INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Information Warfare: A Conceptual Framework
Julie J.C.H. Ryan

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.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-39-9 **I-97-1**

Information Warfare: A Conceptual Framework

Julie J. C. H. Ryan

Julie J.C.H. Ryan is a Senior Associate with Booz-Allen & Hamilton, Inc., where she supports a variety of clients in management consulting, information engineering, and special analytical efforts. Her background includes experience in applied information security, database design and implementation, project conceptualization, program management, and strategic planning. She began her career as an intelligence officer with the Defense Intelligence Agency and the U.S. Air Force, and then became a senior engineer at Sterling Software. Thereafter, she was a senior consultant to Booz-Allen, and then moved to Welkin Associates, Ltd., where she was a member of the technical design review team for a government multilevel secure data processing system for facilitating communications transfers among wide area and local area networks. She then served as a Senior Staff Scientist with TRW Avionics and Surveillance Group. She is a member of the Naval Studies Board of the National Research Council, a member of the Board of Directors of TAC Commercial Services, Inc., and a member of the Highlands Advisory Group to the Assistant Secretary of Defense, C³I. She has written several classified and proprietary documents relating to the impact of information security on the operational integrity of organizations and on governance. Ms. Ryan holds a B.S. from the U.S. Air Force Academy, and is completing an M.S. in information security at Eastern Michigan University.

Ryan: We had a great lunchtime conversation where I started this presentation. I'm sorry not all of you were here to join us, but my method of talking about things is fairly interactive and I would appreciate it if you guys want to jump in at any time.

Tony mentioned that I have a fairly different view of information warfare (IW) from that of the establishment. That's true for a couple of reasons, one of which is that I'm not the establishment. Second of all, my way of looking at things is sort of to analyze the fundamental assumptions that make up changes that occur in life. We started talking about this at lunch. For those of you who were at lunch, I'm going to get more into my analysis framework as we go along. For those of you who weren't, you won't have missed anything.

So, why is information warfare even an important topic (figure 1)? My gut feeling is that this thing that everybody's calling "information warfare" is the tip of the iceberg poking up in a sea, and that there's a huge mountain of stuff that's about to come crashing into our ship, the *Titanic*. And we don't even have a clue about what it is and when it's going to hit. Right now we're seeing that tip of the iceberg, and it is a fundamental problem that we need to analyze and be aware of.

Information warfare is basically warfare in the information dimension. Why is that important? It's important because every aspect of our lives right now is tied to information. That includes everything from the food you buy at the grocery store, how it was produced, how the farmer decided what to produce, how the farmer judged weather patterns, how the farmer fertilized the crops, all the way through to when you woke up this morning and found out we're getting 8 to 15 inches of snow.*

When you start to analyze the information processes underlying our society, they're really quite astonishing. There are dangers inherent in the concept of IW. I think it's very interesting to point out that one of the things that we, as a nation, take great pride in is that we bankrupted the Soviet Union by pushing them into a technological arms race. I'd like to point out that if we push anybody into a technological arms race in information warfare, there

* Chairman's note: Indeed, the Boston and Washington airports closed that evening and Ms. Ryan sat up on a train all night to get home. We owe her a special debt of gratitude.

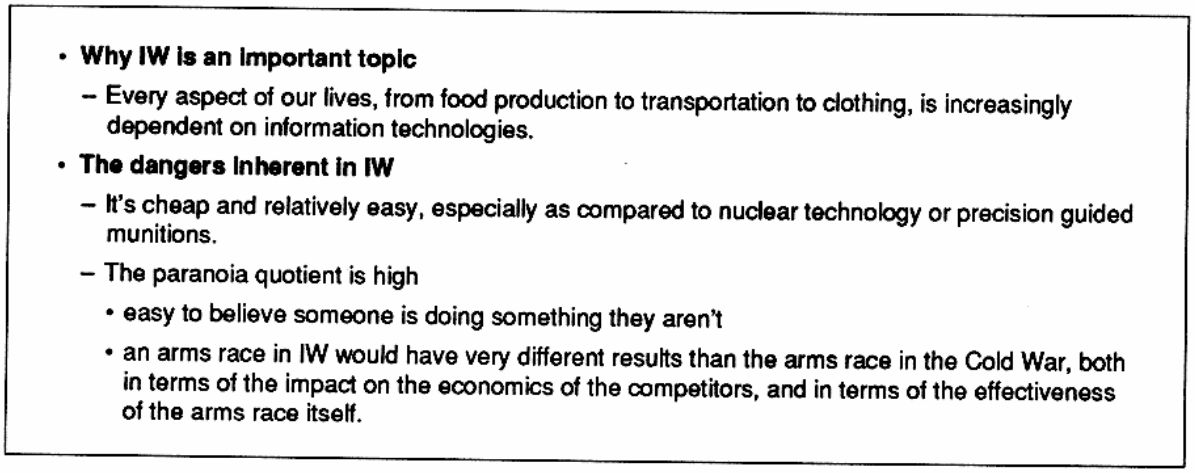

Figure 1

Environmental Summary

are going to be two things that happen, one of which is that their economy is going to improve. The technologies that underlie information warfare are information processing technologies. If you start trying to build an information warfare capability, what you're going to do is increase your nation's capacity to do information processing technology, and that's going to increase your capacity to compete in the global marketplace.

The second thing that's going to happen is that you're going to build paranoia in the global environment. So, I think there are some very tangential topics that need to be considered in information warfare that don't have anything to do precisely with information warfare, but need to be kept in the back of the mind.

Student: When you're talking about information warfare, I'm unclear on your definition of it. You're talking specifically about the electronic storage and transmission of information?

Ryan: Let's skip ahead. What do I mean by information warfare (figure 2)? Funny you should ask. First of all, it is warfare. It's not hacking. It's not crime. It's not espionage. It's warfare. And that raises a bunch of questions in and of itself. For example, what is a strategic attack, in terms of information warfare? It's a very difficult question to answer. Taking down one switch in the public switched network is not a strategic attack. The cascading effects are additionally quite interesting, but the question is: were they intended or were they not intended? Stealing $300 million from a bank is not a strategic attack in information warfare, it's probably not even a tactical attack—it's a pure and simple crime.

So my definition of information warfare is, first of all, it's warfare. Second of all, it's the application of techniques and weapons, on a large scale, for desired purposes, with predictable results, against information assets and systems. Furthermore, in order to be able to do information warfare, I postulate that you have to be able to do it when you want to be able to do it, with predictable results, and where you want to be able to do it. I postulate that being able to do what you can, when you can, where you can, is nothing more than hacking and a nuisance.

Student: I have a question related to this. If we're in a shooting war in, for example, the Persian Gulf, and Iran, in this scenario, has the capability to respond against our civilian information infrastructure with techniques that would normally be terrorism, computer crime, hacking, but it is an orchestrated, strategic attack, does that fit your definition of information warfare?

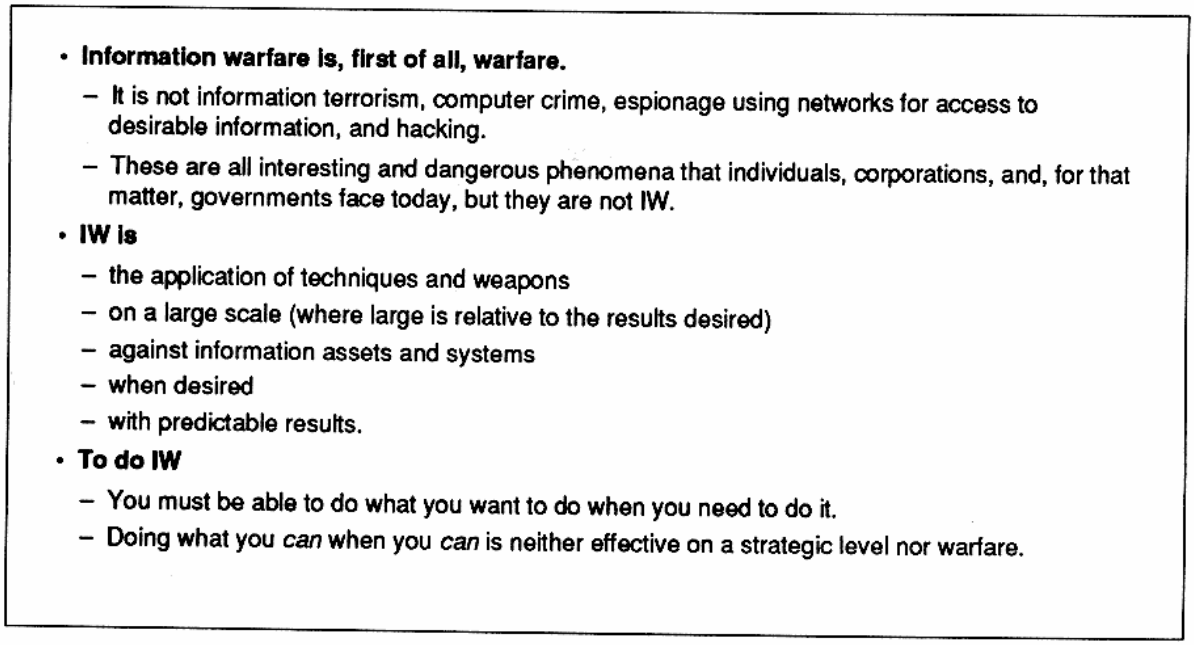

Figure 2
Definition

Ryan: Absolutely. It certainly does. I think that's probably one of the biggest problems. First of all, it's very difficult to detect a large-scale attack. Right now, there is a low level of noise in the information systems underpinning our society. In a large-scale planned attack, that noise could be a wonderful cover and concealment for a purposeful attack in another dimension of our information system. These are very serious options that must be considered.

I think this addresses what you just brought up (figure 3). Military operations are evolving to a very information-intensive environment, and one of the reasons for that is we have high technology, and that requires information systems. You can't do precision-guided munitions without a lot of information infrastructure. Second of all, we've got declining resources and budgets, and we're not as willing to send people in to get slaughtered as we might once have been.

Utilizing information resources enables us to leverage our force ratios much better, so that we can avoid those mass casualties or keep them to a minimum. This also has benefits in the information warfare dimension in that, when you have the CNN pictures of the Gulf War coming into your living room, you don't have to show a lot of Americans being slaughtered for a bunch of Middle East oil.

It's kind of interesting: it's not just American society that is pressured this way, but it's also other societies globally, to include France. When they went into Bosnia, they only sent volunteers. They did not send conscripts.

This is pretty much what I just talked about—information leverages force ratios for operations (figure 4). There's a fair number of military professionals in the room, and this is no news to you guys. To other people, there is a series of equations that are used when determining whether you want to engage or not, and there are leveraging capacities that you factor into those equations. Information is a very high leveraging function for warfare.

So, having given my definition of IW, I'd like to say that I think that it's still very much conceptual (figure 5). This is the tip of the iceberg that I referred to earlier. I think that it is providing a significant challenge to those whom we trust to make policy and strategic decisions for the United States as a whole. And I think there are some first-order questions that need to be addressed, and, by the way, these are being

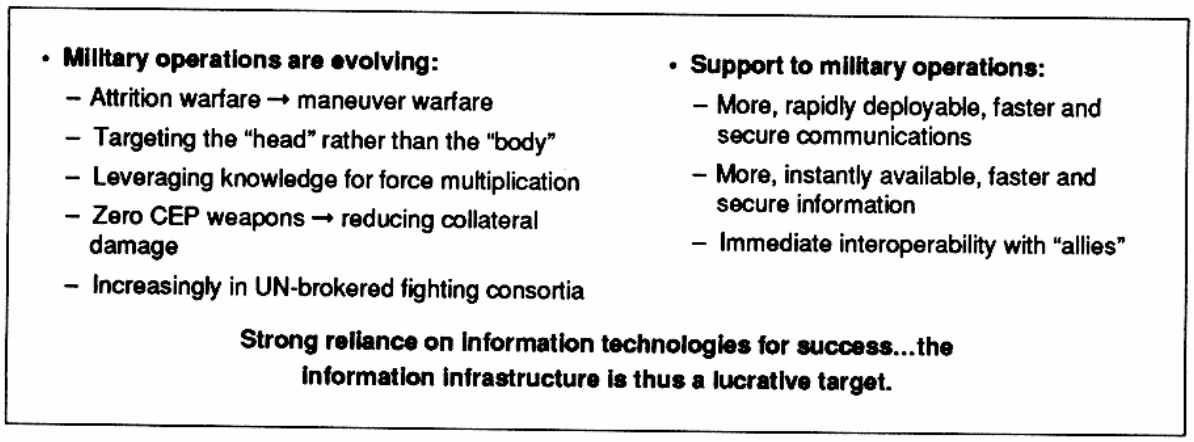

Figure 3

Military Trends

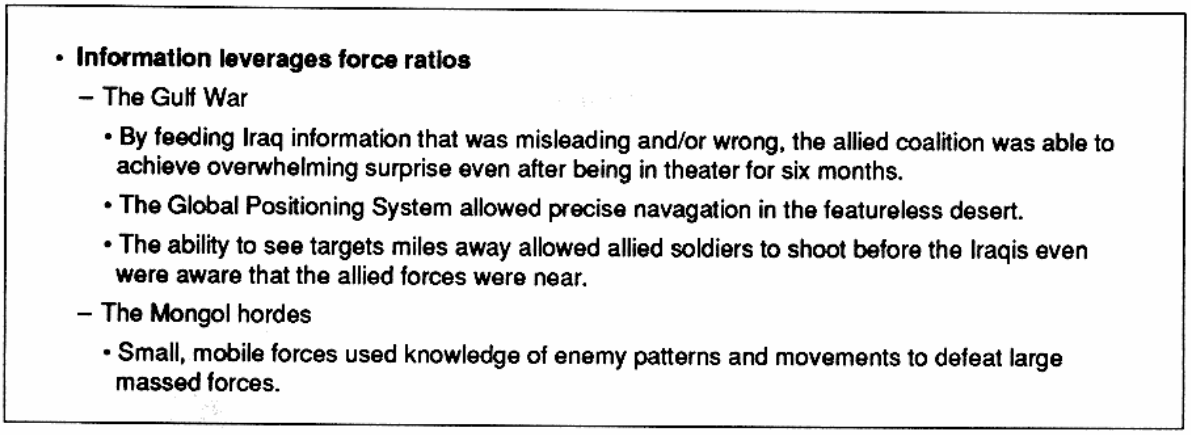

Figure 4

Information and Warfare

addressed. What aspects of the national security are susceptible to information warfare? What is national security?

Oettinger: It seems to me it says "nuclear warfare" on the slide. Do you mean that?

Ryan: Yes, that was an analogy that I was trying. For example, if you have something that has overwhelming power, such as what some people postulate to be a strategic attack in the information dimension, are you best off using an analogy like nuclear warfare where you have a couple of ICBMs coming over? That's one of the things that I've heard: that you have to have at least the effectiveness of five nuclear weapons in order to make a strategic attack in information warfare.

Well, is that a good analogy or not? I don't think so, but it's something that certainly needs to be debated.

Student: Say that again, please.

Ryan: There are some people who say that in order to characterize what would be a strategic attack in information warfare, it should be analogous to five or more nuclear strikes on the United States homeland.

- **IW as a concept**
  - Is still new and evolving,
  - Provides a significant challenge to those responsible for making policy concerning the protection of the nation's security.
- **First order questions**
  - What aspects of national security are susceptible to IW?
    - What aspects of national security are vulnerable to nuclear warfare?
    - How do we assign protection strategies to those entities?
    - What proactive protections do we engage in recognition of value?
  - What parts of the communal defense mechanisms are appropriately engaged in an IW scenario?
- **Assumptions to be scrutinized:**
  - What is national security?
  - What are legitimate roles for the military?
  - What is the difference between warfare and crime?

Figure 5

My View of IW

Student: What would the basis of that be, because one nuclear strike on the U.S. homeland would be a strategic attack on almost anybody's homeland?

Ryan: No, that's not true, actually.

Student: You don't think that if a single nuclear warhead detonated someplace over the United States, it would be focal concern of the President and our national military strategy?

Ryan: It would be a focal point for the national security policy structure, yes, but how they classified it would depend on where it came from and how it was intended and stuff like that.

Student: I think the classifications are actually probably still too biased to the Cold War. A single nuclear detonation would probably dramatically change everything about politics and everything else going on in the United States. To call it nonstrategic, I think, is ...

Ryan: You're raising some interesting points and pointing out precisely why this issue needs to be debated. Different people have different perceptions on what a big threat to the United States is and what a little threat to the United States is.

Oettinger: I think the issue here is an important one. You may be right in terms of a perception, and there might be a reaction on that score, but I think the definition that I hear Julie embracing is one where "strategic" has that sense of being able to bring the United States to its knees, and a real threat to national survival, where mere hysteria may be that way, but that may be self induced as opposed to being produced by the enemy.

Student: Yes, but it's intriguing.

Student: That's right. Strategy is about perceptional management as well.

Oettinger: True, but perception of something that is real is different from perception of something that is not real. We have to keep distinguishing perceptions and reality. Sometimes they coincide and sometimes they don't.

- **This distinction is vital**
  - It endows the ability to determine appropriate response options and responding agencies.
  - Without that distinction, one quickly finds oneself mired in the prospect of sending the Department of Defense against a single 13-year-old hacker.
  - There are real issues here, including the problems of
    - knowing an attack is underway
    - ascertaining the scope of the attack, and
    - bringing to bear effective responses,
  - which can only be resolved after an appropriate framework of policies, practices and procedures has been established.

Figure 6

So What?

Ryan: Yes, that's true. The real question, though, is: Can you know for a fact that an attack is underway? How do you detect that? You have to ascertain the scope of the attack, as we were just discussing, and then you have to bring effective responses to bear according to who's attacking and at what level (figure 6). Without those distinctions, you could have the Department of Defense following after a 13-year-old hacker.

But to really understand what we're talking about here, I'd like to take you through a high-level look at the technologies that are forming the basis for that (figure 7). I've picked one example to go through with you after I run over this slide (figure 8) very quickly.

Student: Before you get into this, does sponsorship of an attack affect whether you consider it to be warfare or not? For example, if it's state sponsored, is that more in our notion of a strategic attack?

In order to understand the potentialities, we must examine the technologies that make all this possible.

Figure 7

The Technology at Heart

Ryan: You mean like when the Libyans sponsored the terrorists to go bomb the Labelle Disco in Berlin, should we have bombed Tripoli or not? Do you mean that kind of question?

Student: It could be sponsored by Libya. or it could be sponsored by Iraq, or it could be sponsored by a nonstate transnational entity. What if it were sponsored by an organization within the United States against the United States?

Ryan: You mean like the Michigan militia type of thing? That's a very difficult question. It's particularly difficult in the information dimension. This is not a new question at all. You had the Whisky Rebellion. You've got a long history of these kinds of problems. Where is the demarcation between an act of war and an act of treachery and just plain crime? Who gets involved—is it the FBI or is it the national defense mechanism, whatever they're called at the time—the War Department, the Department of Defense, or the United States Navy, or the Coast Guard?

This is complicated in the information dimension because of the problem of ascertaining identity. Anonymous remailers, IP

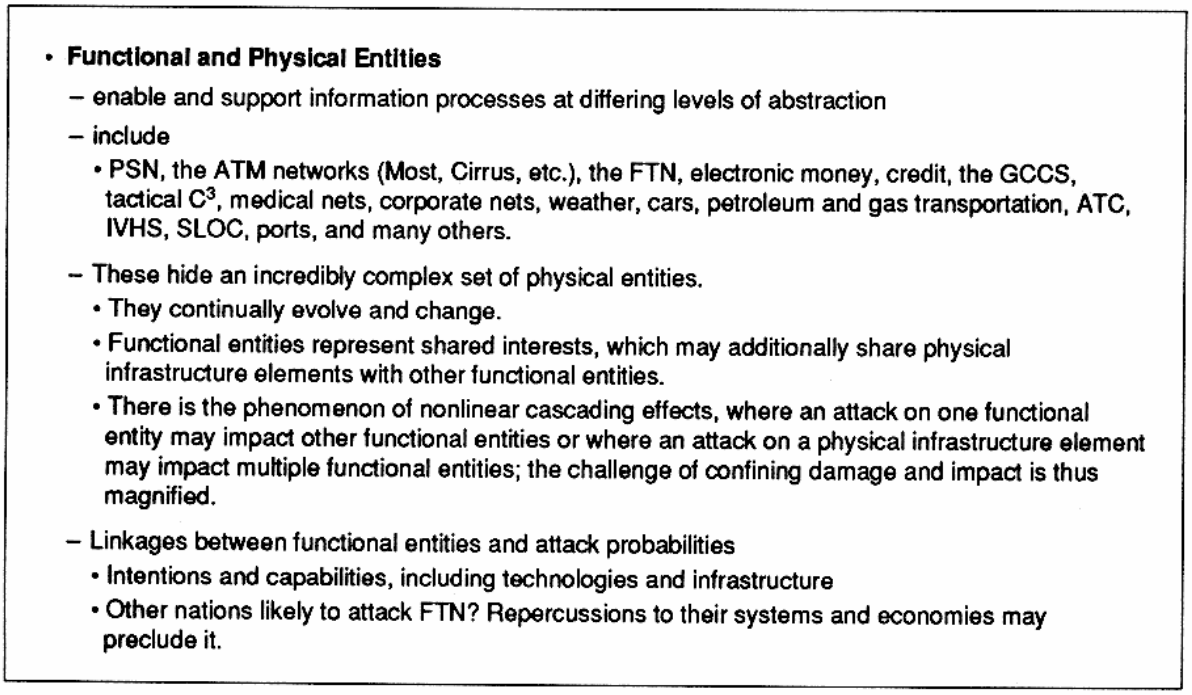

Figure 8

The Evolving Information Sphere

spoofing*—it is possible to have a much greater level of deception about the identity of the person or persons who are perpetrating an attack than in ordinary circumstances, and that has to be addressed at a policy level. You have to have a policy that says that if *this* sort of thing happens, *this* is what we do. If another sort of thing happens, *this* is what we do, and if we find out we're wrong later, *this* is what we do. That's the entire purpose of having policies in place: you have *a priori* thought about problems that may occur, and you have a process in place to address those problems.

We've pretty much covered this slide (figure 8). The society as a whole, globally as well as nationally, is totally supported by an intricate network of functional entities that are, in turn, generally supported by an incredibly complex and ever-changing and evolving level of physical entities. Most people have no clue about them.

Student: On the previous slide (figure 7) about having the Defense Department go after the 13-year-old, I don't understand exactly what the problem is. What does that address? Is it that you don't want the Defense Department being responsible for preventing or assessing, or is it ... ?

Ryan: No. There are several issues there. First of all, who is the 13-year-old? Is the 13-year-old a U.S. person? Is he just screwing around committing a crime or is he actually attacking the infrastructure of the United States? This gets back to the question of processes and policies. If the 13-year-old is just screwing around, do you really want the vast resources of the Department of Defense coming to bear on

* IP snooping: the practice of eavesdropping on networks to pick up IP packets. IP spoofing: changing your legitimate Internet Protocol (IP) packet address to that of someone else in order to do nefarious things; examples include getting through a firewall, using someone's "name" to cover your tracks, or gaining access to a system. Hackers claim this is easy to do. [Speaker's note: Having never attempted it, I have no way of supporting or criticizing that claim. Intuitively, though, it seems a fair amount of sophistication and knowledge would be needed to do that.]

that, or is something that criminal prosecution elements ought to take care of?

Student: But it still should be up to the Department of Defense to detect this 13-year-old's assaults.

Oettinger: That's against the law in some circumstances. Domestic crime is not the province of the military. Now, again, having made that stark statement, there are ambiguities, but that's precisely what makes this a hard question. Just in the first instance, under the law as it exists, who has authority to deal with it?

Ryan: It's not clear. Right now the Secret Service and the FBI and local law enforcement agencies are handling it, and that's probably the right way to go about doing it. The question of detecting an attack or characterizing what appears to be an attack, but is simply screwing around or a nuisance as opposed to an actual attack by an opponent, is a very difficult one.

Student: That slide (figure 8) says "a complex set of physical entities." All the service providers, like in the public switched network, which are only proliferating with telecommunications deregulation, make the physical aspect of this maybe even easier to sort out than all the virtual elements. If you make a phone call and you're using your cellular phone and all the virtual networks it goes through—leased lines, switching capacity—those are even tougher to sort out than the complex switching systems and physical manifestations of that information infrastructure.

Ryan: There's an interesting notion that's called "transparency to the user" that hides much of what's going on underneath in the physical level from the actual people who are using it. I'm not entirely sure it's possible even to have a take on a configuration management from the people who own the service, much less somebody who's trying to break into it. These distributed networks we have change hourly.

Student: The woman who's the vice president for service assurance of U.S. West made the argument last week that the telecommunications law, with all the portability, basically makes it impossible to trace. They're not going to be able to tell anybody who's using their network at any given time, especially when they're required to provide service to anybody who's technically capable of attaching to their network.

Ryan: Yes, especially when you look at technologies like out-of-band signaling.* That just makes it even harder.

Student: With reference to the 13-year-old again, I guess, in terms of the nuclear or strategic route, it's pretty tough to imagine somebody fooling around in their basement and causing a nuclear detonation, but today it seems less impossible to imagine. You make this distinction between careless hacking and sort of playing around versus an actual attack. What are our safeguards against careless fooling around turning into a strategic attack—something really incredible happening?

Ryan: That's a very interesting question. That comes down to how you defend your infrastructure against attacks. The first-order line of defense you have is good engineering. There's a story about a dam—I think it's up in Washington state—that has computer-controlled floodgates that are accessible by the Internet. That is bad engineering! That's beyond the security problem. That is bad engineering. I hope that answers your concerns.

Student: But legally, when you're considering the parties that cause these things, when suddenly someone who is not looking for that sort of responsibility, maybe by breaking some minor laws, causes something that we would look at as almost a military threat ...?

Ryan: Like the Internet worm. It is the great richness of the United States that we

* Out-of-band signaling, also called "out-of-channel" signaling, is the practice of sending control signals in a channel other than the message channel.

protect individual freedoms and liberties as much as we do. As such, even if it were of tremendous import, which some have claimed that the Internet worm was, we treat it as a criminal matter and prosecute it accordingly. I'm not sure any other country would prosecute it any differently, but the notion of treating it as an attack and treating the perpetrator as an attacker, in this particular instance, seems ludicrous.

Oettinger: Especially since he was a Harvard man.

Ryan: I wasn't even going to mention that.

So I'd just like to take you through one tiny little example (figure 9). I had no idea that this was going to be as appropriate as it turns out to be, given the illustrious professor's ingenuity with cellular technology. Does anybody here *not* have a cellular phone? Oh, my God! You can tell I'm from Washington. Between me and my husband, we've got six.

Oettinger: Her reference was to an altercation with my wife last night, when I was unable to answer a call she made to me because I fumbled with the wrong button.

Student: Cellularly challenged.

Ryan: I guess this is a little more appropriate than I thought. The information processes underlying a cellular telephone system are just extraordinary. You've got real-time communications with very complex databases, not only to process the telephone call itself, but also to do the hand-off between the towers, which are operating on very low power frequencies and stuff like

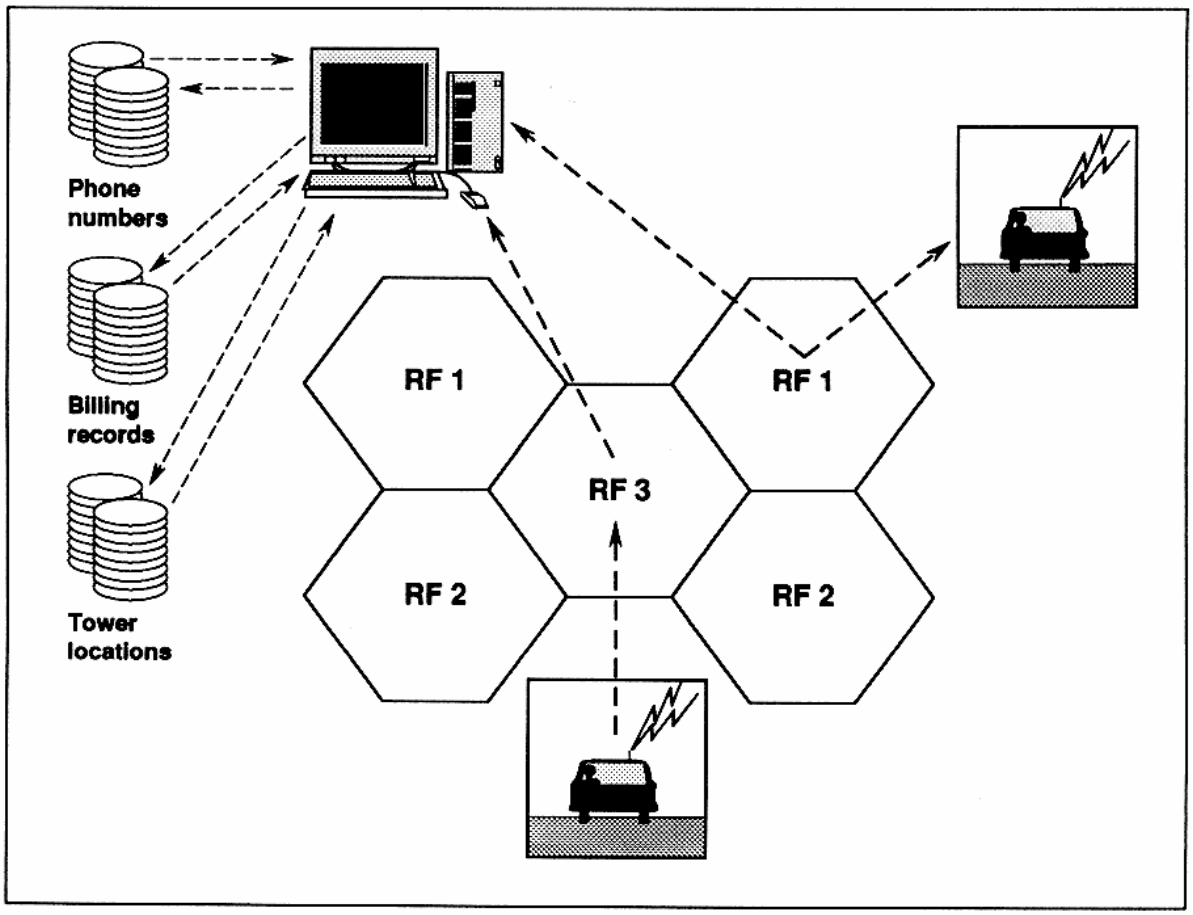

Figure 9

Cellular Technologies

that. Without information processing, and specifically without large capacity information processing, none of this would be possible.

So, then you look at the antecedents (figure 10). The first cellular network, 1979, in Japan. The first U.S. cellular network, 1982. The first mobile telephone, 1946. All this sort of cascaded from when they first figured out how to harness electricity in 1650, and people started screwing around with electromagnetic radiation research. It cascaded to how to put that stuff in use for communications, until all of a sudden you've got just a bunch of stuff coming together to create cellular phones. This is not a unique situation in terms of the information technologies that support us. They all sort of look like this: a bunch of different stuff coming together to create something really new and interesting and innovative.

Now, could you have predicted that we would have cellular phones, even in 1946, when you had mobile phones? No. The ability to predict the future with any degree of fidelity is absolutely impossible. The complex interactions of available technology, human ingenuity, and evolving societal structures preclude foreknowledge. That's

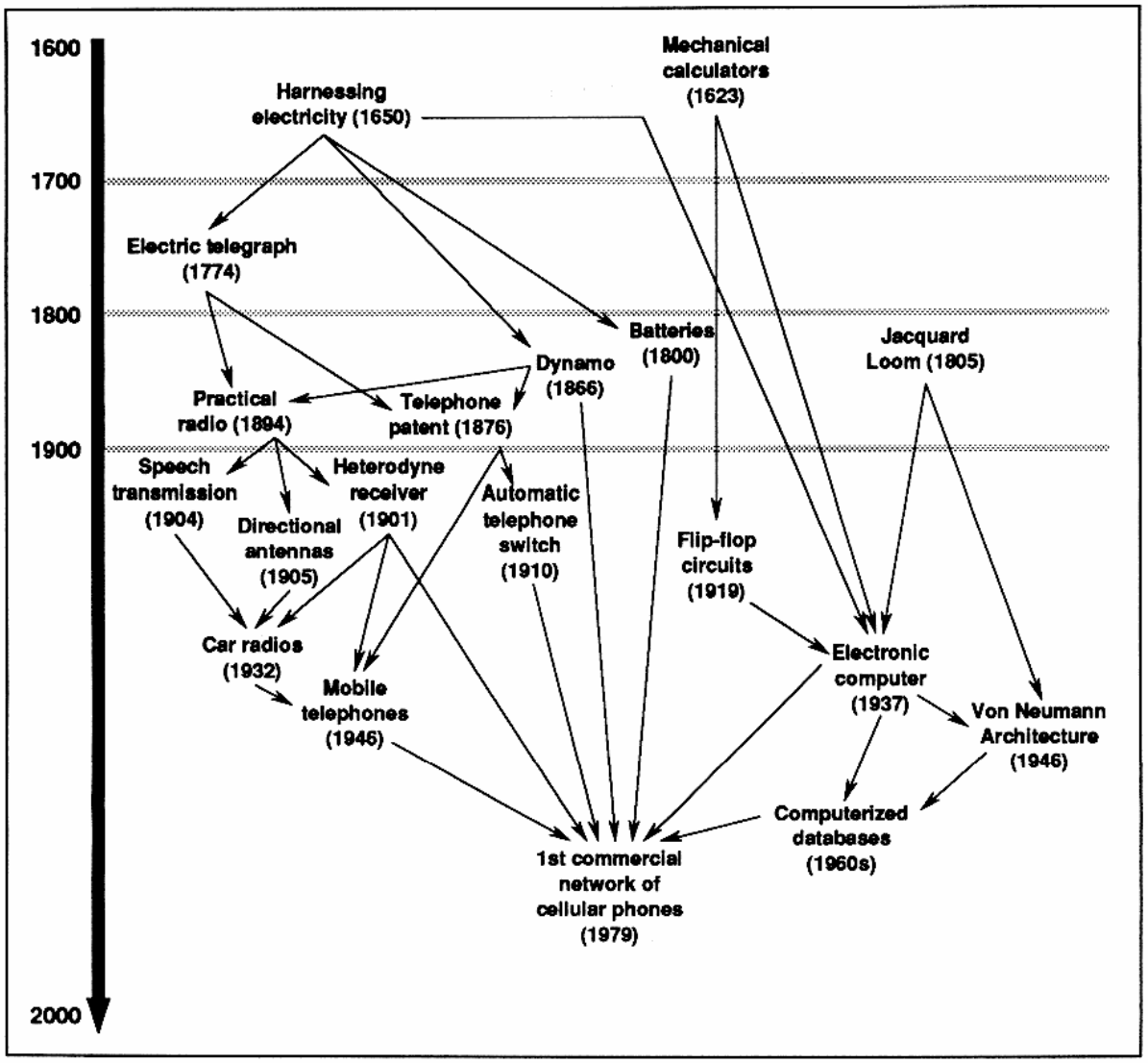

Figure 10

Antecedents

particularly true when you're talking about adapting information technology to lifestyles and society and cultural frameworks and the way we defend ourselves against people who are trying to impact our lifestyles (figure 11).

So, what I've done is set up a framework for analysis (figures 12 and 13). You've got existing things that are used for military operations. You've got tanks, you've got guns, and you've got command and control systems. These things have evolved over time and they are right now very nicely focused on how we conduct competition between nation states.

You've also got new stuff that's coming on line. You've got this increasing interaction of information technologies fundamentally supporting societies, and it's changing the way we run markets. It's changing the way we live our lives on a daily basis. It's giving us increased

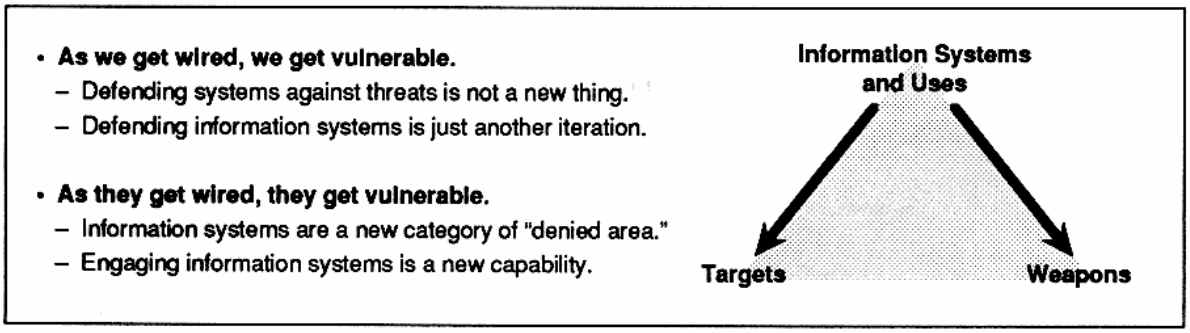

Figure 11

Information Technology

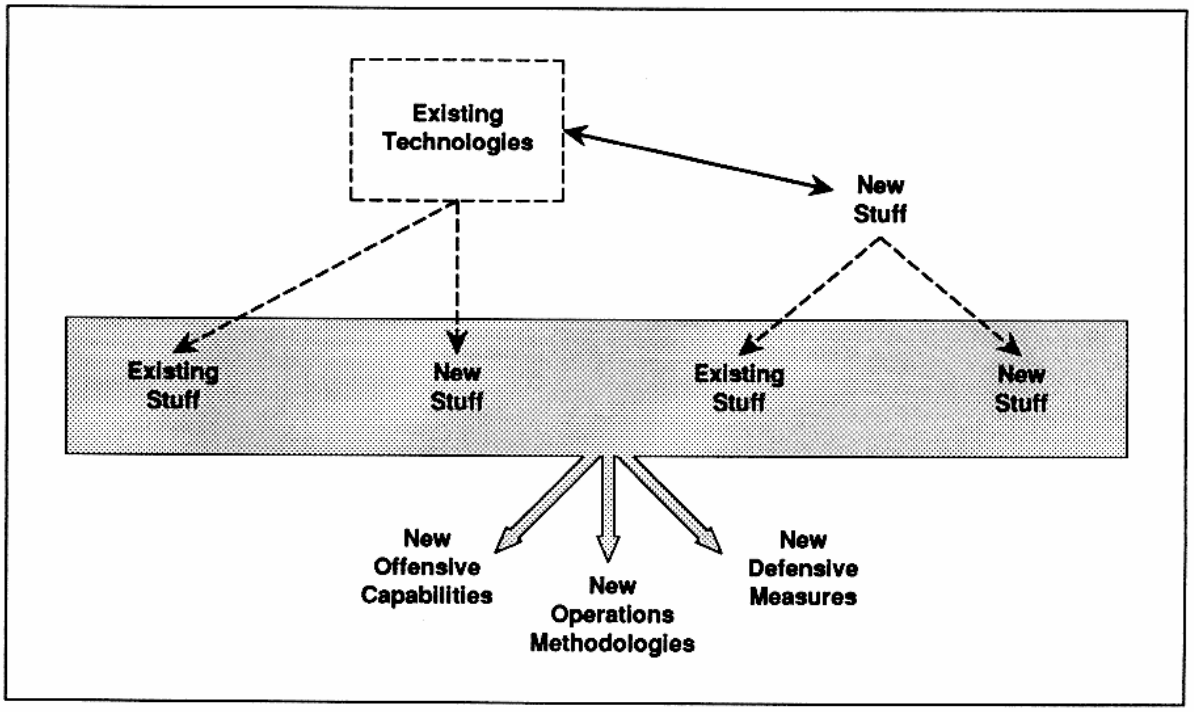

Figure 12

Framework for Analysis – 1

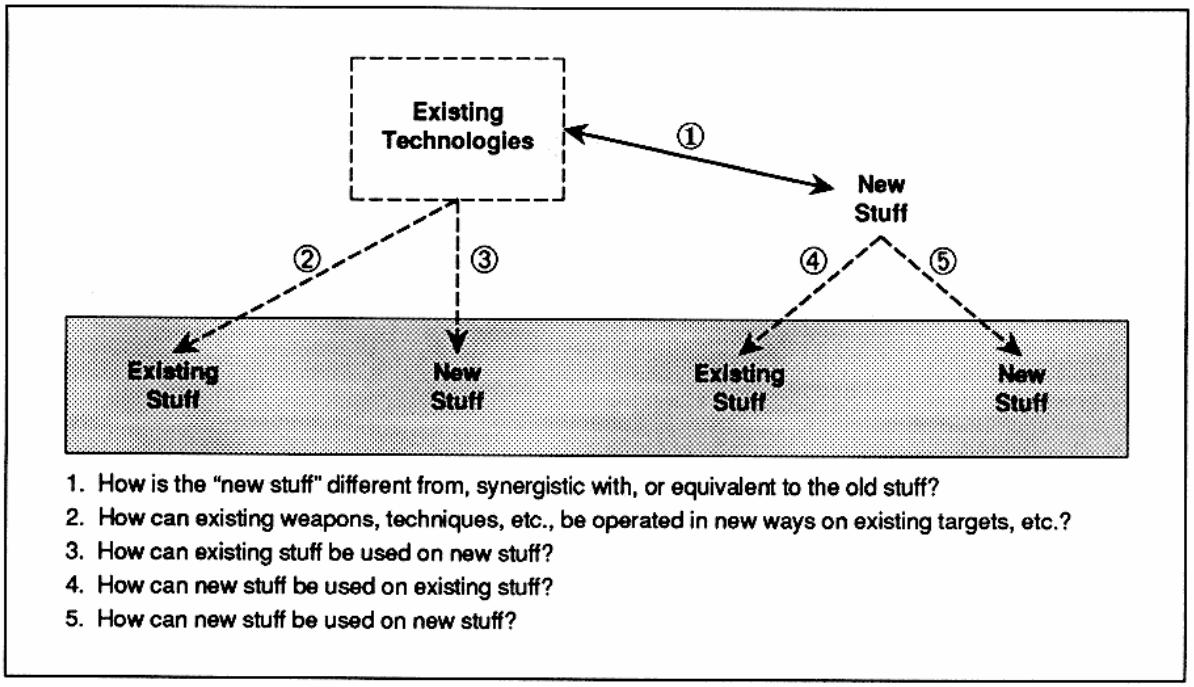

Figure 13

Framework for Analysis – 2

capacity to predict the weather. There are different ways that these things interact. You've got new ways in which technologies can operate on existing targets and techniques. You've got ways that existing weapons and technologies can operate on the new stuff: for example, taking a gun and shooting out the feeder horn on a precision antenna takes out the antenna.

You've got the way the new stuff operates on the existing stuff, and you've got the way the new stuff operates on the new stuff. You have to examine that entire scope to understand what the changes are going to be to the way you conduct warfare.

Another way of looking at it is to put it into knowledge quadrants (figure 14). This is a technique that I like to use a lot. I don't know if any of you guys are familiar with this or not.

Oettinger: They are indeed. You're talking about unk-unks (unknown unknowns).

Ryan: In that case, I can just go right past this, to underscore the point that there are things that you don't know that can be done (figure 15). I particularly like the one on the 3M Post-It Notes: "If I had thought about it, I wouldn't have done the experiment because everybody said that it couldn't be done." This is the course of human events. People do things because they don't know it's not possible, and it turns out to be possible.

So, how does the analysis of new stuff on existing stuff, and existing stuff on new stuff, and new stuff on new stuff, fall into these quadrants (figure 16)? The white rectangle is where most people are comfortable. The darker shaded rectangle is probably where your highest payoff is going to be, and the questions on information technology's applicability to warfare fall mainly in the shaded rectangle. So, where do you find people focusing their efforts? You find them focusing their efforts in the white rectangle.

So, you ask yourself: What do we know that we know and what do we know that we don't know (figure 17)? We actually know quite a lot, but we might not be applying it correctly. We know a lot from information security. We know a lot from

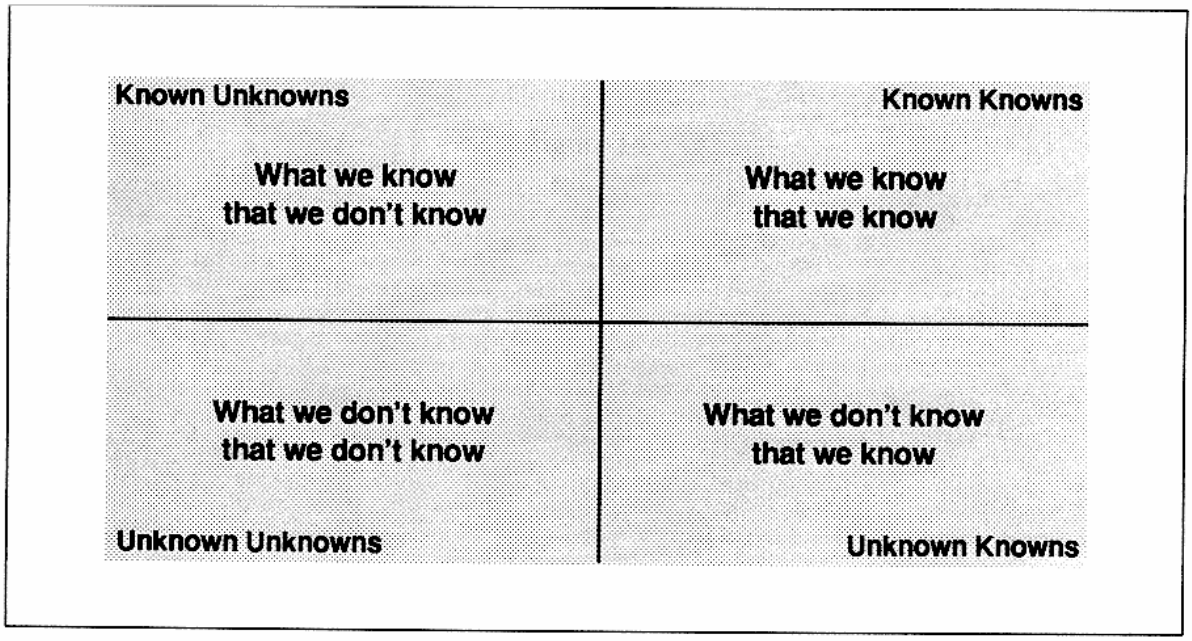

Figure 14

Knowledge Quadrants

- **"Airplanes are interesting toys but of no military value."**
  – Maréchal Ferdinand Foch, Professor of Strategy, École Supérieure de Guerre
- **"If I had thought about it, I wouldn't have done the experiment. The literature was full of examples that said you can't do this."**
  – Spencer Silver on the work that led to the unique adhesives for 3-M "Post-It" notepads
- **"Professor Goddard does not know the relation between action and reaction and the need to have something better than a vacuum against which to react. He seems to lack the basic knowledge ladled out daily in high schools."**
  – 1921 *New York Times* editorial about Robert Goddard's revolutionary rocket work
- **"Louis Pasteur's theory of germs is ridiculous fiction."**
  – Pierre Pachet, Professor of Physiology at Toulouse, 1872

Figure 15

Some Appropriate Quotations

communication security, which probably is the third oldest profession, and we know a lot from our computer security heritage. Additionally, we know a lot just from the course of human events: trying to figure out who's the bad guy and why does he want to do something to us. We just haven't focused it correctly. That's the challenge in focusing it correctly because that's when you push the boundaries of the knowledge quadrants down and to the left (figure 18). What do we know we don't know (left) and what do we not know we don't know (down)? That's got to be derived from an environmental analysis. What are the

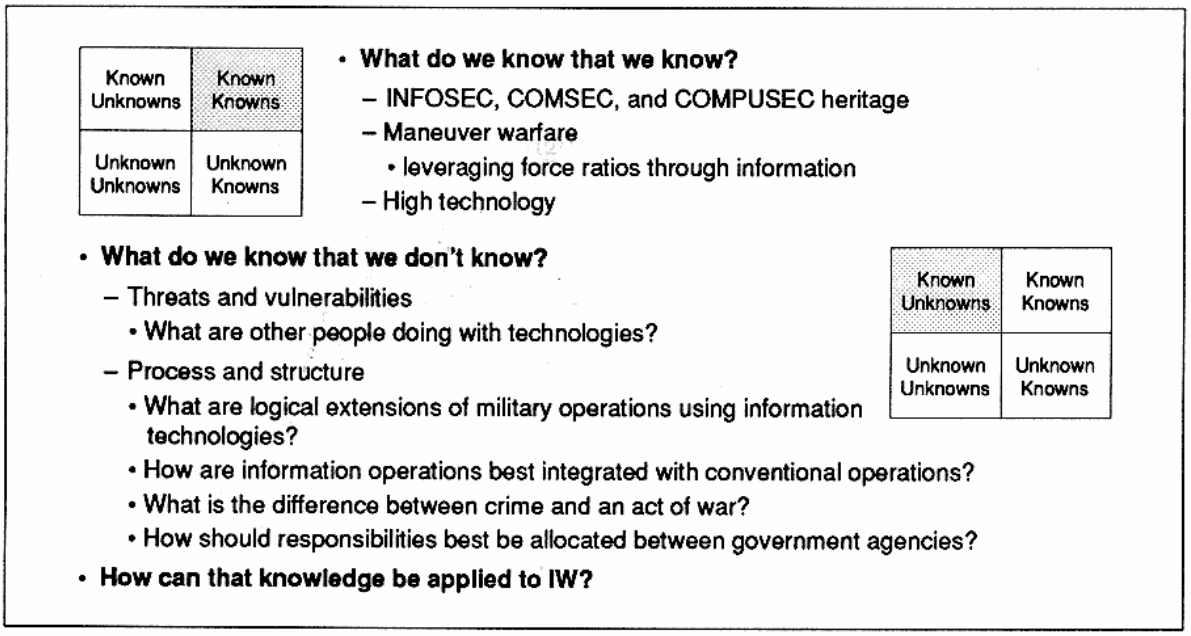

Figure 17

Knowns

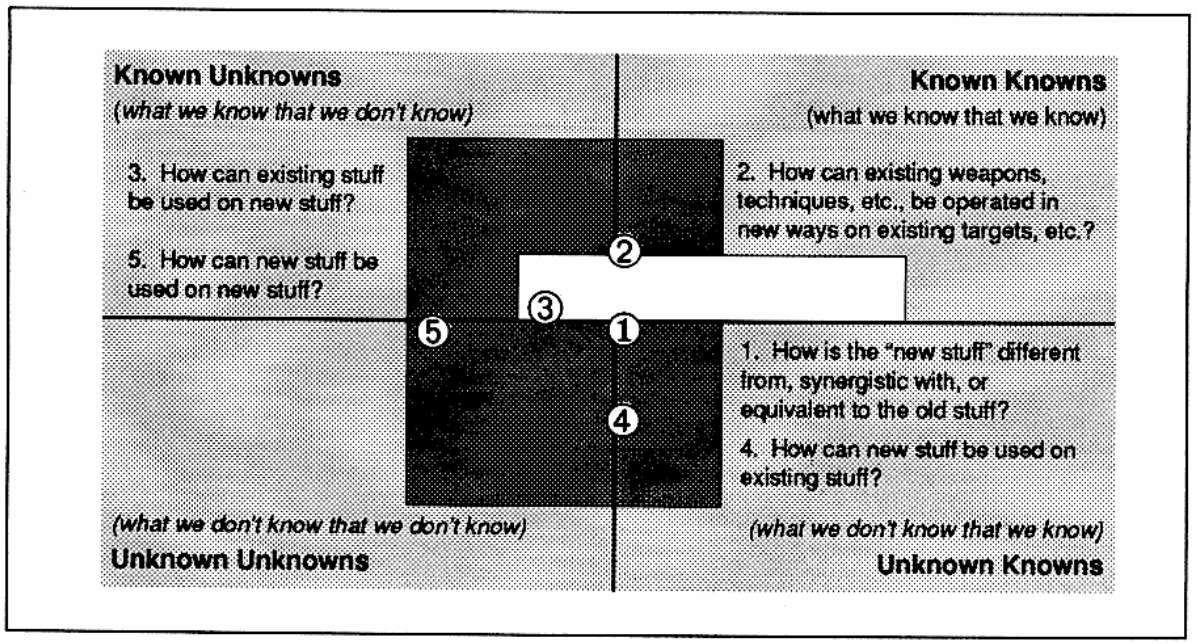

Figure 16

Where to Look

fundamental human needs? What is it that makes us human? What are the societal structures that we have created to support those qualities that make us human, the things we value—things like the military, things like the police department, things like governmental structures, things like education—and how are those things

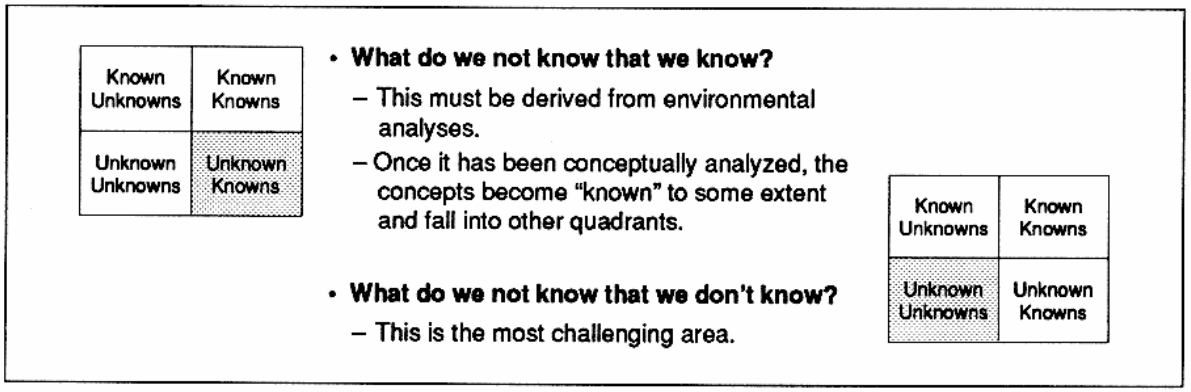

Figure 18

Unknowns

impacted by information technology? It's difficult to do that analysis because you have to throw away the instantiations that you are used to, and go right to the fundamental core of what it is that's important.

In the knowns category, the INFOSEC heritage (figure 19) probably gives us the best insight into information warfare in that it provides us with ideas on how computers can be sabotaged and, therefore, since computers are the fundamental technology underscoring information technologies, how information can be sabotaged. Communications security shows how information in transit can be sabotaged. Operations security, personnel security, and physical security can give us an understanding of how to provide a holistically secure environment, and how to crack that holistically.

Oettinger: Before you remove that, just several comments. On the previous slide (figure 18), on this matter of stretching the mind to foresee, and so on, some of you who are interested in this area might turn back to the 1995 proceedings and look at the discussion by Admiral Owens,* because that set of questions is fairly sharply focused on some discussions there. On this latest slide (figure 19), there's a wealth of material in the proceedings of the seminar for all the years, and there is, by now, a fairly large public literature that you can find in HOLLIS (Harvard Online Library Information System). So, these are two areas that are relatively easy to study.

Ryan: What I propose to do now is just to go through the INFOSEC heritage to show you some of the things that are possible, although not the entirety, because I don't know any more than you do about what the future is going to bring (figure 20).

Speaking of 13-year-old hackers, I have seven pages of weapon types that are appropriate to the information we mentioned: seven slides for it. My brother is probably quaking in his boots because I have too many words on this slide. It violates every rule of briefing "ology" that you can ever imagine. The fact of the matter is that there's a lot of stuff out there, and these things are fairly complex.

TEMPEST involves electromagnetic emanations from your computer screen. There's a new tool that can pick up those emanations from 1,000 yards off; that means 1,000 yards from where you're sitting somebody can be reading what you're writing on your computer screen. If you don't care, that's one thing. If you do care, if it happens to be a national secret, that's a whole other thing.

I won't even touch on computer viruses because everybody know what a virus is.

Covert channels are kind of interesting. There are covert storage channels and

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

- **Computer security research and profession**
  - identify ways in which computers and information processing tools can be compromised and how they should be securely designed.
- **Communications security tools and techniques**
  - provide understanding of the strengths and weaknesses of cryptography.
  - identify weaknesses inherent in electromagnetic media.
- **Operations security, personnel security, physical security**
  - provide supporting understanding on how to develop a holistic secure environment.

Figure 19

INFOSEC Heritage

- **TEMPEST**
  - TEMPEST is the study and control of unintentional electronic signals emitted from ADP equipment. TEMPEST weapons are those that exploit such electronic emissions. Examples include intercepting those emissions, perhaps to gain clock synchronization for other weapons, and jamming the targeted system on the emitted frequencies, perhaps to make a terminal screen unreadable.
- **Computer virus**
  - Probably the best known of these weapons, although not usually considered in that context, computer viruses are those programs that stealthily infect other programs, self-replicate and spread within a computer system or network. Typically small, they are difficult to detect, with some of the more recent versions having active anti-detection protection measures. Modern computer viruses may be encrypted, compressed, or polymorphic to reduce probability of detection.
- **Covert Channel**
  - This is a communication channel that allows information to be transferred in a way that the owners of the system did not intend. Variations include covert storage channels and covert timing channels. Use of a covert channel would be an interesting way to insert a virus into a computer system.
- **Worm**
  - Similar to viruses, worms are self-replicating but not parasitic (i.e., they don't attach to other programs). As demonstrated dramatically by the Internet worm of 1988, they can deny legitimate users access to systems by overwhelming those systems with their progeny. Worms illustrate attacks against availability, where other weapons may attack integrity of data or compromise confidentiality.

Figure 20

Weapons – 1

covert timing channels, and they're fairly complex in terms of defining them. Essentially, it is a way to convey information without actually storing that information. If anybody's interested in finding out anything further about it, I recommend the

NSA Rainbow series. They have a very nice discussion on that.

I guess I don't need to mention what a worm is here at Harvard.

Data manipulation is a fairly interesting weapon (figure 21). If you consider the content of a digital picture, what you see on the screen is a bunch of dots that have been put together. When you look at an increasingly high resolution picture, those dots that you can't physically see could actually be chock full of information, and they could be used for a variety of things. They could be used to convey information to your subconscious or to convey information to somebody else who knows to look for that on a microfiche or microchip.

Electromagnetic bombs are similar to the studies that were done in the nuclear arena on the effect of electromagnetic pulses on information processes. As chips and transistors get smaller and smaller and smaller, the effects of electromagnetic pulse get worse and worse and worse.

In regards to the flaw, I was once involved in a software development activity where the head programmer got up and said, "I have never designed a software program that I haven't put a back door in," and we went, "Aaaah!" He said the reason for that is that you're always going to have some problem. You execute the code, it's operating, and then you have a problem, so how do you get into it? That's why you've got the back door. That's probably one of the biggest security problems that exists.

Oettinger: Just a note so that you'll know what we're talking about. The *Orange Book* referred to in figure 21 is a publicly available publication of the National Security Agency on some of the rules for information security.

Ryan: It has a very nice set of definitions. It's DOD-STD-5200.28.

A logic bomb is a piece of code that is designed to execute when you hit a certain logic state, for example, when the stock market hits 28,000 or something like that (figure 22).

A logic torpedo is one that could be targeted specifically at something. I don't know that any of these exist, but it's an interesting concept.

RF (radio frequency) weapons are kind of interesting. You figure that computers process zeroes and ones and these are transmitted in pulses. What's to stop somebody from tightly aiming an RF beam at your computer to flip some of those bits? It's kind of an interesting concept.

- **Data Manipulation**
  - With increasing technological capability for manipulation of data come opportunities to use those capabilities for nefarious purposes. The composition and content of pictures as well as databases are vulnerable to advanced techniques of manipulation.
- **EMP Bombs**
  - The electromagnetic nature of computers and supporting peripherals makes them susceptible to specific weapons, such as electromagnetic pulse bombs. These weapons overwhelm a system with electromagnetic energy that can erase or badly damage stored data within memory, fuse circuits, and fry modems. EMP is a natural byproduct of nuclear detonations (NuDets), but may be deliberately produced by conventional explosions as well.
- **Flaw**
  - Defined by the *Orange Book* as an "error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed," the use of a flaw in infowar has infinite potential. The insertion of a flaw into a system could be done with other infowar weapons, such as the use of coherent RF weapons, over networks from remote sites, or could be designed in by an agent in place.

Figure 21

Weapons – 2

- **Logic Bomb**
  - This is a piece of code buried within a larger computer system that executes when a specific system state is realized. An example could be a program that checks for the presence of a piece of data within a file (say, an employee's name within a payroll list) and when the specified logic state is reached (the existence of the employee's name is false), the bomb "explodes" (the software program commands the memory of the entire system to be erased).
- **Logic Torpedo**
  - Weapons like viruses are essentially uncontrolled. A weapon that can be aimed at one or more specific systems and then released through cyberspace to hunt down its target would be very useful.
- **RF Weapons**
  - Just as the digital data that a computer uses is composed of ones and zeroes, so can a computer system be affected by the synchronous pulsing of electromagnetic energy at specified frequency ranges. Also known as bit flipping, the use of coherent RF weapons has a wide range of potential, from the random distortion of data to the remote insertion of directed energy viruses. A major criticism of the utility of RF weapons is that for them to be successful, they must be gentle, and that implies a physical proximity. That geographic proximity can be achieved in a multitude of ways; examples include the insertion of a transmitter into a computer by a repair technician or the introduction of modulation onto the power supply to the computer system.

Figure 22

Weapons – 3

A time bomb is just like a logic bomb except that it's set to go off at a certain time (figure 23).

A timing weapon is probably a worse problem than a lot of people realize. When you have communications, the ability to synchronize your timing becomes absolutely critical. If you screw up that timing, you screw up the communications. They can't shake hands.

I've already discussed the trap door.

Oettinger: In fact, one might argue that the clocks in the system are the most fundamental element, because everything else can be working just like a charm, but if the clocks are screwed up, you might as well just have scrambled eggs.

Ryan: Yes. And you certainly can't trust your data integrity.

The most famous Trojan Horse going around right now is the Word Concept Virus (figure 24). It's not a virus, it's a Trojan Horse.*

Then there are conventional weapons. I already mentioned how you could use a rifle to take out an information target. There's an extraordinary range of how you can use existing technology and conventional weapons against information targets to really screw things up.

Some of the more interesting weapons, getting out of the software arena, are agents in place who can put problems into systems: for example, on factory floors and stuff like that (figure 25). There's a new book out, and I still can't remember the name of the guy who wrote it, but it's based on the concept of having a virus

* The reason it is a Trojan Horse is that it is additional functionality hidden inside a legitimate function, rather than extraneous code attachhed to or overwritten on a file/executable. The counter-argument is that it attaches itself promiscuously, and therefore fits the definition of a virus rather than a Trojan Horse. Perhaps a more precise term would be Trojan Virus.

- **Time Bomb**
  - Very similar to the logic bomb, this type of software waits for a specific time to be realized and then executes.
- **Timing Weapon**
  - Also thought of as insidious clocks, these weapons affect the timing of internal clocks to throw off system sychronization.
- **Trap Door**
  - As defined by the *Orange Book,* a trap door is "a hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g. special "random" key sequence at a terminal)." Anyone who has ever programmed knows that despite best efforts, no program ever works correctly the first time (or even the first 10 times). Trap doors are common safety steps used to make sure that there is always a way in to fix bugs, no matter what the problem. The utility of a trap door to provide access for infowar purposes is self evident.

Figure 23

Weapons – 4

- **Trojan Horse**
  - As the image evoked by its name implies, a Trojan Horse is a computer program with an apparently or actually useful function that contains additional functions that sneakily do things that the user of the program would not necessarily execute willingly. For example, a spreadsheet program could contain additional logic to make surreptitious copies of all of the data files on a system. The user of the spreadsheet program would not be aware of those activities occurring while working with the legitimate functions of the program.
- **Conventional**
  - Conventional weapons such as rifles and bombs in the hands of armies and saboteurs can be remarkably effective in offensive infowar operations, not only in attacks against the physical infrastructure of the information dimension, but also in perception management and positioning operations.
    - physical attack against some element of the information dimension including stealing the hard drive from a computer system
    - forcing a user group off one communications link (such as fiber optic conduits) onto a more exploitable link (such as microwave radio) by bombing the fiber switching station
    - swaying public opinion by bombing an airliner and blaming it on an opponent group
    - modifying some elements of enemy databases to undermine the opponent's trust in his own systems
    - assassinating randomly chosen enemy programmers

Figure 24

Weapons – 5

input in the factory into a bunch of laser printers that reassemble themselves every time you hook them up to a network.

Probably the biggest example of non-cooperating weapons is the use of the media in Desert Storm, where we faked out

- **Agents in Place**
  - Agents in place in system development organizations, standards committees, and as network managers can be very useful in terms of understanding system vulnerabilities and planting (pre-positioning) weapons.
- **Noncooperating Weapons**
  - The weapon used for infowar purposes does not necessarily have to know that it is being used or understand the real results of its activities. This situation is common in espionage, where the use of false flag covers in recruiting can turn an otherwise unachievable objective into a success. Use of CNN and the other news media to manipulate perception of events in Desert Shield/Desert Storm is a prime example of the use of a noncooperating weapon.
- **Positioning**
  - The Madison Avenue advertising community has been using what they call "positioning" techniques for years to make people buy certain brands or products. These techniques are used to encourage or discourage certain behaviors. An example would be to highly publicize instances of computer systems locking up with no way to fix or diagnose the problem. Such scare tactics would encourage development programmers to hide trap doors in their work so that if something like that happened, all the work they put into the system would not be wasted.

Figure 25

Weapons – 6

the Iraqis by having the media report that we were going to go up the coast as opposed to through the desert. The media were pissed as hell, and they were definitely a noncooperating part of it.

We talked a little bit about positioning during lunch: about using Madison Avenue techniques. There is an entire subtle capability of positioning people's minds to want to do something, like to buy a Coke instead of a Pepsi, to vote Republican instead of Democrat, to vote for Buchanan instead of Dole. This is probably the hardest problem of all, and probably the one that the United States is the most susceptible to. On the bright side, the rest of the world is very susceptible to it, too, which is why we have McDonalds in Beijing.

Further, we have public relations, which is very similar to marketing, and stimuli (figure 26). Stimuli are an interesting issue for those of you who are actually in the military, because by giving somebody too much information, you cause them to freeze. There was recently a wargame—I mentioned this over lunch—where the commanders participating were given total battlefield knowledge. After a while they stopped acting before getting all the information because they were expecting information. If you condition your enemies to get significant information, either by training or by allowing them to intercept stuff, by cutting off that flow of information you can potentially just stop them cold. The results, of course, are some variation on denial, destruction, or exploitation (figure 27). There's an argument that says that destruction is the ultimate form of denial, but I think there is a middle ground that warrants a separate category.

So, how can you defend against this stuff (figure 28)? You have to know, first of all, what kinds of attacks are expected. You have to know what to defend against. You have to know where the attacks will be coming from, so you know where to position your defenses. You have to know how to detect that, in fact, an attack is under way, and this gets back to the 13-year-old hacker problem. You have to be able to deflect the attacks and then recover from them—reconstitute your information resources. This is pretty easy when you talk about a geospatial environment, but when you get into cyberspace, it becomes a little harder because it can be in multiple dimensions at the same time.

In that manner, it helps to know what the candidate targets might be and what

- **Public Relations**
  - The art of public relations is well understood in politics, marketing, and publicity as a way to get persons to think in favorable terms about the subject of the PR pitch. It could be extrapolated to infowar as part of the deterrence process to keep opponents thinking favorably about us or our interests, and/or to instill a perception that going against our national interests is tantamount to going against their own interests.
- **Stimuli**
  - The use of stimuli to overstress a target system can have desirable effects on that system without necessarily destroying it. For example, an intelligence system designed to produce situation reports automatically could be overloaded by supplying too many inputs (i.e., situations to report), thereby causing a reaction or degradation in the system. The reaction caused would be system specific, but could range from triggering the system's automatic data thinning algorithms, thereby causing the system to dump data, to slowing the system down dramatically as it tries to process all the data being received. In the latter case, the slowdown could result in the users receiving grossly time-late products, which could cause them to miss important data or ignore the data they did get.

Figure 26

Weapons – 7

- **Denial**
  - The manipulation of a target to prevent it from being used reliably by its primary users.
- **Destruction**
  - The physical destruction of a target so that it cannot be used. Examples of destruction techniques include inserting a virus that sends read/write commands to a disk head so often that the head fails, blowing up a switching center or a power station, delivering a strong electromagnetic pulse to a system to fry its circuits, or shooting a bullet through the tracking/pointing mechanisms for a satellite dish.
- **Exploitation**
  - The manipulation of a target to exploit it for some purpose. This can include use of the target as a conduit for other weapons, intelligence gathering, insertion of false or misleading information, or manipulation of the system to slow it down, create distrust, or degrade availability.

Figure 27

Results

attraction or nonattraction those targets have to potential opponents, so that you know where the attacks may come or what they may be funneled through (figure 29). For example, using a medical system to get to the command and control system would be a fairly attractive strategy, were it not for the fact that the Geneva Convention could be interpreted to say that that would be analogous to smuggling rifles in an ambulance. It's not that people haven't done it, but it's something that nice people don't do if they don't want it done to them.

So your targets certainly include things like autonomous sensor systems, since they are, in fact, very information intensive. The command and control infrastructure includes not only the military leadership, but

- **In order to defend successfully against attacks**
  - Must know what kinds of attacks can be expected
  - Must know where the attacks will be coming from
  - Must know how to
    - detect attacks
    - deflect attacks
    - defeat attacks

Figure 28

Defensive Actions

- **Autonomous Sensor Systems**
  - Exploited to send false data back to the controlling system
  - Used as conduits for other infoweapons such as viruses, logic torpedoes, and worms
- **C^2 Infrastructure**
  - Includes civilian and strategic leadership, the decision process, societal support structures such as the police, and other governmental entities like the Bureau of Land Management and the strategic oil reserves.
  - Attacking these targets can sow discord in an opponent's society, thereby fracturing the decision-making process or any consensus, deny an opponent the ability to marshal needed resources to rebuff an attack, or divert attention from other activities.
- **Communications Infrastructure**
  - Physical part of a communications infrastructure includes microwave antenna towers, switching stations, telephones, radios, computers, and modems. Nonphysical portions include the data, electrical systems, and management support systems.
- **Economy**
  - Vulnerable from a variety of aspects, including the control mechanisms (such as exchange rates, tariffs and price controls), the electronic version of money (meta-money), the financial support infrastructure (including money transfer systems and automated stock trading systems), and the management systems that monitor the economy. Less directly, the mechanisms controlling a country's debt could be exploited.

Figure 29

Candidate Targets – 1

also the civilian and strategic leadership and decision processes. For example, an interesting conceptual attack would be to screw up the Social Security mailing list. You'd have every recipient of Social Security calling their Congressman. That would shut down Washington for weeks while they got it straightened out.

The communications infrastructure is self evident. The economy is self evident. We don't have real money anymore. It's all information. It's consensual imagination.

I took a cultural research deviation coming here from the airport. I took the subway, and I was fascinated to see the little information kiosks giving the currency exchange rates. If there was ever any proof

that we're in an information age, that's it: when you go on public transportation and find out what the exchange rates are.

The industrial base relates to having agents in place in production lines, but it additionally relates to things like developing a concept of actually giving opponents technology in order to keep them from being in a position to attack us (figure 30). That can be considered an information warfare technique, although it could also be considered a good policy technique, for example, building a car factory in Tennessee to keep the American people buying Toyotas and Hondas. But when you start thinking about these things, it really makes you look at the events in the world in a very different light.

We've probably already talked enough about the information infrastructure. The power grid is pretty self-evident (figure 31). Everything runs on electricity. If you take out electricity, you take out everything—elevators, your refrigerator, traffic signals, your 911 system—everything.

Then there's public infrastructure. People laughed at me the first time I said that libraries were a target. There's a lot of interesting stuff in libraries, including Internet access. The state of Maryland is totally wired to the Internet. Now, when you go to your public library, you can get on the Web and go browsing all over the place. And those systems are tied into their card catalogs and their interlibrary loan practices, and all the digitized information.

Of course, there's public transit. The lines of communication are always classic military targets, but in the information dimension, they're even more so, since the society as a whole, and the military in general, depend on information to conduct every aspect of operations.

Next, of course, is the medical system (figure 32). I mentioned before about smuggling rifles in an ambulance. Medical support systems also are a matter of life and death, and this also involves interesting process implications in terms, again, of the 13-year-old hacker. If he goes in there and

- **Industrial Base**
  - Includes production lines, research and development efforts, and employment associated with the industrial base.
  - Keeping a country from fielding an advanced system by creating or inducing errors in the system's development cycle could not only keep the country from having that capability but also create self-doubt in its ability to handle advanced technologies, thereby keeping it from trying new or innovative things.
  - Placing agents into the production lines and R&D centers can provide the access to forward base infoweapons.
  - Providing employment by hosting industry on foreign soil can create predisposed favorable attitudes within that populace while providing access for propaganda and perception management activities.
- **Information Infrastructure**
  - Computers, networks, and media
  - Also includes overnight mail delivery companies, fax machines, telephone systems
- **Logistics**
  - Computerized backbone that identifies supply requirements, positions materials, tracks deliveries, and schedules resources. Attacks on that backbone can severely impact the ability of the dependent forces to deploy or maintain a deployment.

Figure 30

Targets – 2

- **Power Grid**
  - Physical support structures such as power stations and transformer nodes
  - Degrading control system reliability can lead to voluntary shutdown of systems, particularly if there is a perceived threat of physical harm (example: compromising the reliability of a nuclear power station control system).
  - Creating a power sink in the system that drains power out, creating brown- and blackouts.
  - Secondary effects on systems depending on the power grid for electricity, such as civilian infrastructure computer systems.
  - New York City blackout illustrates effect on public order.
- **Public Infrastructure**
  - Elements of the public infrastructure such as libraries, local databases (such as DMV), and tax records are lucrative targets for exploitation and data manipulation. Holding such elements hostage could be effective strategies in infowar.
- **Public Transit**
  - The classical lines of communication (LOC) are the sea, air and rail lines, all of which are computerized in modern societies. Cutting these lines dilutes or denies the opponent the ability to move mass quantities of anything—information (e.g., newspapers), people, food, medical supplies, or weapons. Additionally, there are physiological effects that result as side effects of creating holes in the supply system. Interfering with the control of these systems (for example, rail schedules) would create cascading chaos.

Figure 31

Targets – 3

- **Medical Support Systems**
  - Medical technology, such as laser surgery, anesthesia, and gamma ray imaging, is controlled by computerized systems (and dependent on electricity). In the drive to increase the productivity of the medical profession and to decrease the cost of medical services, an increasing percentage of patient support services are also being computerized, from billing to medicine dispensing to life support systems.
- **Smart Systems**
  - Microprocessor controlled products such as cars and planes, robotics, other expert systems, wired buildings, intelligent transportation systems, and network management systems (such as sniffers).
- **Training**
  - If the enemy fights as he trains, by subverting the training system one can degrade his ability to fight. Subversion is possible by subtly changing the rules of the game, by altering data, or by feeding false stimuli into the system (such as leaking one of our training manuals).

Figure 32

Targets – 4

screws up an automatic prescription system so that people die, how is that handled? I'm not sure we have a good understanding of that entire realm of problems.

Student: Excuse me. In medical systems, prescriptions have to be reviewed by at least two individuals, so even if a hacker were to generate bad prescriptions, there is a human judgment element. But more interesting is the development of telemedicine where there are great combinations of your X rays or electrocardiograms (EKGs), your prescription formats, being digitized, and they're being shipped back and forth between hospitals. There were people talking about attacks on telemedical systems where people can manipulate X rays to be somebody else's—to alter the digital picture of somebody's X ray and convey a different disease than the patient actually has.

Ryan: Or have them amputate the left leg instead of the right leg.

Student: Now they have EKG machines that can be wired not only to diagnose certain diseases, but also actually to transmit certain shocks. So, if you were able to insert a bug, theoretically you could kill somebody off by telling the machine to use 200 volts instead of 100 volts.

Ryan: Or there's that ultrasound machine in Florida, I think, that wound up frying a guy's shoulder. Yes, I think that illustrates that there's just no end to the dirty tricks that the human mind can think up.

Oettinger: But that raises a question that I hope you'll get to somewhere, if not at this point, later in the presentation. You've been very good about pointing out that some of these things have analogues in older technology. For example, messing around with transportation nodes is an age-old tactic. So it seems to be equally interesting, or important, to ask why certain things do *not* happen. If there's all that vulnerability, how come ain't nobody doing it? Like poisoning the water supply, for instance. There are many other vulnerable nodes in the infrastructure. I don't know whether you are addressing the levels of threat, because with the whole question you raised in figure 1 about breeding paranoia, how does one arrive at some reasonable gradation? This goes back also to another question you raised about what is strategic and what is hacker or disruptive, or an attack against somebody. If you screw up somebody's cardiogram or whatever, that's not exactly strategic. It may be rather deadly for the individual, but we lose more in traffic accidents. Are you going to sort that out?

Ryan: Yes. In trying to build a framework for what would be a reasonable understanding of what a strategic attack is, and what a tactical attack is, and what a nuisance attack is, and what a crime is, we started looking at the relationship between the ease of attack on a system and the impact on the system, just to understand that relationship. It seemed that to attack a single switch is probably pretty easy, but it's also low impact (figure 33). To attack all the switches would be very hard to do and very high impact, and there's some gradation in between (figure 34).

Student: But if some types of electronic attacks have cascading effects, it may be almost as easy to attack a single node. The AT&T failure on Martin Luther King Day in 1990 was the result of one update to their switching code cascading through the whole system, or much of the system. Getting a massive effect didn't really require that much more effort than attacking a single switch.

Oettinger: That's really a "glass half-empty, glass half-full" example. You can take that same incident and say: "Yup, but how many people are in this room felt the effects of that particular incident?"

Student: That's one incident.

Oettinger: You were saying that is an example of a cascading effect. So the cascading didn't go very far. There are going to be worse disruptions of the airlines today because of the snow than from that particular incident. Bite your tongue.

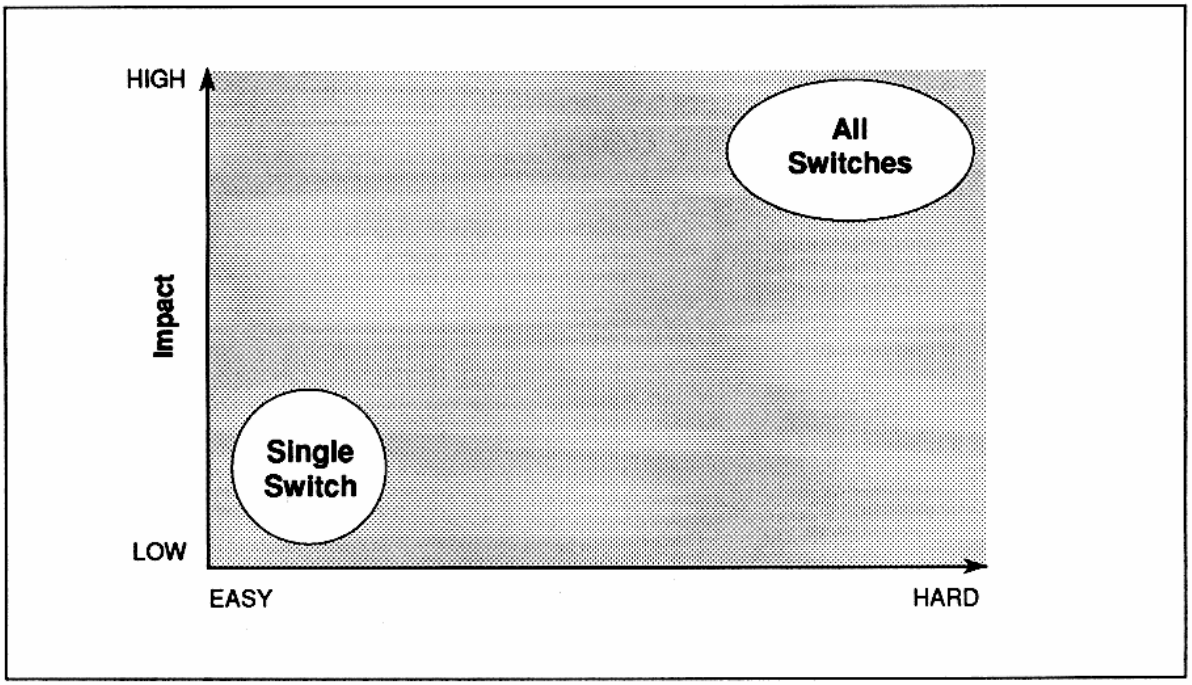

Figure 33
Effects Graph: Simple

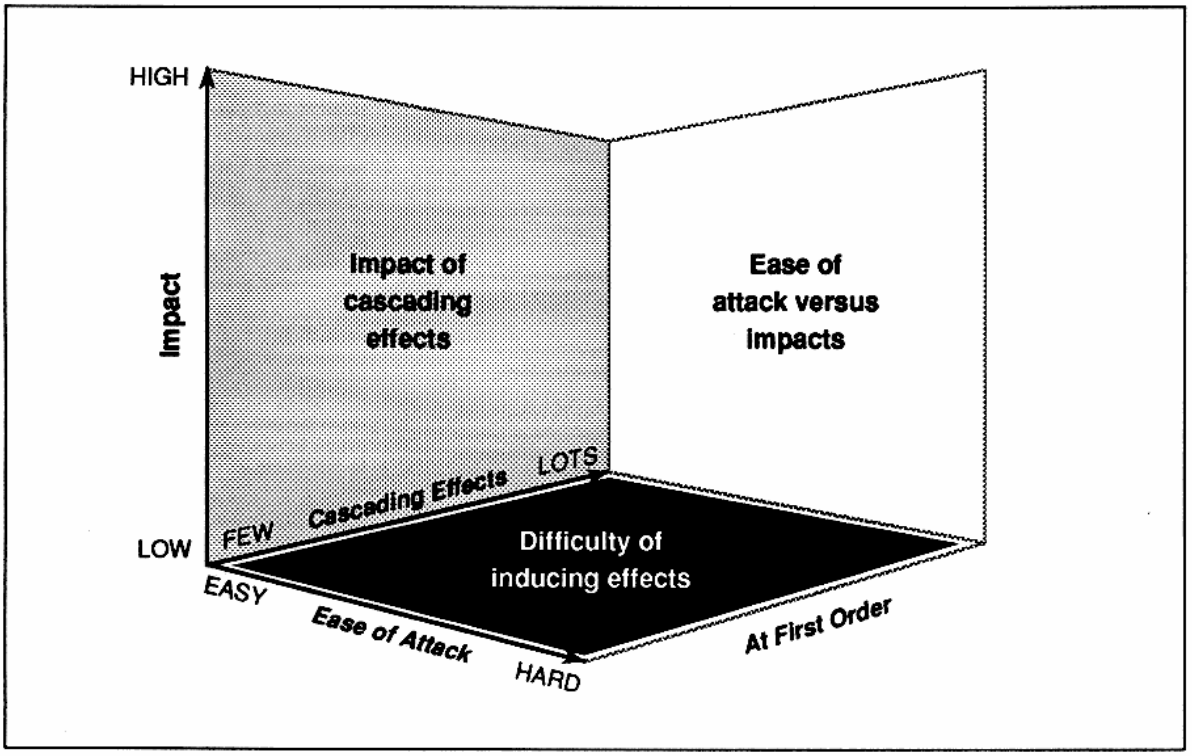

Figure 34
Effects Graph: Complex

Student: Luckily we haven't had multiple cascades at once. If somebody cascades the FAA at the same time ...

Oettinger: But you see, you're making an assumption there that I would hope Julie will speak to. Is it luck or is it intrinsic in the system? She has indicated that there are these possible attacks. Now, how susceptible are these systems or how vulnerable are we? I think that is another set of questions, and I hope you will address those as well.

Ryan: Yes, sort of. I don't have any answers; sorry about that. But that's a very important thing. The calculated effects of that particular shutdown were extraordinary: several millions of dollars worth of damage to the U.S. economy, and personal problems for a lot of people and stuff like that. On the other hand, Tony is absolutely right. Compared to the totality of the United States existence it was a blip. It was nothing. But in considering those kinds of things, you add another dimension to that graph, and if you were able to predict what the cascading effects were to be and to instigate those cascading effects, then you would have a very serious capability, and that would be a very serious threat. I didn't even try to draw anything on here, because I think it would be too hard.

Student: I think that's the counter to your point, Professor Oettinger: that the AT&T thing was not calculated. We've overcome some of these cascades because they're not designed to be part of a strategy or a structured attack. But if multiple events are synchronized, especially since this stuff can be timed to go off simultaneously—everything suddenly happens at 12 o'clock noon on April 1st—we can't prove what's going to happen.

Oettinger: You are absolutely right. Hypothetically that's true. I'm raising questions. I don't know the answers any more than Julie does, but I think it's important to have the questions right in order to put these things in perspective. Think about not Desert Storm, but Desert One—that helicopter raid on the Teheran embassy—which was an order of magnitude less complicated than some of the things you're talking about here. You're saying "synchronize," et cetera. That operation got terribly screwed up because of the difficulties in synchronizing and questions of operational security and one thing or another. You have to be very careful not to overlook threats, but on the other hand, when you start looking at them from the point of view of the attacker—how hard it is for me do something to the other guy—it doesn't make sense to say that it would be all that easy for the other guy to attack us. The complexity of getting at something as highly synchronized as you describe it should not be underrated. Now, I don't know where I net this out, but the beauty of the kinds of issues Julie is presenting is that at least she provides us with an effective way of framing those questions.

Student: In a lot of what you're saying, I see the fundamental question as being: What sort of threats should we take into account in deciding where our money should go in preventing them, and setting up defenses? Your response to my question before about the 13-year-old was, "We need to decide that issue because we need to decide what the policy response would be." But that's a completely separate question from how likely is it, or what would the impact be of an attack on an AT&T computer versus an attack on the Harvard University computer or whatever, and then, where should we put our money for building up the defenses against which attacks? I see these as two different questions, and maybe this is more on the lines of what defenses we choose to spend our money on.

Ryan: That's exactly right. I agree with you 100 percent, and if there is any message I wanted to convey today, it is exactly that message. Once you understand what the potentials are, once you understand what the possible targets are, what the kinds of weapons that can be used are, and what the methodologies are, then you start to understand what the complexities are of the impacts and the cascading effects.

By the way, cascading effects are not limited to the United States. For example,

consider the financial transaction network. You attack a bank, and boy, there are things all over the world that are going to be affected. That understanding gives you a clue as to what's likely and what's not likely. It is not likely that Germany will attack our banking system because they would be hosing themselves just as badly as they are hosing us.

Now, on the other hand, would it be likely for somebody like the IRA to attack our banking system? The answer is no, because they depend on our money just as much as we do. It's those kinds of understandings that direct you to reasonable and realistic defensive postures, policies, and processes.

Oettinger: There is a study that the Program published by Dan Knauf,* in which he makes some distinctions that are very germane to the point that Julie is making as to susceptibility to an attack, in the sense of are you likely to be affected. I'm susceptible to the common cold; we all are. Are we vulnerable to it? Well, to most of us the common cold is no big deal. If you are aged, if you have a heart condition, if you've just been operated on, then your vulnerability to the common cold's evolving into pneumonia becomes very, very high. Then, given some assessment of susceptibility and vulnerability, how likely is an attack? I may be able to control whether I go to a crowded place and expose myself to the common cold more or less. I can take measures to control the probability of an attack.

So, there are a number of dimensions that Julie is helping us conceptualize, and there are not many answers. The merit of what Julie is doing here is framing questions that are worth addressing in an area where, by and large, there's a lot of thrashing going on without the kind of structure for effective thinking that Julie's provided us.

* Daniel J. Knauf, *The Family Jewels: Corporate Policy on the Protection of Information Resources*. Cambridge, MA: Program on Information Resources Policy, Harvard University, June 1991.

Student: Large systems tend to be amazingly resilient. That's really the comment. There are Chicken Littles all over the place. Every time there is a new whatever, there's the Chicken Little. I know you know this. I like to frame this more as a question of means, ends, ways, and degrees of risk involved in this. Right now we haven't even laid this out where we're sure of all the means and the ends, much less talked about the ways and risks involved. I'm enjoying this, but we're still, right now, trying to understand the scope of what we're talking about. Every time I think through something, I keep coming back to the answer that large systems are amazingly resilient.

Student: They are resilient, but what I've tended to see is that people say there's no evidence. They either say we've got a huge problem or we've got no problem because they're resilient, but what Doctor Oettinger is getting to, I think, is that because of these frameworks, people need to start going into a little more depth in painting the picture than saying, "We are vulnerable here." "This is highly unlikely. No one could pull this type of thing off."

Student: That's the risk aspect I was talking about. Absolutely.

Oettinger: He is right. The history of this whole subject so far has been that you either stick your head in the sand and play ostrich or you're Chicken Little, and there's relatively little in between. This discussion, to me, is delightful in that it maybe helps frame how to populate the middle between the ostrich and the chicken.

Student: The only thing I'd throw out also is that right now we have more weapons than we have vulnerabilities.

Student: People would turn that dramatically on its head and say that because we're the most information-intense society, we're therefore the most vulnerable. It is a big leap from being intense users to being vulnerable, but it's a leap a lot of people make.

Student: Yes, unfortunately.

Student: One thing that I've found a little confusing, though, is the mixture of civilian and military applications of this model. The second thing is the mixture of technological problems with much more political problems, like the slide where on the one hand you had worms, viruses and all that, but on the same list you had use of the media (figures 20 through 26). I just see those as very different types of warfare, very different types of issues, that demand completely different responses and detection measures.

Ryan: I would ask you to examine closely the assumptions implicit in the statement you just made. In particular, let's just take the easy statement—the military and the civilian. There is an assumption there that you may not even be totally aware of: that the military and the civilian worlds are separate. Well, look at what the military is. It is a common framework for defense. It's the way we have instantiated our need to defend ourselves as a society, and it just happens to be instantiated as the military that we know today.

Student: I guess my comment was made sort of in response to this gentleman's statement about the resiliency and also the fact that we have a lot of weapons, because it seems like that's more toward the military side: maybe redundancy is built more into the system and there's also the deterrence factor of, "We can do it to them. If they do it to us, we'll do it back," and thus, no one will do anything because they're afraid of the response. I don't see that as being equally applicable to the civilian side. It seems that there isn't as much redundancy. There isn't any deterrence ...

Oettinger: I think you could argue that there's even more redundancy in the civilian system. I said I *could* argue that, but I'm not prepared to argue it. I don't have numbers. I don't have any map of it. I think one of the things this discussion is revealing is a certain profound ignorance about some of the critical factors that we're dealing with here, and I think that between Julie and me and some of the other folks around this table, the collective judgment is likely to be: ain't nobody else out there who has answers to this. That is, I think, a critical message to you guys, because as answers are needed, when you leave this classroom, it's going to be up to you.

Ryan: Yes, that's the message. You guys are going to be in the position to make these decisions.

Oettinger: This is not heavily plowed ground where there are lots of answers.

Ryan: Furthermore, there are some really heavy questions; for example, your statement that we have lots of weapons but maybe not lots of threats. We have lots of weapons in the conventional defensive arena, but we don't have lots of weapons in the information warfare area.

Student: I certainly don't want to take this off on a different track and take everybody's time here. I don't come down on the Chicken Little side of this, obviously, and Doctor Oettinger made the analogy to the Desert One sort of thing and the ability to do something. You know the old joke about, "Any graduate from our trade school down the road here* can build an atomic bomb." Well, not necessarily. There aren't atomic bombs floating all over the place. The same thing on this is that any hacker can attack an electronic system. I'm not a software engineer. I can't get into it, but just my experience of trying to coordinate things and mess with other people's systems makes me aware of the difficulty of actually doing this. It's easy to talk about it. It's much harder to do and bring to a closure. I'm here listening, too.

Ryan: No, I think you're absolutely right. It is incredibly difficult.

Student: You had the power grid up there. Everybody thinks taking down the Iraqi power grid was an easy thing to do. Absolutely not! It was massively difficult

* A reference to the Massachusetts Institute of Technology.

and it came back up repeatedly every time. It takes re-attacking it, as an example.

Ryan: Yes, that's absolutely right. The message that I would hope that you get is not only that one but, additionally, that the civilian infrastructure is, in fact, at risk, and not only from things like electronic intrusions, but also things like broadband TV transmission directly from the attacker to the consensual societal understanding. It is those kinds of really odd notions that warp the paradigm of what it is that we as a society are trying to protect in a communal structure. Everybody's stunned?

Oettinger: That one is not so far out. If you think of the effect of Nazi propaganda before and during World War II, you have a good antecedent for that particular kind of manipulation.

Student: But the problem is America will just turn to another channel.

Ryan: No they don't. They all watch *Roseanne*.

Student: No, they don't. I never watch TV.

Ryan: I don't either, actually ...

Student: There you go, see?

Ryan: But you and I are, by far, the minority. I find myself having to watch TV probably about once every couple of months so that I can talk to folks in the office and have a basis for relating to them, so they don't think I'm a real weirdo. That's American culture.

Oettinger: Yes, but there's an interesting by-play here because you all, including yourself, Julie, are confessing to being elitists who don't do what *hoi polloi* do, but there's this notion that *hoi polloi* now are always glued to their television sets. That is an illusion or a fact or factoid or something that the networks and television folks love to play up because it plays into their advertising rates. But if you go back to the Gulf War, and all this mention of CNN and so on, AT&T had put into Saudi Arabia lots of telephones that the GIs could use to call back home. I don't know of any study of the effect of direct communication between troops in the field and folks back home as either leverage or antidote to CNN. I have never seen a joint study of the CNN and the telephone effect. So, I haven't the vaguest idea, but the question is hardly ever asked. I'm the only one who seems to ask it.

Ryan: I don't think I've seen a study on that either. It would be particularly fascinating to see that kind of study juxtaposed against Somalia.

Oettinger: In what way? Amplify that.

Ryan: There's been a lot of talk that the only reason we went into Somalia to begin with was because of TV, and the reason we got out of Somalia was because of TV showing the guy getting dragged through the streets.

Oettinger: Those two cases would be fascinating to look at, but I am not aware of any civilian, military, government ,or private sector study of that kind of question.

Ryan: Does anybody need a thesis topic?

Student: I just don't see it being that easy for anyone to manipulate the American public, because Desert Storm was a unique example. Everyone tuned in to CNN just because I think it was unique, it was new, it was big. But in terms of anyone trying to pass a message along—even the Iraqis were broadcasting TV—unless it's really high quality, everyone is just going to change the channel. I don't think the attention span is long enough.

Oettinger: But if you look at the prior record of the seminar on the public press, I've heard people say around this table—and Julie mentioned it earlier—this reluctance to tolerate casualties is usually ascribed to the public media and the sight of body bags, et cetera, is a pervasive Western phenomenon. It's not just the United States, but also the French. I'm recounting what I think is the perceived wisdom.

Student: Can I jump in? I'm going to differ on something on the French. The French sent only volunteers to Bosnia because their draftees are in for 10 months, and they don't have them long enough to get them actually involved in units to do that. The French military exists for the greater glory of the French Republic and are used that way, whereas ours is different. Ours exists to defend the Constitution of the United States. They are totally different things. I didn't say that when you brought that up. That's one of those you just let slide. But, since you used that ...

Ryan: I think that it's fascinating you should say that, because my source for that data was the French ambassador in Washington, who stated it in such a manner as to convey the message that the reason they didn't send anybody except volunteers was because the French populace would not tolerate casualties.*

Oettinger: It's an interesting empirical question. My childhood was spent in French public schools. I can guarantee that you're absolutely right. When I was a kid, *la gloire de la France, mourir pour la patrie*, were still deeply embraced. What she's saying is that modern technology and the passing of Charles De Gaulle have eroded even this. When I was a kid we would sing the Chant du Départ, "*Mourir pour la patrie, c'est le sort le plus beau*"—dying for the Fatherland is the greatest. That was parodied as "*Mourir pour la patrie—mourir pour les jeunes filles*"—dying for the Fatherland, dying for the girls. So, even in those days, and in school, in the *lycée*, there was a certain irreverence about it. Perhaps after De Gaulle it has eroded. It's an important and interesting question.

Student: The ambassador said that. We don't have to believe it. I've got a processor up here, too, that works.

Ryan: Yes. That's the reason I brought up my source, because I find it fascinating.

Oettinger: I just want to nail down that this area we've been discussing for the last five minutes is one where there's a certain amount of dogma, which I think is totally baseless. By and large, these are unexamined statements whose truth, one way or the other, I'm damned if I know, and I suspect that most people who mouth them with great assertion, even certitude, don't know what the hell they're talking about. The main message to get out of this session, which Julie is doing marvelously, is that there are questions and here's a framework for addressing them. Most of the answers that are floating around there are, to put it politely, just crap.

Ryan: I just love talking with Tony. I learn something new every time. This is great.

Student: I find the discussion of public perceptions, and the role of the national security bureaucracy in responding to, or attempting to dictate, or having a role in what information is being sent to the public, problematic from a democratic perspective, in the sense that I'm not sure what the role should be for the government in actually taking an active role in shaping perceptions, especially the role of an unelected bureaucracy in shaping those perceptions. I'm not necessarily saying that there is no role, but I just see it as a completely separate issue from how concerned we should be about someone hacking their way into the Fed's computer system. I just see them as completely separate issues, requiring different methods of analysis.

Ryan: I find this fascinating that that statement—which I totally agree with, by the way—is coming from the same guy who at the beginning of this lecture said, "What's the matter with the Department of Defense taking care of the 13-year-old hacker?" That's the fundamental point here.

Student: My statement in that context had to do with who has the responsibility for protecting computer systems.

---

* Specifically in an interview conducted by Diane Rehm on FM 88.5 (date unknown)..

Ryan: Responsibility for protecting computer systems, which are information systems, which are perceptions.

Oettinger: Wait a minute. You don't know how smart you are. That debate in this democratic society has yet to be had. It is absolutely fundamental. You're asking the right question. She said she agrees with you. I agree with you.

Student: But I don't agree that it's going on. It's been resolved.

Oettinger: No, it has been broached, at most, in some arcane inner circles of the federal bureaucracy, in the dark, among special interests that do not reflect the full glory of the decision-making apparatus of a grassroots democracy. Sorry, I'm on a soapbox.

Student: I think you lost me.

Ryan: And with a very strong elitist flavor, too. "Joe Sixpack can't understand this, therefore we have to act in his best interest. Let's not even try to explain it to him. Let's just act. He won't care, anyway."

Oettinger: We don't mean to thwart you. We meant to applaud you. You're raising all the right questions.

Ryan: Yes, you are, absolutely. If nothing else happened but that you guys went home and talked to your families about this, I think that would be a step in the right direction.

Student: I don't think I necessarily agree with ...

Ryan: With what you said?

Student: I guess I appeared to contradict myself in my question about the 13-year-old and you said, "Because hacking into a computer creates information, which somehow affects perceptions." I don't accept that syllogism.

Ryan: No. What I was saying was that protecting computers is fungible to protecting information, and thus is fungible to protecting perceptions. What you've done in one fell swoop is given the Department of Defense the right to protect the American society against perception.

Student: I don't see that because I don't see how you can argue that.

Ryan: I'd like to engage our lawyer over here.

Oettinger: They're both lawyers. You've engaged them.

Student: I think that's true, because the hacker on the system is influencing perceptions, depending on what the hacker is doing, of course. When you're influencing perceptions that the DOD controls, then the Department of Defense is interfering with that process. I think there is some truth to that.

Student: It just seems to me that, at the level of national security issues, individual perceptions have always been subsumed within this larger context. Giving the individual a right to hack into a system, simply because that's apparently the popular notion of something to do when national security issues are at stake, apparently, the individual understands ...

Student: But when you do that, when the DOD has control over a 13-year-old hacker, that's analogous to having military intelligence officers on college campuses during Vietnam spying on American people to some extent.

Ryan: It would never happen.

Student: You should not do it. It's a violation of our law.

Oettinger: Unless the law happens to be the Alien and Sedition Act. There are precedents in American history for lurches in both the more authoritarian direction and the excessively libertarian direction. These

are serious issues at the heart of governments in a democratic society.

Student: These laws were written prior to the age of technology. Laws are slow to catch up. But I would still suspect that you'd run into legal problems if the Department of Defense has the authority to investigate local American citizens operating on computers. It's a dangerous precedent.

Ryan: The question is, do we, as a society, want to give our Department of Defense that power and privilege? And the historical stance has been, "No, we don't."

Student: I don't think they'd even ask for it.

Student: They framed the question differently. They don't want it.

Student: The Department of Defense has the responsibility for protecting against getting hacked into and, on detection of an attack, handing off to the Federal Bureau of Investigation to deal with it, which is kind of the procedure that exists right now.

Oettinger: The procedure is cloudier than that. There is on the record a 20-year-old debate over the assignment of responsibility for some of these issues to the National Security Agency, which is a national-level organization for which the Secretary of Defense is the executive agent, and the National Institute of Standards and Technology (NIST), which is an arm of the Department of Commerce, and an ineffective one. If you look at HR-145, which is now Public Law 100-235 (1988), that's the structure under which we're operating, which is very uneasy and, by and large, not even visible to most ordinary citizens. I wish I had thought of this earlier, because it would be a wonderful term paper topic: getting all the history of HR-145 and the balance as it exists. That's what I was referring to earlier as this occult warfare between NSA and NIST over this set of issues. Try to grab any number of people on the streets and say, "Have you heard about the warfare between NSA and NIST?" and see what they say! The issues that are being framed around this table are what that's all about.

Ryan: By the way, the Department of Defense, as a whole, probably would not want this responsibility. But there are elements of the Department of Defense that would just love to get their hands on this, and, in fact, are fighting hard for it. It means money, resources. And, by the way, they think it's their responsibility.

Student: Yes, it's a big thing.

Student: Who are those people?

Oettinger: It is not ruled out that maybe they should. To me, the question is entirely on the table.

Student: You're right. What we've run into right now is statutory problems for doing that. The Department of Defense, with various executive orders, is statutorily prohibited from doing a lot of the things we're talking about, which I know you know but which is not common knowledge.

Ryan: It's not common knowledge because it's fairly arcane and it has not, until now, become important for anybody to know about, because it hasn't impacted on our lives. Now it does.

As to your question as to who those people in the Department of Defense are, there are two primary agencies and some smaller ones. The two primary agencies are the Defense Information Systems Agency (DISA) and the National Security Agency, which, admittedly, is not a part of the Department of Defense, except that the Secretary of Defense has executive authority to run the NSA for the federal government. On the other hand, it's staffed almost wholly with people who are paid by the Department of Defense, and, in fact, it is an intelligence agency.

Oettinger: The Director of NSA has been historically, almost invariably, a military officer in uniform, as contrasted with the Director of CIA, who's always been statutorily a civilian. So these are significant

questions, as the question that Julie raises is rising in importance: the basis in law and democratic consensus of what the hell we are doing and why we are doing it. Are we doing it wrongly or rightly, and so on, requires far more debate and far wider debate than they've received so far.

Ryan: I'd like to answer an issue that you raised, and that is, not giving the Department of Defense the authority to prosecute a 13-year-old hacker does not mean that we've given the 13-year-old hacker the right to hack systems. It just means that there's a different procedure for handling it.

Student: That's correct. The civilian authorities, as you said earlier, handled that through the regular criminal courts of this country.

Student: When you started out your talk saying that the level of hacking has to be so severe before the Department of Defense even enters the picture, you have a built-in protection against small-time hackers like that, anyway. You said five nuclear weapons were the threshold for considering something a strategic attack.

Ryan: I said that there has to be a framework. It does not currently exist, and I want to make sure that you understand the distinction. That is the fundamental problem: the framework does not exist for either identifying an attack or understanding whether an attack is crime, nuisance, hacking, strategic, tactical, or whatever.

Oettinger: Let me underscore why that's an important question. The history of issues in this area and any other is riddled by questions of jurisdictional competence, and that tends to work to the detriment of what you're protecting because the odds are that things will fall into a hole and therefore nobody will feel responsible. So whenever you smell jurisdictional dispute, it's not just bureaucratic balderdash over budgets and rice bowls and so forth and so on. It has to do with the fact that things may be get mishandled or, worse yet, not get handled at all, because it's nobody's baby. That's a serious situation.

Ryan: Let's just skip straight to what I would postulate as a strategic attack. By the way, I don't think that hacking constitutes a strategic attack or even an organized attack. I think hacking is hacking. In order to make something happen that is of strategic importance to the United States as a national entity, I think that you need something a lot more structured than hacking. It's got to run the gamut of electronic intrusion through suborning personnel in the system and stuff like that.

Take, for example, the Citibank crime, where anywhere from $400,000 to $400 million has been estimated to have been lost. Citibank has admitted $400,000 has been lost. They said they recovered everything else. I believe it.

Oettinger: It's only money.

Ryan: It is. The way that worked was not that some smart hacker sitting in St. Petersburg, Russia, hacked the system. The way that worked was that smart hacker in St. Petersburg, Russia, had a bunch of his cousins working in Citibank in New York City who sent him the password file. This was not exactly what you would call hacking for hacking's sake. This was a very structured and very thought-through and very precise attack for a very purposeful reason.

Oettinger: There is another lesson in that about the cousins. I was working as a consultant for another bank in New York way back, and you'll see in a moment how far back. When questions of security came up and they developed an enormously complicated system of interlocks and one thing and another, restricted access to the computer room, et cetera, the punched cards and all the records (that begins to give you the date) were put out with the garbage.

Student: Not shredded either, I imagine.

Oettinger: Not shredded either. So, there are a lot of complications.

Student: Do you think you could spin us a scenario, for say, 30 seconds or so, which would illustrate some of this about

how interdepartmental rice bowls might be involved over a potential hacking attack?

Ryan: Sure. Let me pick a good example that actually occurred. Have you read *The Cuckoo's Egg*, by Cliff Stoll?*

Student: I've heard the book on tape.

Ryan: Then you are familiar with it. If you think about the government entities that were involved in that and the commercial entities that were involved, it gives you an idea of what exactly we're talking about here. First of all, Stoll went to his local police department, and they couldn't help him. Then he went to his local FBI, and they sort of blew him off. Then he went to his good buddy in the local AT&T office and managed to get some traces going, and he wound up operating not only with the FBI, but also with the Air Force Intelligence Agency—it was then Electronic Security Command—down at Kelly Air Force Base in Texas, and the National Security Agency and the Defense Intelligence System Agency, and ... who else got involved?

Student: The Germans.

Ryan: Right. The Bundespost. I always forget that because "Post" to my mind is letters, and I keep forgetting they run the phone system.

Oettinger: They did. Now, it is Bundespost und Deutsche Telekom. It is also separated.

Student: That one was easier to prosecute because it came from Germany, and we had agreements with Germany and they went after them.

Ryan: But it wasn't easy to prosecute at all. It took an incredible effort on Cliff Stoll's part to force the processes actually to work and continue working and to prosecute them. Everybody just wanted to ignore the problem, and it basically came down to that it wasn't anybody's responsibility and it crossed jurisdictional lines.

Oettinger: By the way, for the period in which that occurred, which was a decade or more ago now, that is not so bad. By and large, it's a good example of how things start. When you have a new phenomenon you wouldn't expect there to be structures. So that, in and of itself, is not a bad sign.

Going back to what you said earlier about there being no law, of course there's no law. The law catches up. Here is my favorite statement by Justice Holmes about why the law is always behind the times: "It cannot be helped, it is as it should be, that the law is behind the times. ... As law embodies beliefs that have triumphed in the battle of ideas and then have translated themselves into action, while there still is doubt, while opposite convictions still keep a battle front against each other, the time for law has not come; the notion destined to prevail is not yet entitled to the field."*

You're looking at a very fundamental process. When you have new things happening, there are no preexisting structures. It takes time for the new structures to evolve, and you don't want them to come online overnight because the odds are that then they will address the wrong problem. This is why, I think, Julie and I are putting such stress here on the mish-mash of democratic processes to address these questions. They now are before us. It's no longer as it was when Stoll made himself a sort of one-man vigilante, which was perfectly reasonable at the time. There wasn't anybody looking.

Ryan: By the way, what Tony said about the law catching up with changes is a good thing. Integrating any technology into existing processes has to catch up, too, as the technology matures, which is one of the problems that I'm seeing right now in the military's adopting a concept of information warfare. I have to tell you, I do not work in

---

* Clifford Stoll, *The Cuckoo's Egg: Inside the World of Computer Espionage*. New York: Doubleday, 1989. The book describes how German hackers broke into presumably secure computer systems using gateways into data networks.

* Oliver Wendell Holmes, *Collected Legal Papers*. New York: Harcourt, Brace and Company, 1921.

the military. I do not work in information warfare. I do something totally different: I do management consulting. I just sort of watch this as a hobby. But it seems to me that there's a round peg in a square hole problem that's going on right now. There's trying to be a forcible fit of the concepts of information warfare into existing processes, into existing budgets, and into existing mission areas, and probably for no other reason than to protect those mission areas on budgets and stuff like that. We're probably going to see some dramatic changes as those things fall out because it will become glaringly obvious that it's the wrong thing to do.

What I've postulated here is something that I'm throwing out on the table for debate (figure 35). It is a definition that can be used as a framework for understanding what a strategic attack might be. The first thing is that it has to embody an intention (it can't be accidental) by an adversary to inflict overwhelming damage with the desired goal of breaking the system. By the way, I've added the caveat "over time" to incorporate the concept of cascading effects.

What this requires, I postulate and open for debate, is the ability purposely to target entities while coordinating the time and the location of the attacks, and inflicting specific levels of damage with some degree of probability. You're not always going to hit the target, but you've got some degree of understanding of what your probabilities are of hitting it. I postulate further that this requires significant intelligence capability to understand exactly what parts of the information structures, the decision processes, and all the other things that go along with that, must be attacked and must be impacted in order to have your desired effect of break. It also requires a means to deliver that attack. And I postulate that the scale of a strategic attack is such that it would be difficult to conduct it covertly. Now, who would like to comment?

Student: I don't understand what the last line (figure 35) means. Does that mean that the actual conduct of the attack is covert? Does that mean the effect of it is covert, so that it covers the tracks of the ones who committed the crime?

Ryan: Spoken like a true lawyer. What I intended to convey by this line was that it would be 99 percent impossible for the perpetrator of the attack to go undetected.

Student: What do you mean?

Oettinger: Before or after the fact?

Ryan: That's a good question. I would say after; maybe during.

Oettinger: That's not so bad, is it?

Ryan: No, it's not too bad.

- **How can a strategic attack be defined?**
  1. One that embodies an intention by an adversary to inflict overwhelming damage with a desired goal of *60 to 100% loss of capability over time.*
  2. This requires the ability to puposefully target entities while coordinating time and location of attacks and inflicting specific levels of damage.
  3. It additionally requires significant intelligence capability, to include comprehensive understanding of the target functionalities and processes, the reliances placed on individual targets, and cascading effects.
  4. It also requires the ability to deliver the means of attack.
  5. The scale of a strategic attack is such that it would be difficult to conduct covertly.

Figure 35

Strategic Attacks

Student: Though in terms of warning, in an intelligence sense, that's an important distinction—before or after—because if you can do bullet 3 (figure 35) covertly, that's relevant. The other comment I would make goes back to earlier in the discussion: it's the presence of bullets 2 through 4 that may be the answer to the question, "Why not, or not yet, anyway?" Maybe it's because orchestrating bullets 2 through 4 takes time and effort beyond the capability of the average attack, although money (and attention span) may be limiting factors.

Ryan: I just don't think that it's possible to do the intelligence gathering and analysis on $10 a day, even for a tactical attack (figure 36).

Student: Not yet. As this is an asymmetric strategy for a possible opponent of the United States, the relative expense involved in those compared with trying to compete with the United States in the battlefield could be considered to be very low.

Ryan: Yes, and by the way, this highlights something that goes to your question of whether it's detectable or not. If you have adopted this kind of definition, it gives you a way of detecting potential attacks, and that is looking for the activities that support such an attack, such as the intelligence collection activity.

Oettinger: Let me muddy the waters just a little bit lest you think even at this stage that this is simple. Paul Capasso's predecessor, Rick Jensen, has finished a paper* that, if some of you are interested and want to get some guidance on how to think about this, makes analogies between this and the strategic bombing in World War II, for which somewhat similar claims were made. We are now 50 years past those events, and the books are not closed on the question of effectiveness or ineffectiveness. But it is for analytical purposes not a bad set of precedents to look at because it helps flesh out some of the questions raised here.

Student: Also, when you say 60 to 100 percent loss of capability over time ... 60 to 100 percent of what?

Student: What does that mean?

Ryan: That is a brilliant question, because that is the crux of what this is all about. It depends on the intention ... I had a slide, but I didn't bring it, and now I'm kicking myself for not bringing it. Let me see if I can draw it on the board (figure 37). You've got some functional entities like the FTN. You've got command and control systems. You've got the PSN, et cetera—a bunch of functional systems. You want to do a strategic attack? Well, what if you postulate that for a strategic attack, you've got to do *that* 50 percent, and you've got to do *this* 100 percent, and you've got to do *this* 75 percent, on down the line, so that the total adds up to 60 to 100 percent loss of functionality on a U.S. national level. That's a framework for discussing what it is. I purposely didn't specify what the target space would be because I think the target space depends on what the desired effect is.

Oettinger: But, you see, the hairiness of this, if I may borrow a bit from Jensen's analysis, is that one of the beliefs about strategic bombing in World War II was that by knocking off the German ball-bearing factories you would cripple the German war effort. By one measure, which would amount, as Julie said, to taking one of these out, it was incredibly successful. Production was knocked to damn near zero at Schweinfurt. Now, two things happened. Number one was, as she pointed out earlier with respect to some other things, it got resuscitated, even in Schweinfurt, more rapidly than anybody thought it would. Second, everybody had forgotten about Sweden, and it's not a long way from Stockholm to Berlin, so the ball-bearings came from Sweden. So the question of what that universe is, where the 100 percent is measured from, somebody got wrong.

---

* Richard M. Jensen, *Information War Power: Lessons from Air Power* [research draft]. Cambridge, MA: Program on Information Resources Policy, Harvard University, April 1996.

- **How can a tactical attack be defined?**
  1. One that embodies an intention by an adversary to inflict specific damage on a target that could result in the total loss of capability to the set of targets attacked, but that results in *10 to 59% loss of functionality* to the functional entity or entities supported by the target(s).
  2. This requires the ability to purposefully target entities while coordinating time and location of attacks and inflicting specific levels of damage.
  3. It additionally requires significant intelligence capability, to include comprehensive understanding of the target functionalities and processes, the reliances placed on individual targets, and cascading effects.
  4. It also requires the ability to deliver the means of attack.
  5. The scale of a tactical attack is such that it would be possible to conduct covertly.

Figure 36

Tactical Attack – 1

○ *Desirable*
⊘ *Essential*
● *Mandatory*

	PSN	ATMN	FTN	E-Money	MedNets	GCCS	TAC 3	Corp Nets	WX	Cars	Petro/Gas Trans	Credit	Logistics	SCADA	Process Controls	Interfaces	Transportation	ATC	IVHS	SLOC	Ports
Strategic Attack	○	⊘				●	●		⊘	⊘	●		●		○		●		⊘		⊘
Tactical Attack																					
Stealth Attack																					
Espionage Attack																					
Felonius Attack	⊘	⊘	⊘	⊘	⊘			⊘			⊘	⊘	⊘		⊘						⊘
Misc. Crime	○	○		○								○	○								
Crusader Attack	●		●								●			●							

Figure 37

Candidate Matrix

Student: But the point of what the 100 percent is, relative to the objective, is different too, because we were then engaged in a struggle for national survival with Germany. If somebody is simply trying to deter us from doing something we were at the margin of wanting to do anyway, the level of damage they have to achieve may

be considerably lower to deter us than to come in and try to undermine our national survival.

Ryan: A good point, yes.

Student: So what would you call an attack on just those three—the FTN, C^2 systems, and the PSN—as opposed to the rest of the functional systems?

Ryan: Let's see. At the levels that I've indicated?* Probably a tactical attack.

Student: Let's say it was New York City and the World Trade Center, for instance, and you said, "I don't need to blow up the World Trade Center, but I can do an information attack on the FTN switch, the PSN switch for New York, and maybe blow up some of the power grids, and make the physical attempt that way." Would you consider that a strategic attack, if his objective was to disrupt the United States? Because I think by taking out New York you would ...

Ryan: No, because I think that we proved with the great Northeast Power Blackout [in 1965] that you could take out New York and not materially affect the nation's functioning.

Oettinger: Nobody missed it, at least for the short time it was gone!

Student: The question is becoming "What is strategic?" Strategic, in that paradigm, is this issue of survival, but it may be strategic in terms of whether it causes enough psychological damage to the United States so we would not want that to happen again and we don't intervene in some country we would rather not intervene in anyway.

Ryan: That's always a good question: the political debate that goes on when you're gung-ho for going in and blowing somebody up versus when you'd really rather not. People redefine things very quickly.

Oettinger: I have a marvelous paper on record, done by Paul's predecessor umpteen times removed, Sid A'Hearn,* in reference to the New York power grid. The way that the National Command Authorities, as we now call them, found out about this was that the President's science advisor, who at the time was Don Hornig, had a daughter here at Radcliffe, who was watching television and saw things sort of black out. She called up her father at the White House and asked, "What the hell is going on? Is there a nuclear attack?" And her father said, "What? There's nothing that's happened in Washington." But, being a good guy, he got on the phone and tried to find out a thing or two, so that by the time Secretary McNamara called him and asked, "What the hell is going on, Don?" Don had the beginnings of an answer. So McNamara was ready when Lyndon Johnson, who was at that time cruising the ranch, heard on his network radio that New York had blacked out and called him up. McNamara was able to say, "What we have found is yea or yea." The alerting trigger was somebody's daughter here at Radcliffe. The details are in Sid's paper.

Now, aside from being kind of a funny yarn, it says something about the robustness and redundancy of systems. This was not planned as part of the national scheme for alert against nuclear attack, and yet the National Command Authorities got alerted. So, again, is the glass half full or half empty? Look at the details.

Ryan: I'd like to point out something else about this schema** that I've thrown out for debate, and that is that when you adopt this sort of schema, it gives you a very nice framework for understanding what you've

* There is not an exact match between figure 37 and what was drawn.

* Francis W. A'Hearn, *An Interview with Donald F. Hornig, June 30, 1983: The Northeast Power Failure and Lyndon B. Johnson*, Cambridge, MA: Program on Information Resources Policy, Harvard University, October 1983.

** A reference to figures 35, 36, 37, and 38, collectively.

got to protect and what you don't have to protect. For example, if you adopt a schema that says that to do a strategic attack, you don't need to touch the financial transaction network, maybe you want to give the FTN a little less protection than you want to give the PSN. Comments? I've lost everybody.

Student: I guess the problem is that these are commercially owned, and it depends on where you sit and who is hollering the most.

Ryan: That's kind of interesting, because 95 percent of DOD traffic goes over the public switched network. Doesn't that make you feel good, especially with Milstar under attack budget-wise? One of the smartest guys whom I've heard said that Milstar is nothing more than a protected order wire, so that when everything else is down, you can still get an order back. That's a fair impression ...

Student: Nah.

Ryan: If you take it down to a fundamental capability, you have something that is so robust and so protected that when everything else has evaporated, you can still get an order back.

Here is the other half (figure 38). Having defined a strategic attack and a tactical attack, what's a threat?

Student: I was just wondering: even if you accept that model of combining every possible node (figure 37) ...

Ryan: ... which you don't have to do.

Student: Let's say that we do. Then how do you decide between the different parts of that spectrum to protect? You said there's a 75 percent attack against one, and the other one is 100 percent, and another is 50, so it sort of gives us the sense of how much we need to protect each one. But then, how do we assess the relative importance of each one?

Ryan: It's a resource management problem, a risk management problem. Some things are inherently more robust than others. In doing the systems analysis of those things, certain things are going to show up on the knee of the curve as being high-payoff things to do, like making sure everybody who has a password changes it monthly. That's a really high-payoff thing to do, and it's low cost too, by the way. But it requires a buy-in by the people who are using the system so that they actually do it. So there are trade-offs. You obviously know what I'm talking about.

Student: If we're able to have this discussion on the most fundamental level of what we're doing, do we have the deterrent capability? It's scary to think that we're having these sorts of talks, and I just wonder if we are cultivating in the military or in some diverse DOD departments the ability to counterstrike and that sort of thing.

Ryan: That's a very interesting question. The history of information security has been within the Department of Defense for a variety of reasons too numerous to go through. The intellectual capital resides within the Department of Defense. Are they capitalizing on that intellectual capital to build the offensive capabilities to retaliate in kind? I don't know. Do we have the capability to nuke the heck out of somebody who does this stuff? Yes, we do. There is no law that says you've got to retaliate in kind.

Student: Sure, we have conventional capabilities, but the question of who did what is unsolvable. They don't do us much good if we can't figure out who the attacker was.

Ryan: Yes, there is an interesting concept of a national I&W center that's being postulated, and that is having something, probably at the Vice President's level because that's where the two different chains come up (I heard that; that's a groan), actually keep an eye on the information structures and find out if they are whole or not. Of course, that raises a bunch of other questions: who is going to staff it and where are the budgets going to come from, and how do you detect attacks anyway? Those are questions that are still to be resolved.

- **Organized Threat**
  - The ability to attack WHERE you want to, WHEN you want to, and ACHIEVE desired results.
- **Nuisance Threat**
  - The ability to attack where you CAN, when you CAN, and achieve whatever you CAN.
- **Crusaders**
  - The group of entities which are motivated by philosophy, including terrorists, Luddites, and "the man who knows he is right." The ability to launch strategic attacks successfully would be assumed to be limited by their ability to gather and analyze comprehensive intelligence to support such an attack, as well as coordinate and launch comprehensive attacks. On the other hand, the effects of fratricide and cascading actions could be of less concern to the crusader.
- **Crime**
  - Primarily concerned with exploiting systems or escaping detection; may result in losses that will be limited in relative scope.

Figure 38

Tactical Attack – 2

Oettinger: Let me ask another complicated question on this. It comes out of Cold War things, but has its concreteness and its analogues here. It has to do with how real the threat is. One of the things that emerged out of the Cold War command and control studies is the question of: let's say that there's an accident in the Soviet Union and the United States sort of begins the attack and everybody realizes, "Hell's bells, there's a mistake! How do we stop it?" So the question of war-terminating capabilities became a crucial one.* It turns out that war-terminating capabilities and war-fighting capabilities are very much the same. So you run into all these questions of mutual trust and all that. But an interesting element of it is that if you believe in some measure of rationality, as opposed to being suicide prone, then it turns out that in fact there's a high premium on maintaining the stuff, even though it is usable in an attack, as the only way you might correct the mistake. Therefore, you begin to have a joint interest on the part of potential antagonists in maintaining the safety of certain things. It isn't completely nutty. In World War I and World War II, the postal systems, by and large, continued to operate. Now, you say, "Okay, let's not be mesmerized by Cold War stuff in the new blah, blah, blah. This may not work against terrorist or intermediate range things." But, again, it's a range of considerations. So the question of why would one not attack is as important a question as why one would attack. The Cold War example of the warfighting and war-terminating capabilities being essentially the same is just one concrete example of why that isn't a completely abstract, nonsensical question.

Ryan: The symbiosis that refers to is particularly relevant to the discussion of information systems because they are increasingly intertwined. This goes back to my comment that a nation would probably not attack our financial transaction networks because it would be a really stupid thing for them to do.

Oettinger: Even Khadafy might not, because the odds are that he's got his money stashed away in New York and Switzerland, and the two are interconnected.

Ryan: So that allows you to characterize the threats in different ways, like organized threats or sane threats versus unorganized threats versus crusaders or Luddites versus crime. And that, again, gives you additional

* Richard Martin, *Stopping the Unthinkable: C3I Dimensions of Terminating a "Limited" Nuclear War*. Cambridge, MA: Program on Information Resources Policy, Harvard University, April 1982.

insight as to where the potential problems are going to come from, and what the potential problems are.

Student: With reference to your previous slides (figures 35, 36, and 37), where you're trying to differentiate strategic from tactical using a percentages marker, how is this differentiation useful in developing a defense? It goes to the heart of what you said earlier—one nuclear bomb is bad. If it's a 10 percent degradation of my capability, then that's bad, but not so bad versus 100. Obviously there are scales, but would you build your defenses any differently to guard against 100 percent attack versus a 10 percent attack?

Ryan: Yes, I think that if you look at the history of military operations, the defenses against a strategic attack and tactical attack are very different. As a matter of fact, you may not defend against tactical attacks at all, depending on what you hope to achieve.

Oettinger: Let me give you an example from the civilian world, because this is again one of the things that complicates matters. There are several reasons why the civilian part of the economy is sort of reluctant to get into this. Regarding the attack on Citicorp, I made the comment halfway facetiously that it's only money. Think about what the civilian sector does *not* defend against. Your supermarket does not defend fanatically against pilferage because it's cheaper to tolerate a certain rate of pilferage than it is to lose customers by having excessive security in the store. Banks likewise—that's why there's relevance to her example of Citicorp; it's only money. So banks will adopt certain measures, but they won't go beyond that. It costs too much. An insurance premium is higher than the probability of loss. So there is a very important element, in a practical sense, between judging what is tactical—namely, I can sort of ensure against it, it's no big deal—versus something that is strategic, where I'm dead! I take a very different attitude, obviously, if I think nationally as well. If you think about the tactical stuff ...

Student: That's premised on knowing what the uncertainty is. If you have a very important, highly leveraged database where you might not know what could hit it to take it out ...

Oettinger: You have an unk-unk.

Student: ... your degree of uncertainty would drive how heavily you defend it. Supermarkets kind of know where the pilferage is coming from, but with a complex information system, with all the different weapons, you have a high degree of uncertainty on how that attack might come.

Oettinger: But the attackers do too. You've got to think of both sides of this. The important thing is to think both attack and defense, because unless you look at it both ways—and that, by the way, is another element of organization—you're in trouble, for very good reasons. Remember, one of the things I did at the beginning of this semester that drove you crazy was pose this notion of being a kid at a lemonade stand making decisions versus large organizations. It's easy in the lemonade stand to think of attack and defense as being the same. But when you have a bureaucracy, where the attackers and the defenders are in different bureaucracies, it sometimes gets to be very hard to put the two types of thinking together to address a problem. So this is really a poignant question.

Student: Could I ask a theoretical question on some of the theory of the course, in the sense of the role of the unk-unks? It seems like an unk-unk is sort of the equivalent of a strategic nuclear attack on somebody's argument. Then you can always say, "Ah, but you didn't consider the unk-unks." This problem seems very vulnerable to that sort of response in the sense that you could say, "The financial network is really not that vulnerable because most nations have a stake in it." But then the response could be "unk-unks." Who knows what terrorists are out there?

Oettinger: That argument is made every day by folks who want higher budgets. It may even be right.

Ryan: Yes, who knows?

Student: Where you were talking about the different possible threats (figure 38), I have the same sort of question: to some extent, why does it matter? Basically, in terms of defending yourself, for instance, the President has his Secret Service agents, and I'm sure there is not a separate corps to protect against civilian shooters and then a separate one protecting against military shooters. I'm sure that the threat is the threat is the threat, so ...

Ryan: Actually there are two. The ones that you see running alongside the limo and stuff like that are the criminal part. That's the part that's protecting him from crimes and terrorists. The United States military is the one that protects him against military shooters. The answer to your question (we've got 20 seconds here, so I'm going to answer quickly) is that by characterizing it, you give yourself a framework for responding, even if it's totally conceptual.

Oettinger: Before I thank Julie, I want to alert you to a potential problem. You may have noticed me bobbing out with my instrument here that I finally learned how to operate. I was gathering some intelligence. Julie, here is the situation. My 6:00 p.m. plane was canceled, and the airline gave me a reservation on the 8:00 p.m., which has now also been canceled, so I don't have an airplane. Now, the same airline is asserting that your 6:15 to Baltimore is running.

Ryan: I know what the problem is. It's National Airport.

Oettinger: It may be National, so maybe I should go with you to Baltimore. The alternative is the train. My strategy is clear. I think I'll go to the train station. Amtrak says that the trains are running 10 minutes late, but that's as of now, and who knows what will happen by 9:00 p.m. The other piece of intelligence is that the airport was closed for snow clearing until 4:00 p.m., so it may be reopening now, but it is also the time at which the storm is about to intensify. I've called the weather service.

Anyway, I want to thank Julie for an outstanding presentation.

[Added in editing: I also want to thank her for her riding home all night into the blizzard on a train, when I had chickened out and canceled my trip.

Added by speaker: ... which turned out to be the intelligent choice. Thanks for making the train reservation; it was actually quite stunning rolling into New York City at 0dark:30 and seeing the skyline from the perspective of the train.]

INCSEMINARS1996

ISBN-1-879716-39-9