'd rediscover all those places that have the UNIX systems or whatever with the mail system that has the trapdoor that nobody ever bothered to close.

Student: I guess what I'm thinking of is that if we have 300 of these attacks, and 200 of them fail just because the backups work or whatever, but 100 of them still happen, does that count as a digital Pearl Harbor?

Libicki: It depends on what your effect is. What happened in Pearl Harbor? They destroyed a lot of battleships and, therefore, our ability to conduct military operations and so Japan quickly took a large chunk of Southeast Asia and the Southwest Pacific. It gets back to: If you have merely annoyed people and have not affected their ability to use counterforce, have you done anything worthwhile? A lot of that depends on the relationship between the ability to use military force and the dependence on the civilian infrastructure. There are a lot of issues there.

Clearly, for instance, you cannot take down the nuclear command and control system by hacking the phone lines, because of the way it's set up. I suspect there are a lot of other systems, particularly classified ones, that, in fact, are relatively invulnerable. You could probably take down a lot of logistics systems if you were very lucky. But logistics systems play out over periods of weeks and months, not hours. If you can restore a phone system manually within a period of hours in such a way that they have now changed the settings to make it very hard to do the same thing a second time, you really haven't done much to the military. Do you see what I'm getting at? We're really dealing in an area of unknowns, even this late into the game. My hunch is that it's easy to overestimate, but it's just a hunch, because there's a lot we don't know.

Student: When the J-6 was here a couple of weeks ago, his hunch was just the opposite.* He said his hunch was that, "Since we have gone from being a 'just-in-case' force to being a 'just-in-time' force, I need to have confidence that I can mobilize troops and get them where they're supposed to go on time. That is my top concern, and I don't know that we can do it." I don't want to paraphrase too much of what he said, but he demonstrated a sincere concern about the 95 percent, or whatever the number is, of defense communications that go over civilian infrastructure. His hunch is different than yours, and my question is, why? Is it because he's been convinced by Winn Schwartau or Alvin Toffler, or he's not thought this through?

* See Admiral Cebrowski's presentation in this volume.

Libicki: I hesitate to answer that question, because you're going to ask me to put myself in somebody else's mind.

Student: I was asking from your side about ...

Libicki: I'll ask you a different question. Why should you believe me and not him?

Student: That's a good question.

Student: You're here now.

Libicki: All I can say is that people tend to emphasize the importance of the problems that it's their responsibility to solve, or of those systems that they have responsibility for relative to those systems they don't have responsibility for. That's the basic human situation. He might be very impressed by the ease with which this sort of stuff is done, and he may be right. But I tend to be impressed by how disorganized and sloppy and disaggregated and full of failure any system is.

It took us five months to mobilize for the Gulf. If you lose a couple of days in that process, it's really no big deal. On the other hand, if there's any glitch in the system, and CINCEUR has got a phone out, whom is he going to go to? Whom is he going to put his finger on? He's going to put his finger on the J-6 and the head of DISA and say, "How come you're not supporting me, guys?" If a ship sinks, and you can't get things there, he's not going to go to Cebrowski, so Cebrowski is not going to care so much if a ship sinks. He's going to care if something under his responsibility doesn't work.

I'm not suggesting that he's saying things that he knows aren't true. It's just a natural human tendency basically to see that your part in the universe is big and the rest of the people's part in the universe is very small. Also, there's a wide divergence of opinion in this matter. But the fact is that nobody really knows, and we ought to know. In fact, when I get into do's and don'ts, number two is that we've really had to spend our time understanding the vulnerabilities and the incidence (figure 13); that is, our lack of knowledge at this point. I suspect that, in fact, it is the lack of knowledge, and not that the knowledge is highly classified, which is unfortunate. We really ought to be sifting through the system and saying, "If you can hit this point, what will happen? If you can hit that point, what will happen?" Until then, it is my hunch and his hunch, and we really shouldn't be conducting an enterprise that some people think is so important on the basis of a bunch of hunches.

Student: There is a bureaucratic barrier to even asking those questions right now. If the people we have to ask them of are not within the Department of Defense, they tend to be outside, public network operators, and although they're fairly cooperative, they want to answer the question B, and want to be on tap when we want the question answered.

Libicki: Let me answer one thing. From what I understand, our military logistics

- **Defend defense systems**
- **Understand vulnerabilities, incidents (vice threats)**
- **Upgrade the technologies (also standards, tests)**
- **Focus on the public infrastructure (fix the Internet)**
- **Clarify law (red-teaming, force majeure, global accords)**
- **Promote digital signatures**
- **Seek a good trade-off between security and other values**
- **Respect heterogeneity**
- **But don't make it a war**
  - Responsibility is good.
  - Inflexibility in response is bad.
  - Paranoia is ugly.

Figure 13

Hacker Warfare: Do's and Don'ts

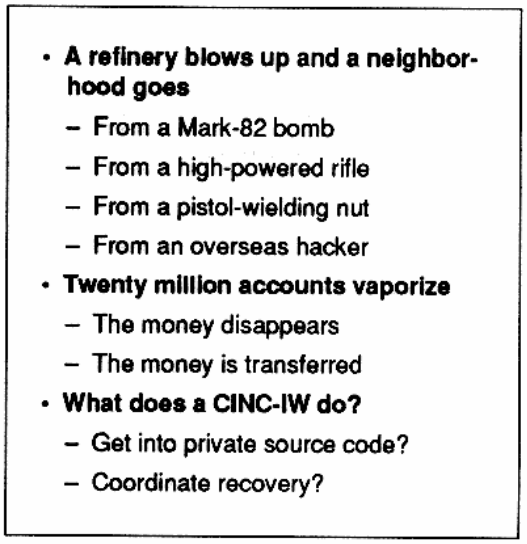
system, which is on the Internet, is, in fact, probably too vulnerable. Money that we spend trying to fix that system up and harden it is probably money well spent.

I have a boss, Dave Alberts,* and he's got one brief that in many ways comes from a diametrically opposite point of view. One day I compared his recommendations and my recommendations, and they're not that far apart. It's really a question of attitude, and how you approach it. It's like nuclear defense. I'm not going to say that it's impossible to hit the United States with a missile, or that Russians will never do it, or the Chinese will never do it. It's really a question about whether you want to excite the country to build an SDI (Strategic Defense Initiative) or whether you're satisfied with the GPALS (Global Protection Against Limited Strikes). I'm saying that in today's information environment let's concentrate on GPALS, and let's not worry about an SDI.

So, do's and don'ts (figure 13). Defending defense systems is extremely important. Understand our vulnerabilities. Upgrade the technologies. We spend about $100 million in R&D on computer security. Done right (and I have to assume it's done right), that's money well spent. There are a lot of places where technology can help. By the way, advancing the technologies, not taking on the role of protection, is what's important. Making protection automatic and easy to use is what's important.

Focus on the public infrastructure is part of the GPALS philosophy. If you're really worried about the hacker attack, focus on the phone system, power distribution, safety systems, and funds transfer. It turns out that only a very small minority of the entire country's computers are in those areas, but those are important to protect if you think you've got a large threat.

How do you upgrade these things? Let me go through the last slide for a second (figure 14). It has to do with the division of responsibility. This is in many ways a legal situation.



- **A refinery blows up and a neighborhood goes**
  - From a Mark-82 bomb
  - From a high-powered rifle
  - From a pistol-wielding nut
  - From an overseas hacker
- **Twenty million accounts vaporize**
  - The money disappears
  - The money is transferred
- **What does a CINC-IW do?**
  - Get into private source code?
  - Coordinate recovery?

Figure 14

Hacker Warfare: Responsibilities

Let's say I have a refinery, and it's located in an urban neighborhood. I'm operating dangerous machinery (a refinery is a very dangerous piece of machinery). Somebody is upset with me, takes an airplane, and drops an Mk-82 bomb on the refinery. The refinery blows up, and the neighborhood is decimated. Who is responsible for the decimation of that community?

I would argue that (using a random oil company) Exxon is not responsible. The reason they're not responsible is that we've taken the problem of national defense and we have socialized it. We have the military to make sure that people don't drop Mk-82 bombs on us. We don't expect people to build refineries to take these hits.

As you start going down the list, the responsibility changes. What about a high-powered rifle? Is it cost-effective to make refineries able to withstand a high-powered rifle attack that would cause the refinery to blow up? That's a little more ambiguous. What about a pistol-wielding nut who gets into your refinery gates? The fact is, you're operating dangerous machinery. You have a public obligation to take prudent steps to make sure that a pistol-wielding nut doesn't get into your refinery. It's called having guards, having gates, not putting the

* Dr. David S. Alberts, Director of the Center for Advanced Command Concepts of the Institute for National Strategic Studies at Fort L.J. McNair, Washington, D.C.

controls where they're too easy to get to, et cetera.

If it's an overseas hacker, at this point I would say Exxon's responsibility ought to be total. If an overseas hacker gets into the refinery and mis-sets a few dials, and the refinery blows up and the neighborhood is decimated, Exxon, in fact, does owe the neighborhood compensation because it was operating dangerous machinery that is entirely under its control, and has not done so wisely and has created public risks. That's all by way of saying that when it actually takes time to securing the systems, it's not something the federal government can do. It's something that owners of computer systems have to do. The federal government is not going to come to Harvard and go to their systems administrators and say, "We want you guys to be secure, and, by the way, I'd like to look at your source code and your operating manual and your accounts to make sure you're secure." A, they ought not do it, and B, they can't do it.

The problem with the military taking up this banner of IW is that they've gotten themselves straight to a point where they have no choice but to say either, "We can't fix the problem," or "We will fix the problem in a very obnoxious way." It's a bad position to be in. I'm surprised that somebody hasn't pointed that out to them already. Should we have a CINC for information warfare? What the hell is this guy going to do? Snoop into everybody's private source code? Coordinate recovery mechanisms? What happens if a system at Harvard is attacked and goes down? You're not going to call some lieutenant colonel. You're going to call the system administrator and say, "How come this is happening? Get my system back up!" There's no need for external allocation of resources because Harvard's systems administrator, for instance, is probably not going to be needed by Mass. General Hospital, which has its own systems administrator and so on. There probably will be some consultants who may have multiple demands on them, but we're getting down to the weeds here. The fact is that there's nothing to coordinate even in terms of defense or protection, and that's something to consider when you start talking about a CINC IW.

Getting back to the previous slide (figure 13), how would you, in fact, get the public infrastructure to get fixed? How would you nudge these guys to do their jobs? I would say two things. One is that we have a lot of agencies for nagging people, such as NSTAC, the National Security Telecommunications Advisory Committee. Many systems owners are regulated industries. Part of getting a public license to be a monopoly is to guarantee a certain quality of service. To some extent, if circumstances warrant, you should be able to hold some people's feet to the fire in terms of proving that they're secure.

The other thing is in terms of liability. One of the reasons I am really uncomfortable with calling hacker warfare "information warfare" is because once you call something "warfare," it's no longer the responsibility of individuals but of governments. The last thing you want is for Boston Edison to say, "Aha, *force majeure*, guys; I'm not responsible. It was an act of war. We're not responsible for that. We don't have to worry about security anymore." You start calling these things information warfare, and you deprive people of responsibility. What you want to say is, "A hacker got into your system, Boston Edison. Shame on you! Start cutting checks to the people whom you have negatively affected, because you haven't done your job."

Student: We need legislation ...

Libicki: No, I don't know if you need legislation. I'm not a lawyer. My sense is that you don't, but I could be wrong. It's also a question of common law responsibility and what is considered normal and what is not considered normal.

Student: I just don't think there's a lot of case law precedent to determine either way at this point why legislation would be very helpful to clearly define this.

Oettinger: Yes, but we get back to the point that legislation that hasn't been preceded by a spate of court adjudications is very rare, and there hasn't been enough experience in this area.

Student: But, because there's not enough experience, Exxon doesn't feel they're liable if a hacker causes their refinery to blow up.

Oettinger: But that's another reason, though, for not calling it war, because a couple of good liability suits would get the message out and catch attention.

Student: I don't have any argument at all with what you said in the past couple of minutes, but I do with the issue that you first brought up, when you said there are some critical things we ought to worry about, like the public switched network. I think you talked about energy and federal wire transfers. If we're going to talk about extraordinary attacks (using your words) or what some people have called structured attacks, the market will not drive commerce to build against a structured attack or an extraordinary attack, because it is not their liability. Now, if we're to focus on that, is the government going to be willing to put forth dollars to help fix that problem if they hear from you and you say it's not really that big a deal, don't really worry about it that much, or are they more apt to hear it if they've got somebody coming in saying, "This is a big deal. You've got to pay attention to this. These are the critical nodes that we need to fix."

Libicki: Why do you say it's not their responsibility?

Student: I think that what you're telling me is that the market will drive a lot of these solutions, and I agree that for the big chunk of this, the market will drive what people will expect. If you want people to stay in your bank, you ought to have a security level that will provide protection against what you call an ordinary attack, an unstructured attack. But is the bank going to go out and spend extra money to protect against a structured or an extraordinary attack?

Libicki: If they're liable for it.

Student: Yes, but why would we make them more liable for that than we do for getting bombed, because they're both national security sites?

Libicki: Precisely because the mechanisms that the bank has to protect itself are within its control, but the mechanisms to protect itself against a bomb are not within its control. That's the whole theory of responsibility. Things that are within your control, you're responsible for getting right.

Student: Whereas we don't want the bank putting an anti-aircraft gun on top of the roof.

Libicki: Yes.

Oettinger: I think that's a very important point, which, until you guys emphasized it, hadn't really fully sunk into me. There is a significant difference.

Student: You're saying, though, that you believe that it is the corporation's, the commercial market's, responsibility to provide protection against a structured attack, or what you call an extraordinary attack?

Libicki: Yes.

Oettinger: If you follow that manner of reasoning, which is very interesting, it may be the responsibility of the government to provide the intelligence with which to alert the private sector to the possibility because, taking his argument one step further, the bank has it within its power to control its information systems, but it may not be aware of a structured attack mounting up, et cetera.

Student: Going upon precedents that we talked about before, the National Security Emergency Response Preparedness actions, the executive orders that drove our preparedness for still being able to have communications after a nuclear exchange, provided government funding that was helping the telephone corporations and so on to ensure that we had that kind of capability. That's a structured attack, but the government says, "You guys don't have any incentive to provide to this level of capability, so we're going to give you some extra money to give us that capability."

Libicki: There may be some call for that as well. In other words, if there's a communications system that you need for a certain military function, then it may be worth the government going out and ensuring the security of those particular nodes that are relevant to that function. To my mind that's good military planning. But that is not going to cover every single phone system in the United States.

Student: Doesn't this discussion assume that the methods of protection lie within the operational control of the banks?

Libicki: Yes, they do.

Student: I can imagine threats (I don't know what they would be specifically) for which the only countermeasures are outside the operational control of the organization, in which case it seems that it's justified for the government to go in and ...

Libicki: If that were true, could we think of an example?

Student: I don't know enough about what a bank does, but you could imagine systems that step out of their control. What you're assuming are vulnerabilities that are inherent within the daily operation of the given organization. But it doesn't seem unreasonable to imagine threats that are outside of the ordinary day-to-day operations of ...

Libicki: I'll give you an example. If I'm transferring money to you, and the money gets lost, is it my responsibility or your responsibility or the responsibility of the guy who owns the wires? That's a legitimate question. But, among the three of us, the responsibility is complete within that loop.

Student: You sent me money, and I didn't get it. Why is it my responsibility?

Libicki: How do I know that you didn't get it because you were hacked?

Student: Then there you go.

Oettinger: Maybe you're lying? Maybe you're saying it so I have to pay twice.

Student: Have him take a polygraph.

Oettinger: No, but he's right. It's among the three of us.

Student: We're going to be chasing each other's tail.

Libicki: Welcome to reality.

Oettinger: Yes, but an outsider doesn't care. A quick last word?

Libicki: That's basically it. Let me just finish up here (figure 13).

Security is good, but security is not the be-all and end-all. If you have so much security that you have to validate every single computer system innovation for years before approving each one, and you can't get any new innovations in there, you may not be doing yourself any favor. By the same token, if we're so busy trying to keep cryptography out of other people's hands that we don't have it in our own hands, we may not be doing ourselves a favor either.

In respect to heterogeneity, coordination is not necessarily the key to security. In fact, an uncoordinated, heterogeneous, mixed-up, not terribly interoperable world in many ways is the best defense against widespread attack.

Student: That's true. We're in a university. We're safe.

Oettinger: That's not an unimportant point.

Martin, we want to thank you very, very much for a fantastic, stimulating, and illuminating presentation.

INCSEMINARS1996

ISBN-1-879716-39-9