INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Strategic Information Warfare
Gregory J. Rattray

Guest Presentations, Spring 1997
Philip B. Heymann; Kenneth Allard; Denis Clift; Douglas D. Bucholz; Arnold E. Donahue; Charles A. Briggs; Anita K. Jones; David S. Alberts; Gregory J. Rattray

April 1998

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-47-X **I-98-2**

Strategic Information Warfare

Gregory J. Rattray

Major Gregory J. Rattray, USAF, is currently a Ph.D. candidate at the Fletcher School of Law and Diplomacy, Tufts University, studying the security implications of the information age. His previous assignment was at the U.S. Air Force Academy in Colorado Springs as an assistant professor of political science and deputy director of the USAF Institute for National Security Studies. He served as an intelligence officer at Headquarters Strategic Air Command, Offutt Air Force Base, Nebraska, dealing with arms control and national intelligence estimates from 1989 to 1991, and with the 18th Tactical Fighter Wing, Kadena Air Base, Okinawa, Japan, from 1987 to 1988. He is a term member of the Council on Foreign Relations and co-editor of Arms Control Towards the 21st Century, *Lynne Rienner Press, 1996, as well as the author of numerous studies and articles on arms control, proliferation, and conflict in the information age. Major Rattray received a B.S. in International Affairs and Military History from the USAF Academy in 1984 and an M.P.P. from the John F. Kennedy School of Government, Harvard University, in 1986.*

Oettinger: I am delighted to present our "bonus" speaker, Major Gregory Rattray. You have seen his biography, so I won't cut into his time with a long introduction. Greg, it's all yours.

Rattray: My name is Greg Rattray. I'm an Air Force officer, as of this morning starting the process of writing my dissertation full time up at the Fletcher School. The topic that I'm going to talk about today, and the topic of my dissertation, is strategic information warfare.

Just so you'll know a little bit of where I'm coming from, I'm an intelligence officer in the Air Force. I was teaching at the Air Force Academy before I went back to get my Ph.D. I decided that if I were going to get a Ph.D., I would move away from what I had been focusing my career and my studies on—strategic nuclear issues and arms control—and move into what I still think is an important, and yet ill-defined, area of national security concern: information warfare. My particular effort is to try to draw some boundaries between the very important work that's being done about enhancing the effectiveness of battlefield forces and whether a separate concern exists about a strategic threat.

I'm going to use the analogy to strategic bombardment in World War II, where one attempts not to have to fight the other guy's navy and army, but to go straight to what Clausewitz called "the center of gravity of the opponent," and influence his political decisions by specifically attacking his critical infrastructures. Dr. Alberts did a good job last week of saying that the information infrastructure, for modern societies, underpins a lot of other important infrastructures.[1] Does it now constitute a specific center of gravity that's worth talking about?

I doubt anybody tried to look up that World Wide Web address that I put on the table last week. This is now obviously a major national concern. The President put together a commission last July, which in fits and starts is trying to get its hands around the problem. The Web address for the President's Commission on Critical Infrastructure Protection is www.pccip.gov.

This is what I will talk about (figure 1). I want to discuss the concept of vulnerability and what we really don't know about vulnerability, and some different conceptions of the major drivers of information infrastructure vulnerability to outside attack. I want to advocate that we can think about

[1] See Dr. Alberts's presentation in this volume.

- **Vulnerability of information infrastructures**
- **Thinking about information warfare as military force**
- **"Strategic" information warfare**
  - Success factors
- **Creating and sustaining strategic information warfare forces**
  - Acquiring vs. assimilating technology

Figure 1

Topics to Discuss

information warfare as military force and really try to reconnect to past frameworks we've had about how political entities use force to achieve their objectives. I will use these frameworks for thinking about whether strategic information warfare is a significant problem or not.

Then I'll talk about what I think is a useful conceptualization of what strategic information warfare is, and about what past strategic warfare efforts demonstrate to be key success factors. What do you have to do to wage strategic warfare, generically, whether it's air warfare, or an economic blockade, or attacks on information infrastructures? Then I am going to step off and make some assertions or initial judgments about how I think information warfare might stack up against these five key success factors that I've identified.

Something that I think gets talked about very little right now, yet should be of primary concern, is that even if this potential infrastructure is vulnerable to attack, what must an international actor do to create an organization that on an ongoing basis can attack this infrastructure? My opinion is that it's not six hackers and $10 million. You've got to create a large, substantial organization in order to target, assess, and be ready to go when a crisis emerges, as opposed to when it's convenient. I'll finish up with that.

What I'm not going to talk about is much about specific hacking incidents—the hacker tools, the different viruses. I'm not a technologist by training, so I'd be out of my depth anyway doing that.

What have you guys read in the course? Did you guys read Schwartau's book?[2]

Student: Yes, it was helpful.

Rattray: The second edition, or the first and second editions?

Student: The second.

Rattray: Anything else specifically?

Oettinger: They've heard Alberts.

Rattray: I was there.

I call this slide "Vulnerability of Information Infrastructure—An Agnostic's View" (figure 2). It's interesting that Professor Oettinger this morning encouraged me to take an agnostic view, and last night I decided that was the term that I would use for my own perspective.

- **Reliance ≠ vulnerability necessarily**
- **Significance of vulnerability = f(threat, susceptibility, value)**
  - Importance of insiders
- **Two views: cascades and perceptions vs. redundancy and self-assurance**
- **Significance of attack on vulnerability dependent on objectives sought**

Figure 2

Vulnerability—An Agnostic's View

Oettinger: He pulled the rug right out from under me. I thought I was going to make a beautiful point of it in his exam, and he whipped out this slide.

Rattray: A lot of people say that the United States is the country most reliant on information infrastructure; therefore, we are the most vulnerable. What that first bullet is supposed to mean is that the two are not necessarily equal. In my estimation—and I

[2] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunders Mouth Press, 1991.

am piggybacking it on some other work that was actually done for the Program on Information Resources Policy a while ago—the significance of vulnerability of your information resources is a function of three primary things: the threat to those resources, the susceptibility of a given resource to attack, and then the value of the resource. Understanding the significance of all three factors tends to be what's missing in a lot of the evaluations of infrastructure vulnerability right now.

This framework was created by a guy named Dan Knauf. I'm sure Professor Oettinger can give you the citation from his study.[3] I just kind of condensed a couple of his diagrams.

Oettinger: This man was from the National Security Agency and was liberated to do a little real thinking here. It didn't seem to do him any harm: they just promoted him to Senior Executive Service rank.

Rattray: Starting off looking at the vulnerability of any specific resource—like a company's intranet, the Internet writ large, a database—first, when you think about the threat to network systems, there are definitely lots of instances where people out there would like to intrude and disrupt information resources. But they're not all hostile. We have plenty of instances, maybe even more significant instances, where, inadvertently, these information infrastructures break.

The other thing that I think is important right here is that we talked a lot about hacking, with people not connected with the organization targeted as the major concern. But insiders are, in many people's estimation, much more important. They certainly simplify your problem if you look at it as a targeting problem of what you want to break, and how you get access to it or how you get to the target. I'm not going to talk about that again, but if you think about this problem, remember that the normal play of espionage and counterespionage or counterintelligence is going to be a very significant portion of the overall problem.

Then, are these things susceptible to any number of different types of manipulation and damage? We certainly see that information networks, generically, can be hacked into. The Defense Information Systems Agency conducted a widely quoted study where they ran red team attacks against open, unclassified information systems, and 80 percent of them were vulnerable to attack. A guy named Dan Farmer, who was a co-author of something called the SATAN (Security Administrator Tool for Analyzing Networks) did a recent survey of banks, government sites, and even pornography sites on the Web, and tried to see which of these were most vulnerable to simple, scripted hacking attacks. He found that over 50 percent of these sites were vulnerable; actually, the banks were the most vulnerable of all the different places.

But what's not really in that equation is the value of these resources. The Air Force, CIA, and Department of Justice Web pages have all been hacked and defaced. But how significant is that? If we're talking about a strategic attack, which I'm going to get into, you need to think about the relative value of the resources. They might be vulnerable to attack in an aggregate sense, but it is not clear that, in terms of achieving political objectives, you can disrupt enough value to achieve your objectives.

The example that I'll use is the heavily cited Citicorp attack. If your objective is financial, if you are a criminal, and you can hack $100 million out of Citicorp and get away with it, that is certainly significant from your perspective. But if you're Iraq and your objective is to get the United States to pull out of Saudi Arabia and to give up on Kuwait, that same attack is not strategic in the sense of it achieving your objective. We definitely saw in World War II large levels of damage inflicted on populations and economies, but because of the high level of national concern and objective in the situation, they were willing to take a lot of damage before any strategic impact was achieved.

[3] 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.

I want to go to this slide (figure 3) for just a second, just because Dr. Oettinger had the upper hand last week. Dr. Alberts

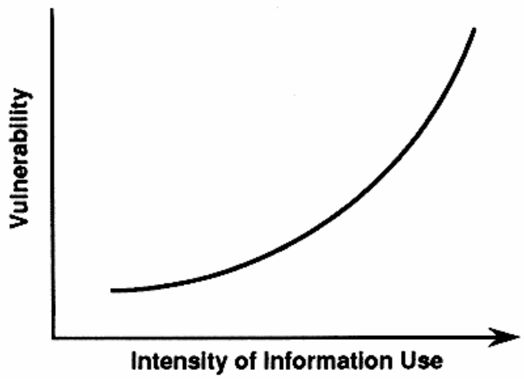

Figure 3

Information Reliance vs. Vulnerability: Cascades and Perceptions

would argue that as information reliance goes up, vulnerability goes up (figure 3). His argument was, I think, two-fold: that as you become more information reliant the systems get more complex, you don't understand them that well, and you have the possibility for cascades. Plus, reliance makes people's perceptions important, and if they can't rely on important information systems, you get a lot of effect from the fact that they are disrupted.

Other people who work with Dr. Alberts would argue that the relationship actually works in the opposite way (figure 4). As the intensity of your information use grows and your society becomes more networked, then because of redundancy (if you can get the operators of these infrastructures to self-assure that they'll work properly), basically, as you get more information dense, you become less vulnerable.

Oettinger: I might just point out that, in terms of tensions and so on, my sense is that there's a genuine tension here. Both of these viewpoints are tenable. For those of you who may have studied engineering, one can give very good small examples of

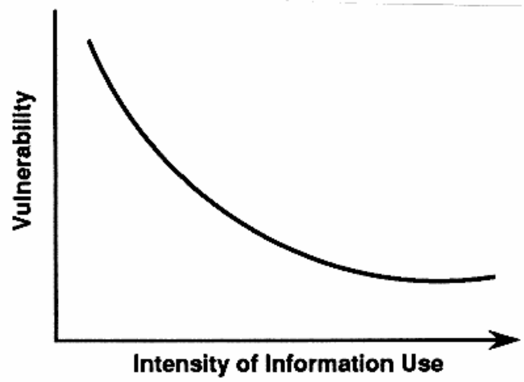

Figure 4

Information Reliance vs. Vulnerability: Redundancy and Self-Protection

either one being true. The critical question is, empirically, what is going on in reality? Which of these dominates? You can't do that by just putting your finger in the wind and sensing it. That's a hard empirical job, in protecting against attack, or in designing a system, or in mounting an attack. You cannot do that, I think, without knowing the answer to those questions. Conceptually that's neat, but it doesn't give you empirical knowledge. It's like a model without parameters.

Rattray: It isn't either/or among these two models. You could certainly have other functions where certain societies, as they build their information infrastructures, either decide, like the Chinese, that they want centralized points of control, which creates nodes of vulnerability, or else the nature of the technologies is such that they are centralized through need for some degree of large-scale information processing capability. Then, as you move from mainframe computers to PCs and they become distributed, you start to lose vulnerability (figure 5). Again, I don't have an answer among these three, but this would be one way to test empirically which of these relationships was the viable one.

Thinking about information warfare, not even at the strategic level necessarily, but just as breaking another guy's

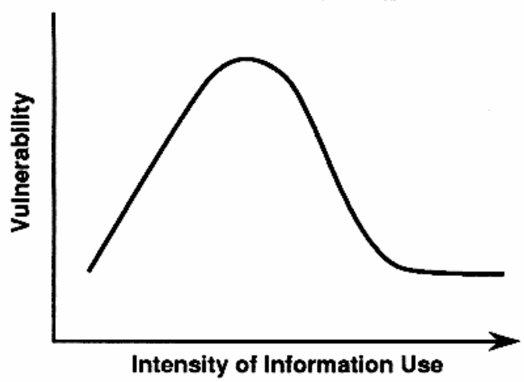

Figure 5

Information Reliance vs. Vulnerability: A Hybrid Situation

information systems, I'm going to try to segregate it by means and ends (figure 6). This is not new. As long as nations have waged war, and people have been in conflict, they have tried to disrupt the other side's ability to process information. You can do that mechanically. You can bomb the other guy's radar systems, his command and control centers. You can go in with a pair of cable cutters and cut a fiber-optic cable. That would be a mechanical attack.

Actually, I should probably have left pulse off here. If you have electromagnetic attacks, they certainly can disrupt information systems. In the Cold War, we worried a lot about what would happen if the Soviets set off a nuclear weapon at 100 miles' altitude. What would be the effect on all the ignition systems of cars and more critical information systems as this wave of electromagnetic radiation moved through wires like the one running down this table and fried the equipment at the end of them? Also included in electromagnetic attacks was jamming: directed energy in order to disrupt the ability of a system to work.

- **Means—mechanical, electromagnetic pulse, digital (i.e., hacking)**
  - What's new? Digital is hard to observe.
  - What's not? All three are physical.
- **Ends—warfare is force to achieve political objectives**
  - Other objectives possible, but not warfare
  - IW as microforce—examines similarities and differences from existing constructs

Figure 6

IW as Military Force

What's new about all this information warfare hype is the ability to go in there digitally and manipulate the bits in an information system and change its ability to function properly. One of the reasons I think that everybody's pretty hyped up about it is that this is very difficult to observe, and it seems to exist almost independent of the physical realm. But my argument is that this is a dangerous way of thinking about it, and Professor Oettinger has been encouraging me to try to find the right words to explain this.

All three of these are physical. When you flip the bits in somebody's computer, you actually have to send some micro piece of physical energy through the wires so that you achieve the effect you desire in the other side's computer. If you think of this as all virtual, you tend to forget, first, that there are other ways of disrupting information infrastructures besides simply the virtual or hacking way, and second, that because hacking is a physical act at a micro level, there are defenses that can be put up against it. If you think about it in a physical form, it tends to make you conceive of offense and defense: getting to a point and then being able to put barriers in the way of getting to that.

Oettinger: That is not a red herring that he's putting up. Most people, including many in responsible positions in this area, have fallen victim to the kind of nonsense that's in Nick Negroponte's book *Being Digital*,[4] which contrasts bits with the

[4] Nicholas Negroponte, *Being Digital*. New York: Knopf, 1995.

physical world, as if bits were incorporeal. It's complete nonsense, yet lots of people believe it.

Rattray: The other thing that I think is very important, if you're going to talk about strategic warfare—and if you're going to talk about warfare in the Clausewitzian sense—is that warfare is political. Warfare is not espionage and it's not financial crime. I'll acknowledge these other objectives are possible, but these don't fall into classically defined definitions of warfare. Right now, if you conduct an act of espionage, international law handles that one way. If you conduct an act of aggression, international law tries to define that differently in terms of the appropriate responses by international actors. So, one thing that's going to underpin my concept of strategic information warfare is one actor trying to achieve a political objective against another actor. Therefore, I get around to saying, "We can conceive of information warfare as microforce," and then use existing constructs from national security studies about how force works in terms of achieving political objectives and what's the same and what is different for information warfare.

These constructs come from Robert Art and Tom Schelling (figure 7). Schelling's name should resonate with some people at this school. I think the classic conceptions of deterrence, defense, and "compellance" all need to be properly applied to this problem. I'm going to try to do some of that.

- **Art/Schelling constructs: IW can involve the first three**
  - Defense
  - Coercion/compellance
  - Deterrence
  - Swaggering
- **IW as forces in being vs. attack when ready/out of the blue**

Figure 7
Functions of Military Force

I also want to talk a little bit more right now about strategic warfare (figure 8). During the Cold War, which we have now moved out of (at least for five or six years), in the United States, things were strategic if they were nuclear or if the delivery system was intercontinental. I spent three years in the Strategic Air Command headquarters building in Omaha, Nebraska, and that was the definition of "strategic" we used. I think one other legacy of the Cold War that we're fighting right now is that because the United States is so used to the homeland being a sanctuary, anything that can get to the United States from outside our borders is considered strategic just because it can hit us. That is why I think a lot of people tend to call the Citicorp incident or the English hackers getting into Rome Labs computers strategic. Just because they did it from a long distance connotes "strategic" to those of us who were brought up in the Cold War, and I don't think that is useful.

I call this "non-Cold War" instead of "post-Cold War," because I think through most of the history of strategic studies, strategic warfare has generally meant hitting the enemy's centers of gravity. This goes all the way back to Clausewitz, who defined the concept of a center of gravity as the focal point that you want to push

- **What is strategic warfare?**
  - Cold War: nuclear/intercontinental
  - Non-Cold War: ability to hit enemy centers of gravity without fighting fielded forces
- **What is strategic information warfare?**
  - Waged by strategic entity for political objective
    - Both state and non-state actors
  - Use of new means (digital/microforce) against new center of gravity (information infrastructure)
  - Crosses legal boundaries and constitutes an act of aggression

Figure 8
Constructing a Framework for Strategic Information Warfare

against in order to achieve your objectives. In Clausewitz's time, you generally had to fight the enemy's fielded forces to get to his centers of gravity, but in the 20th century, air power emerged as a way to go right after populations or economic resources that the enemy holds dear without fighting fielded forces.

Student: I agree with you 100 percent. Can I just offer you an analysis, because I'm a strategic warrior myself, and did a lot of time in SAC. What you're hitting on right there is really that, during the Cold War, we focused on means. The term "strategic" was means oriented instead of ends oriented, which is what "strategic" always meant before and means again now. So what is the end of strategy?

Rattray: I think that's a legitimate distinction.

Student: That's why I think you're right on, and that would be very useful if you can keep that tied together with your previous slide, and then with what it looks like you're going to say next about information warfare.

Rattray: Whether it's distance or whether it's the means that cover that distance, in the Cold War, a nuclear confrontation was something we wanted to avoid, so there was no debate about ends. The ends were clear, so therefore we started to define it in terms of means, as you were saying.

Oettinger: He's made a very important point, but let me just jump in because it gives me a lever for making another. You keep saying "define," but "define" (I've said this to the class in a number of comments on papers and so on) drives me nuts because it suggests logic chopping, abstraction, irrelevance, neither here nor there. What you're both talking about is "usage," which is a much stronger concept. Again, it's empirical. You're saying that some folks use it this way. Some folks use it that way. That's a statement that has some weight. They're real people and there are real actions behind it, and they don't care about definitions. So, stick to "usage." It has that empirical, physical, real connection. Stay away from definitions. Every time you say "define," ask yourself if you really mean that, or if you can throw it out and use "usage," because then there are real things behind it, empirical content. Then you're able to sort out the kind of issue that he's talking about, because he's saying a lot of different groups, different periods, have used the terms in a different way. That's reality. That's not academic bullshit.

Rattray: Usage of one set of terms drives the decisions you're going to make about how to achieve your objectives, and therefore usage is important.

I've already talked about this: that strategic information warfare is waged by a strategic entity (figure 8). I'm going to use the definition that it's any organization that can define its objectives and bring resources to bear to achieve those political objectives. I am not going to try to argue that any definition of strategic warfare doesn't have very porous boundaries. You can argue a lot about what is "political," but I don't think there can be much argument that both state and nonstate actors, using the means that we talked about a little while ago, can certainly attempt to achieve political objectives by strategic information warfare. I'm going to concentrate on these new means—the digital microforce—directed against new centers of gravity—information infrastructures.

Oettinger: Is "microforce" your term? It's lovely!

Rattray: That term emerged from a discussion that we had.

Oettinger: Oh, good!

Rattray: I'm willing to have anybody give me feedback, but I do think that at some point "strategic information warfare" means that you start to cross legal boundaries and undertake a clear act of aggression. That is an important thing, a little bit distinct from just trying to achieve a strategic political objective. The problem is that the current legal constructs for international law particularly, but also domestic law, do not deal well with microforce as a means of aggression.

Oettinger: That's where you use that Holmes quotation that I gave you this morning, not the Montesquieu part of it, but the one that the law is behind the times.[5]

Rattray: The other difficult part about the current international legal constructs is not only what constitutes an act of aggression, but also that information infrastructures are so "internetted" that they cross all types of boundaries. The tactical satellite that is carrying your opponent's communications is probably relied upon by neutrals, your allies, possibly yourself, and therefore, whom have you committed an act of aggression against? If an attack goes through Britain to get to the United States, does Britain assume some type of responsibility for that?

Oettinger: What you ought to read in connection with that is Matt Bencke's book, *The Politics of Space.*[6] Did I mention that to you? It's brand new. For some of you who have not seen that, it's a beautiful book. The reason for its relevance right here is that in terms of strategic weaponry and counterintelligence and so on, the United States and the Soviets essentially developed new law in connection with this whole question of overflying. The overflights by airplanes are technically violations of airspace. It describes marvelously this bit of arm wrestling over whether space assets would or would not be handled by the same regime. Essentially, the political definition of this by the United States and the USSR during that period from the shootdown of Gary Powers on through now is a marvelous example of the nebulosity of the law, but it wasn't a bunch of legal eagles who did it. It was negotiations and realities ... I won't say on the ground, but in space and so on, and there might be some useful precedents there.

Student: There's a very interesting book published by MIT Press called *Cyberspace and the Law,*[7] and it discusses just the things that you're talking about. I don't know if you might be interested in that.

Rattray: I would be.

Student: There was an act passed by Congress a few years ago that attempted to deal with this. It didn't deal with it very effectively, but it did make things like breaking into corporate accounts that you're not authorized to be in felonies, criminal acts.

Rattray: Yes, there are definitely two levels to this. There is a need to strengthen domestic laws to make malicious intrusions clearly felonies. At the international level (which is actually going to be the more difficult level, and, for strategic attacks, the more relevant level) it's going to be a lot harder to formulate international law that deals well with this.

Student: Based on your slide (figure 8), I have to ask if the focus of your paper is strategic information warfare or strategic warfare in the electronic realm? It seems to me that there might be a nuance of difference there. I think you might have trouble putting your arms around "information warfare" as it's currently used in DOD terms.

---

[5] "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 battlefront against each other, the time for law has not come; the notion destined to prevail is not yet entitled to the field." Oliver Wendell Holmes, *Collected Legal Papers*. New York: Harcourt, Brace and Co., 1921.

[6] Matthew J. von Bencke, *The Politics of Space.* Boulder, CO: Westview Press, 1996.

[7] Edward A. Cavazos, *Cyberspace and the Law: Your Rights and Duties in the On-Line World.* Cambridge, MA: MIT Press, 1994. See also William C. Saturley and Gordon J. MacDonald, "Jurisdiction.com: Personal Jurisdiction in Cyberspace," *New Hampshire Bar Journal*, June 1997.

Rattray: I'm not going to use the DOD definition. What I'm going to say is that there is a strategic level with these types of boundaries around it. I'm only going to deal with the concept that basically you could attack another nation's, or even a nonstate actor's, information infrastructure and get them to do what you wanted them to without having to fight their armies and their navies. Most of what DOD calls "information warfare" now deals with enhancing the ability of the Army, Air Force, and Navy to fight other armies, air forces, and navies.

Student: The only other thing is something that you might want to consider taking a look at as you do your research. In the early 1950s, the Air Force ran a research effort called Project Control. It was the first effort after World War II to make strategic application for nuclear warfare. Since you're dealing with information warfare, which is a major (I hate to use the word "paradigm,") paradigm shift in warfighting, it may offer some thoughts on how you go ahead in dealing with a completely different way of doing business. It had all the brain trust in the United States at the time working on it: Bernard Brodie, Paul Nitze, and the like—the people who did it were just incredible. It was a two-year study. It's all in the archives at the Air University.

Rattray: Down at Maxwell? Thank you.

Oettinger: You two ought to get together and keep picking each other's brains. Thank you so much.

Rattray: The stuff I have right now actually looks more at the evolution of strategic bombing from World War I to World War II, in a kind of attempt to get their hands around a new tool to achieve strategic ends, and then at World War II and at what worked and didn't work about that.

What I found was that to wage strategic warfare successfully, you need these five things (figure 9). There's no conclusion here, but I think that in strategic information warfare now, you probably can get offensive advantage for a lot of reasons we could talk about. But it's the other four factors that are missing from a lot of the analyses of strategic information warfare.

- **Offensive advantage**
- **Significant vulnerability to attacks exists**
- **Vulnerabilities can be identified, targeted and damage assessed**
- **Prospects for effective retaliation minimized**
  - **i.e., not reliant or good defense**
- **Effective command and control possible**

Figure 9

Conditions for Successfully Waging Strategic Warfare

First, as we talked about, I'm not sure we can assert that significant vulnerability to attack exists, even in the case of the United States. Certainly there are a lot of actors who do not need information resources as much, which may create asymmetric vulnerabilities that are important to think about.

In terms of targeting, which I've alluded to a lot, if you're going to arrange a successful strategic information warfare campaign to achieve a political objective, you need to be able to identify targets in advance and assess the damage that you're going to do against your targets. I was trying to press Dr. Alberts a little bit last week, because this is where I really think that the analysis that relies on these cascades and perception management falls short. Very few nations, I think, launch attacks with no idea exactly of what the effects are going to be. It's a risky course at a minimum. If the attack creates results that are so much more damaging than you think they're going to be, you invite your opponent to retaliate by other means that you may not want. You may get an escalation that you may not be able to control. Therefore, relying on cascading effects on information infrastructures, which potentially could kill tens, hundreds, or thousands of people, against a nation like the United States, means you rapidly lose control over achieving your objectives, and you get yourself into an escalating conflict, which again I think is underanalyzed right now.

Related to this is that if you're going to unleash these tools, the prospect for effective retaliation against yourself needs to be minimized. Either you're not reliant, or you've got good defenses, which are choices that actors could make if they plan on developing the offense.

Oettinger: Aren't you violating your own contrast between reliant and vulnerable?

Rattray: You're right.

Oettinger: Make a note for yourself to fix that. We've gone beyond that point.

Rattray: Another thing that most air power theorists have come to understand over time is that effective command and control is necessary. The Air Force works a lot on more or less centralized control and decentralized execution: having a central place where the enemy is assessed, and hitting the targets that need to be hit next in a manner which maximizes effectiveness. There's a real tension here, I think, with the types of activities that are supposed to be anonymous, like hackers, or the use of insiders. The more anonymous and "inside" your offensive resources are, the less ability you have to control them, the more difficult the communication is, and the more likely it is that you might tip off your attack in trying to communicate with your attack assets. It's a very speculative statement, but I think there is something of weight in there.

Student: Have you thought yet about the mechanism behind the target that's going to produce the political influence? Because that's kind of the perennial problem of air power theory: the targets are easy to identify, but the specifics of the mechanism between when you destroy the target that produces X effect and the stream of events that produces an actual political outcome is much more nebulous. It seems that in information warfare you're really attacking a target that changes the structure of society, which is different from a physical threat from a soldier, a sailor, an airplane, or whatever that threatens the existence of certain segments of society. Therefore, the political calculation that changed their strategic stance is going to be based on some sense of how they want to maintain the structure of their society.

Student: It seems to me that the logical problem, from the attacker's perspective, is that when you're evaluating the possible linkages between these forces and the political outcomes, you've actually changed that society, so you're not even dealing with the same society you started out with when you were first doing that evaluation.

Rattray: I really haven't thought about it in those terms, because that assumes a very long-term war; that you're doing this to such an extent over time that they really have to adapt. Because they can't use certain information means, like electronic transmission of banking information, they can't use banks, and now they've got to undertake a massive transformation of how that aspect of society works. That is something I definitely have to think more about.

In a shorter-term sense, though, if you did attack the banking system, the idea is that the linkage to political effect would be runs on the banks, and people would lose faith in the banking system or in the stock market in its arguably inflated mode right now. A little bit of disruption might be the thing that causes the market to fall, and economic pain from that, particularly economic pain for the advantaged, would then turn on the political authorities to do something about it. If the political authorities did not have the means to respond against the adversary, they might capitulate into whatever the adversary was trying to achieve through these attacks. That's about as far as my thinking has gone: that these are the steps beyond hacking the bank that you're implicitly positing when you say you're going to get political effect, and that history would tell you that these are not easily estimable effects. Usually these are miscalculations as opposed to calculable ...

Oettinger: Yes, but I think these suggestions give you another gradation on that scale, and you might as well mention it. You may not have the time to bring scenarios that far into the longer term, but conceptually you have some very interesting suggestions.

Rattray: I mentioned at the start that most analyses say that people could get into information systems, and therefore they can then attack them, but very few point out that these attacks would be launched by a force that is in being, waiting for a political crisis where it is called upon to be the instrument of force for an actor (figure 10). That is a very different thing from simply finding out where the enemy's holes are and attacking him instantaneously before he has a chance to change the infrastructures (which happens very fast, even inadvertently, in information infrastructures), let alone discover your attempt and defend himself.

My argument right now is that getting the technological tools to conduct digital warfare, especially as Alberts defines it, is fairly easy. Assimilating those tools into an organization that fits in with your other military missions and your national security constructs is a much more difficult task. What I tried to do is look at both civilian and military literature on what causes organizations to be successful in assimilation.These are the conditions that I found facilitate successful assimilation (figure 11).

These are some of the assimilation challenges to organizations tasked with offensive information warfare and organizations tasked with defensive information warfare (figure 12). I'll just leave it at that.

Oettinger: All right. This is by far the best organized overview of how one ought to be thinking about this that I've ever heard anywhere. Thank you very much, Greg.

- **Back to idea that these are forces in being, not one-off attacks**
- **Acquiring technological tools—fairly easy**
- **Assimilating technological tools to conduct new military missions—much more difficult**

Figure 10

Creating and Sustaining Strategic Information Warfare Forces

Contextual

- **Fertile institutions**
- **Systems integration**
- **Available human capital**
- **Connection to international technology networks**
- **Social/cultural mesh**

Organizational

- **Emphasis on learning**
- **Managerial initiative**
- **Internal technological expertise**
- **Linkages to outside networks**
- **Demand-pull motivation**

Figure 11

Success Factors in Information Technology Assimilation

Offensive

- **Totally new mission**
  - State vs. non-state
- **Desire for secrecy cuts against networking**
- **Stronger demand-pull for those who can't fight by other means**

Defensive

- **Protect existing mission capability**
- **Monitor fast-changing information infrastructure**
- **Outside government control**
  - Coordination crucial
- **Demand-pull?**

Figure 12

Assimilation Challenges for Strategic Information Warfare (Organizational Level)

INCSEMINARS1997

ISBN-1-879716-47-X