INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Information Operations
Gregory C. Radabaugh

Guest Presentations, Spring 2002
Robert B. Brannon, Gregory C. Radabaugh, Robert A. Rosenberg, Gary L. Salisbury, Roberta E. Lenczowski, James B. Plehal, Dean W. Cash, Patrick F. Kennedy, Warren B. Rudman, Joseph K. Kellogg, Jr.

November 2002

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 1-879716-81-X **I-02-1**

November 2002

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Inc.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Sonexis
Strategy Assistance Services
TOR LLC
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

Information Operations

Gregory C. Radabaugh

February 21, 2002

Gregory C. Radabaugh is chief of the Information Analysis Division, Air Force Information Warfare Center [AFIWC]. A career intelligence officer, he began in 1974 as an enlisted linguist (Mandarin Chinese) for the U.S. Air Force [USAF] Security Service. He was commissioned in 1979 and spent tours at the Air Force Electronic Warfare Center, Air Force Intelligence Service, 6903rd Electronic Security Group, and the Defense Intelligence Agency [DIA]. In 1989, he transitioned from active duty to a civilian position at the DIA, where he conducted analysis of Soviet/former Soviet strategic weapons research and development and production, including over 25 tours as an arms control inspector in the former Soviet Union. He transferred to the Air Intelligence Agency's Directorate of Plans and Programs in 1996, and spent 1997 as the USAF representative to the Unified Cryptologic Architecture study. In 1998 he was hired by the Joint Information Operations Center, serving as its chief of intelligence and deputy chief of the plans assessment division until July 2000, when he assumed his present position. An active USAF reservist (lieutenant colonel), he is currently assigned to the Joint Staff as a combat targeteer supporting combat operations in the Middle East and Kosovo. Other tours have included duty with U.S. Central Command, the intelligence community staff, and the United Nations Military Observation Group. He has a B.A. in clinical psychology and Chinese from the University of Maryland and an M.S. in strategic intelligence from Defense Intelligence College. He is also a graduate of the Air War College, Air Command and Staff College, Squadron Officer's School, the USAF Special Operations School, and the Defense Language Institute.

Oettinger: I am delighted to introduce our speaker, Greg Radabaugh. You've read his biography, so I won't go into a lot of detail about his background. Also with us, by the way, is Greg Rattray,[1] author of your reading for today.

Rattray: I'll take all your spears. Tony always sends me all the class's comments on the book. There might be an opportunity at the end of the class for you just to spear me right here.

---

[1]Lieutenant Colonel Gregory J. Rattray, USAF, is deputy chief of the Defensive Information Warfare Division, Headquarters, USAF. He is the author of *Strategic Warfare in Cyberspace* (Cambridge, Mass.: The MIT Press, 2001).

Radabaugh: Let me begin with the most dreaded words known to mankind: "Hi, I'm from the government, and I'm here to help you." I hope you've seen my biography, some of which is actually believable. I started in the intelligence business in 1974 and have somehow managed to survive it ever since. Unlike some of the speakers you will have in the future, who are way up there in the stratosphere, I am but a lowly cog in the machine who actually has to do things when some people way up there say, "That's a good idea! Why don't you do it?" I've been an enlisted person, an officer, in the reserves, on active duty, and a civilian with AFIWC. I've done SIGINT [signals intelligence]; I've done HUMINT [human intelligence]; I've done special operations; I've worked for the DIA and the NSA [National Security Agency]. What should that tell you? I can't hold a job. What it should really tell you, though, is that I've got enough background, enough experience in the real world, that maybe what I say will have some *gravitas* and some reality to you.

Oettinger: *Gravitas* and *veritas*!

Student: Not if you're in Congress!

Radabaugh: I have to make a couple of disclaimers right up front. First off, what I'm about to say should not be construed in any way as the official Department of Defense [DOD], U.S. government, or USAF position. It is my own personal opinion in all this. They cattle prod me if I don't say that.

Second, this is an unclassified environment. If you ask me questions—and I encourage you to ask questions, make sarcastic, biting remarks, and all those things I'm used to—and I hesitate or stop for a while, it's because of one of two things. One, I'm trying to figure out in my own mind whether my response is classified or not and what unclassified information I can tell you. Two, I haven't a clue what the answer is, but I'm hoping you'll think that I'm trying to figure out in my mind whether it's classified or unclassified. I'll let you try to figure out which I'm doing. Finally, just so that you'll feel comfortable, rest assured that no animals were hurt or killed in the development of this presentation, so that should be okay for Harvard.

What I'm going to try to do in essence is take about a month's or a week's worth of studying the area of information operations [IO] and cram it into two hours. To do that I've actually forced myself to sit down and write notes on where I'd like to go and what I'd like to say. Of course, if I'm at all lucky, some of what I say will actually have some relationship to the notes I wrote in my columnless format.

Since this is a mixture of military, government, and people who have never seen the military or the government in their lives, and since what I'm talking about is the field of IO, which, in essence, is a warfare kind of thing, I'm going to give you some of the basics of warfare so that you have a common understanding of what this is all about. Then I'll talk a little bit about "What is this beast called IO?" because there are a lot of different thoughts about what it is, why it is, and why you should care. From that point, since IO is so heavily dependent on intelligence, and since I'm an intelligence officer and that's what I do, I thought I'd put intelligence in anyway, because it's good. Write that down in your notes: Intelligence is good!

Then, because a lot of people think of IO as the cyber realm—cyberspace, computer network attack [CNA], and so on—we'll talk specifically about that. I'll try to leave about ten minutes at the end so that if anybody has questions for Greg about his book, like "Why did you write *that*, you dummy, when you know it was supposed to be *this*?" or "Why in God's name is it so heavy?" that will be your opportunity to make biting, sarcastic remarks to him, and I hope you may be able to argue some points with him, because this man is the expert.

Oettinger: He's willing to autograph the book.

Student: For twenty dollars.

Rattray: No fee. I can't accept any money for that.

Student: I tried!

Radabaugh: From that, I'll try to describe the state of IO today. How well do I think it's working? Where do I think it's working or not? From there I'll go to where I see IO going in the future. Finally, I'll wrap up with, "After all this blathering and chattering on like a gerbil on crank, what is it I want you to take from this when you walk out of this room?"

With that said, I'll just begin with everybody's favorite topic: war. It must be everybody's favorite topic, because we've been doing warfare ever since there were people clawing around on the ground and deciding that "What you've got I want." The thing to understand about warfare from, in essence, a professional standpoint—that of people whose livelihood and profession are warfare—is that there is a very distinct taxonomy to it: a distinct doctrine, ideas, the ways things work.

Basically, what is warfare? In its essence, it's compelling your enemy to do your will. You want him to do something or not do something. That's it.

Why would you want somebody to do something or not do something? There are generally four reasons why peoples or nation-states will go to war. The first one is honor. We saw that kick off World War I, when Germany decided it had to honor its treaty commitments to Austria, which had decided to kick the crap out of Serbia for shooting Archduke Franz Ferdinand. That kicked off a whole chain of events. Everybody was thinking it was not going to happen, but because of honor, treaty commitments—the same things that took France and Britain into World War II in defense of Poland—started warfare. You feel honor-bound, like the Hatfields and the McCoys, to protect your family's honor.

Then there's defense. You're sitting there fat, dumb, and happy, and some idiot comes across your border and starts shooting at you, so you're going to shoot back.

Then you have people who just like to go conquer things. It's an ego trip. It's a need. It's glory. It's Caesar spreading Rome all the way to England and Germania.

Finally, there are resources. They have some neat stuff that you want, so you're going to go take it, which then drives them to the defense model, which is "There are people coming over the border shooting at me."

Because of these various things, there have been conflicts among people ever since there have been people. Because of the development of societies and cultures and technology, warfare has progressed from one person against another person, where it's *mano a mano*—"Nice hambone, Grog! I think I'll take it!"—to tribal conflicts, where you might have the Sioux going against the Blackfeet because of some slight. From there it developed into war between city-states, like the Peloponnesian War between Athens and Sparta. Then you start moving to nation-states, where the Treaty of Westphalia [1648] kind of said, "Yea, verily, you are now states. These are your borders. Cross these lines and bad things happen." Then it moves into things that are cultural, like the Crusades, and, centuries later, the Muslim culture made it all the way to the gates of Vienna [1683] before the Christian culture of northern Europe pushed it back. We have it even today in the events of September 11, in which a culture is saying, "We're going to push you out of your side of the planet," and now the United States is pushing back. So, there are still valid reasons for this thing called warfare.

As Clausewitz said (for you military people, try not to throw up), "Warfare is the continuation of politics by other means." For you nonmilitary folks, they force us military people to read Clausewitz as soon as we get off the bus. He was a wonderful Prussian general who took a look at all of Napoleon's campaigns and said, "Somewhere in there must be ways of doing warfare right." He came up with all these great maxims, some of which you've probably heard, like the one just quoted. When you think about that, what is politics but social activity among people deciding where they want to go or what they want to do or where they're going to be told to go?

While Clausewitz was observing Napoleon prance around Europe, he also discovered that there were things that you go after, called centers of gravity. That's very important when you're thinking about IO, because these are what you focus your efforts on. In essence, the principles of warfare, like mass maneuver and so on, come down to that you want to get the most bang for the least buck. So if you go after the center of gravity, that's a way of compelling that adversary to do your will.

Oettinger: Stop me if I'm going to say something that you're going to get to later, but you worry me by talking about the centers of gravity. It was a wonderful late eighteenth/early nineteenth century metaphor. The problem is that taking it literally doesn't mean anything, and so when you get into realms such as IO, if you're a Clausewitzian you're going to have to spend a great deal of time figuring out what the hell a center of gravity might be. I don't know if you're going to get into that, but I wanted to inject that note of caution. In warfare theory, as in economics, there is a sense of precision about terms that is often lacking in reality. I hope you regard that as a friendly comment.

Radabaugh: Absolutely. Part of the wrestling with IO planning is exactly what Tony said: it's trying to figure out what these centers of gravity are. From a military standpoint, and even from a martial arts standpoint, that center of gravity is very important, because once you get your opponents moved off their center of gravity, you can basically do whatever you want with them, whether it's throw them to the ground or put an armlock on them. Centers of gravity are very important in martial arts, hence, also in warfare. The difference is that you're not looking for an actual, physical center of gravity that you can move somebody with; you're looking for a cultural,

economic, or political center of gravity that you can apply pressure to, and when you move that, the rest of the opponent's ability to resist goes with it. That makes warfare much easier.

Here is a chicken-and-egg question: Which comes first: warfare or technology? Does warfare drive technology, or does technology drive warfare? What you find is that it's kind of a love affair between the two, because technology presents wonderful opportunities, such as the cyber domain. Did the military come up with the cyber domain? No. Do warfare and the military push technology into other areas? Sure, because as soon as you get a new toy that makes you better, faster, or stronger than your opponents, your opponents are going to do one of two things. They're either going to get their own toy (or a better one), or they're going to put their hands up and say, "You got me." Most of them don't opt for door number two. They go out and they get their own, which then pushes you to go further, which then pushes them to go further. So you've got this push going from Grog with the stick to the bow and arrow, to the spear, to the hoplites with the short sword, to gunpowder, to the bomber. It's a progression. If you want to read a great book about the evolution of weapons in warfare, there's one by Trevor Dupuy, a retired Army colonel.[2] It takes you from the very beginning of stone on stone all the way up to the modern day and tells you why things happened, where they happened, and what drove them.

What that drove us to is warfare becoming faster, cheaper, more direct, more accurate, and more precise. World War I was, in essence, our first mechanized war.

Student: When you say "cheaper," do you mean cheaper to prosecute?

Radabaugh: Cheaper to prosecute. One that comes to mind is aerial bombardment. If you think about what happened in World War I, you had the first pilots in biplanes dropping hand grenades out of the side of the airplane and later actually suspending bombs and dropping them. In World War II you had massed air armadas trying to take out an industrial park with thousands of bombs. In Vietnam, you got it down to a few hundred bombs to try to take out a bridge. In Desert Storm, you could put a bomb through a bunker in a specific part of downtown Baghdad. In Kosovo, you could actually put a cruise missile through a specific window.

Now, in Afghanistan, you could throw a JDAM [joint direct attack munition] off an airplane and it would go where you tell it to go. In essence, it's like a GPS [Global Positioning System] receiver and a set of maneuverable fins. If you put it on a regular bomb, like a Mark 82 500-pound bomb or a Mark 84 2,000-pound bomb, and you dial in the coordinates, you say "I want you to go *here*." That way you don't have to worry about weather, or when you drop it. That takes care of a little problem we had in Kosovo and Desert Storm. Laser-guided bombs are great, but if there are smoke and aerosols on the battlefield, that laser gets dispersed and your bomb doesn't know where to go. If there's bad weather it's not going to see that poor SOF [special operations forces] troop who hunked his butt all the way through the mud and slime for two days to get to a spot to irradiate the target, and it can't see the target. Now you find the target and you tell the bomb, "Go there," and it does. So here's technology allowing you to, in essence, prosecute war more cheaply, because where it took 500 B-17s and thousands of bombs in World War II to take out a small target, now you can do that as part of a mission of one B-2. As it flies along it kicks off one JDAM here and another there; it's going to get the target, and it decreases the amount of

[2]Trevor N. Dupuy, *The Evolution of Weapons and Warfare* (New York: Da Capo Press, 1990).

collateral damage. So, from that aspect, it's really a much nicer way of war, so to speak, because the U.S. way of war is something that you don't want to be on the receiving end of.

Let me summarize the U.S. way of war. Number one is firepower. Because the United States and the West believe that its soldiers are worth more alive than dead, it will expend a lot of munitions and ordnance on an enemy to ensure that those people remain alive. If you're on the receiving end of that, what it mostly means is that before you see an American face you're probably going to feel an American bomb or an American bullet.

The other thing is that we have CINCs [commanders in chief]. On the basis of our World War II experience, where we had the European theater operations under Eisenhower and the Pacific theater of operations under Nimitz and MacArthur, the United States found it was easier to divide the world up into specific geographic locations, so that we have one four-star general who worries about one area. That four-star general is in charge of what's called a combatant command, and being in charge he's called the commander in chief, or CINC. So for the Pacific area you have CINCPACOM, or CINCPAC; for the European area you have CINCEUR. That also drives how we do warfare, because anything that comes into that CINC's sphere belongs to that CINC. The way the U.S. military is set up, we have the services, like the Air Force, the Army, and the Navy, which provide the forces and the training, and then the people are sent off to the various CINCdoms to become part of a CINC's arsenal. How do you do that with forces that stay back in the States and yet can still have a reach globally? We'll talk about that when we get to the cyber portion.

Oettinger: As a footnote to what he's just said, that was a very quick passage over a very large set of issues. The structure of the U.S. military in the services is enshrined in Title 10 of the U.S. Code. It's legislated. The CINC structure is also legislated, though later. These two are in perpetual conflict, and many of the anomalies that you may observe in the behavior and organization of the military have to do with that. I just want you to make a note of that. It's a very quick statement of a very profound set of issues that are highly influential in most of what you hear this semester.

Radabaugh: The other Western way of war is enshrined in what is called the Law of Armed Conflict. For those who are not in the military, you may think, on the basis of Arnold Schwarzenegger or Sylvester Stallone movies, that the military goes in and just bombs indiscriminately, shoots anybody they want, and, yeah, that's a fun thing to do. What you have to understand is that when you apply military force, under the Law of Armed Conflict it has to meet four conditions.

The first one is that it has to be a military necessity. You can't just go out and blow up a bunch of stuff because it's in your way. You have to satisfy the requirement that it be a military necessity; that you have to attack that target in order to achieve an objective, and that you cannot do anything that's forbidden by international law.

The second condition is that you're not allowed to cause unnecessary suffering. Usually, the best instance of that is glass projectiles. If you shoot people with glass, it's very difficult for them to be taken care of in a hospital, because glass doesn't show up on x-rays. It's very difficult to find glass in the human body, so the Law of Armed Conflict therefore says, "You don't do that, because that causes unnecessary suffering in the people whom you wound."

The third condition is proportionality. You are not allowed to use more force than necessary and cause excessive civilian casualties. Notice I didn't say "no civilian casualties." It's an accepted part of war that there will be civilian casualties. There are always going to be the 10 percent who never get the word that there are a lot of tanks coming over the hill and, if they'd like not to be there, now is a good time to leave. But you're not allowed to level an entire town in order to get one sniper. That's a violation of proportionality.

Finally, you have to practice distinction, which means you have to understand that you're going after the other side's military. You do not attack civilian targets. Where that becomes a problem is with groups like today's Al Qaeda. They are, in essence, a terrorist organization that is not part of a standing military, so they're kind of criminals. How do you look at a room full of people and tell who's Al Qaeda? It's very difficult to apply this distinction, so people like Al Qaeda are considered outside the Law of Armed Conflict and are not accorded the Geneva Conventions. They have not bound themselves as soldiers in a recognizable military.

Where does that leave us? On the basis of all of this, what's happening is that warfare is becoming faster, it's becoming more intense, more accurate, more precise. When you look at just the past twelve years alone, we had Desert Storm, which was the first precision war. After six weeks of bombing, in a hundred hours the ground troops could take everything apart. Then you go to Kosovo, which was the first war you actually watched happen on CNN [Cable News Network]. My favorite example of people now being so blasé about warfare that they can sit and watch it as it happens around them was the great CNN shots of Belgrade that showed people in a café having their wine and their coffee and saying, "Oh, look, there goes another cruise missile!" In World War II, those people would have been the hell out in the countryside, because the whole town would have been leveled by B-17s. We've reached the point where they just watch missiles go by and they're not worried because they know that we're not after them.

Oettinger: Unless they're in the Chinese embassy. I say this to underscore the point of making intelligence more accurate.

Radabaugh: Now you get to Afghanistan, where we managed to roll up an entire country in three weeks. Notice the differences. We were able to do that with a small number of ground forces, with air power, and with paramilitary forces and the Central Intelligence Agency, as compared to Desert Storm, where we faced a conventional enemy and took half a million people over into the theater.

In all of this, from Afghanistan all the way back to whenever we picked up a rock and beat somebody for a banana, information has been key, because information is what drives you to plan, to decide where you are going to go, what forces you need, where you are going to place this, and what you do next. There is a wonderful concept by John Boyd called the OODA loop. What this stands for is observe-orient-decide-act. That's basically what humans do when they're presented with a situation, and if you can force your opponent to act faster than he can orient himself and make decisions, then you've beaten him, because now you've displaced his center of gravity. That's what IO can do for us: it allows us to get inside that loop.

Oettinger: If you want more details on that, go back to your reading in Coakley.[3]

Radabaugh: That brings us to: What is this thing called IO? For most of us, long ago it was just part of a song about Old MacDonald. (I know, that's a stretch.) In a nutshell, stripped of all the doctrine and crap about it, IO is that you're basically diddling with your enemy's information and information systems while making sure he doesn't do the same thing to you. Because what is information? It's the basis for how people make decisions, and you're really going after the decisionmaker. It's a step in warfare that says, "Yes, you have to worry about the physical forces—the armies, the navies, the air forces—but what you really want to go after is the person who decides to send them somewhere, the person who decides where they're going and how they're going to be employed. If you can get to that person, then you've reached a significant center of gravity".

IO evolved from something called command and control warfare, which back in the good old days of the 1980s and 1990s was the concept of trying to strike at the leadership that commands and controls the opposing forces, on the theory that if you cut off the snake's head the body dies. In this case, it means that if you disconnect the leader from his forces, his forces will become very ineffective and will be unable to coordinate any response to the actions you take against them.

There are a lot of things that we can bring together under the IO umbrella to make that happen: to reach that decisionmaker. Among the things that we can use is deception. We've been doing deception for thousands of years. In this case, the military looks at it as "How can I make this person think I'm going to do something or not do something? How can I make him do something or not do something that will aid my force structure and allow me to achieve success?"

There are psychological operations, or PSYOPs. A lot of people kind of pooh-pooh PSYOPs, because they think of guys throwing leaflets around in the jungle and the people basically saying, "Oh, thank you very much, I was out of toilet paper." What they don't realize is that what you're trying to do is take the prevailing attitudes of a culture, of a people, and turn them so that it's to your advantage. Remember that in PSYOPs and in deception, the preconceived idea is actually the best one to use, because people were already thinking that way. Now, it's your job to spin that and twist it to your advantage.

As I will say later on, the problem that we in the United States have is that our adversaries run the gamut from first-wave to third-wave opponents. We've got the Somalis and the Haitians on one end, and we've got the Serbs on the other end…and, potentially, the Iraqis, the Chinese, and whoever else could be an adversary. We, as the United States, have to be able to contend with that whole range. We can't just say, "We're over here with the more advanced people, because they think like us, they have weapons like ours, they talk on cell phones like us, they use computers like us," because most of the crappy things happening in the world are happening at the other end and we still have to go there and take care of business. That means we still have to put boots on the ground; we have to put people with rifles on the ground; we have to take care of

---

[3]Thomas P. Coakley, *Command and Control in War and Peace* (Washington, D.C.: National Defense University Press, 1992).

things in a very basic way. So we as a military have the challenge of having to be ready for all of this.

Then there is a thing called operational security (OPSEC). That's making sure that the adversaries don't know what you're doing until it happens to them, because, obviously, if they know what you're going to do, then they can make life miserable for you when you arrive at that spot.

Electronic warfare is actually part of IO. You may say, "What do beeps and squeaks have to do with IO?" It's because you're thinking of information in a textual, verbal manner, but information is also electronic. Pulse-repetition frequencies and pulse modulations are information that tells you what is out there, what kind of radar or air defense system you're facing, and what you can do to that air defense situation to make your enemy think you're somewhere else. So, in essence, you're still dealing with information and changing the information that the enemy has to affect their decisionmakers.

Oettinger: I want to take you back once again to underscore the one sentence that touched very quickly on OPSEC. I want to use that as leverage to remind you that the categories he's outlining are not independent or autonomous. You'll recall from reading in my pamphlet the notion that operational security and operational effectiveness are different ends of the scale.[4] The more OPSEC you have, the less effective you may be, because you're denying the information to your own people as much as to the other guy. I'm not quarreling with the list he's rattling off, but just pointing out that this is again one piece of a large web.

Radabaugh: Another piece of that is physical destruction and attack. Shooting things and blowing things up is actually a part of IO, because what you're trying to do is have an effect with that attack, and what this comes down to is a concept that we call effects-based targeting. You're trying to get your military commanders to look at what their requirements are and then say, "What effect do I want to have to achieve my objective?" Before, it was, "Okay, I need to blow *that* up, blow *that* up, blow *that* up, and shoot *that*." Now it may be, "I want to turn *that* off for an hour so that I can get in and out," or "I want to turn the power off somewhere for a short time." It doesn't require blowing things up. What you're now trying to get people to think of is, "What effect do I want to create on the battlefield that will allow me to be successful?" Blowing something up could very well be a part of that, because it could be the best way, or you could be better off using nonlethal means.

That takes us to computer network operations. That's a two-edged sword. You have computer network defense, because you have to protect what is yours, and there's the aspect of CNA, which means you're going out and trying to affect the information in the other guy's computer network. It's nonlethal, although using nonlethal means could have a lethal effect. If you go into an adversary's air defense system and you make the leaders think that their air defense radar says one thing when it says something else, you could fly somebody into a mountain.

---

[4]Anthony G. Oettinger, *Whence and Whither Intelligence, Command, and Control? The Certainty of Uncertainty* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-90-1, February 1990), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/oetting\oetting-p90-1.pdf

Oettinger: Conversely, if you go into Iraq and blow up bridges that carry fiber-optic cables, then you're using lethal means to affect the flow of information.

Radabaugh: There are two other things that round out IO: public affairs and civil affairs. Public affairs basically means news, and that means that you're trying to get out your story about what's happening. As you saw in Kosovo and elsewhere, we do a really crappy job of perception management. We do a really crappy job of fighting the CNN wars, so to speak. So public affairs is presenting the truth about what you're doing and why you're doing it to as wide an audience as possible to counteract all the things that your adversary is saying about you in his propaganda.

Public affairs are a very important part of IO, and so are civil affairs. Civil affairs mean that when you go into a battle area afterwards, or even before, you're helping people with their infrastructure. You're helping people build hospitals, or improve their communications or their sanitation. You're building good will, so that if conflict ever comes you can take your PSYOPs and bring that good will down to earth, and say, "Remember when we were helping you? We still want to help you. We're not against you; we're just against your government." So think of this entire package as dealing with information to affect the decisionmaker, because in warfare you want him either to do something or not do something.

Student: I'm struggling a little bit with some of your laundry list. If, in fact, warfare means coercing your enemy to do your will, at what point do you draw the line? If you want command and control of the commander as the ultimate decisionmaker, can you not define anything as IO in this environment? It seems from your list that IO has its tentacles into everything. I hadn't really looked at it in that way before. What falls outside IO, and reasonably so? Are you talking about physical destruction, influence, civil affairs, PSYOPs? Give me the official pitch.

Rattray: I'll make a stab at this. I've been in a lot of doctrinal discussions and held forth on Air Force and joint doctrine. At the end of the day, you hear that people who are information warfare (IW) or IO advocates are forced into this logical extension of their argument: that all warfare is IO. What I've tried to do consistently for years now is say, "That is not useful in a practical fashion, at least for how the U.S. DOD conducts war," because it immediately gets everybody up in arms. They say, "You IO guys don't own everything. You don't own tanks, you don't own airplanes dropping bombs on Saddam Hussein." Tony mentioned where you start to set boundaries. Physical attacks that go after information flows and systems are an intersection between other forms of warfare and IW. The PSYOPs thing and the public affairs campaigns are also very fuzzy boundary problems. If you talk about managing international public perceptions and the perceptions of leadership elites, again, you're orchestrating a variety of means to cause people to come to different conclusions or make different decisions. IO bleeds upward into all those things. Tony knows, and disciplined me quite a bit when I was doing my work, that setting clear boundaries or being articulate about what your boundaries are is critical in struggling with the set of activities you're trying to organize.

Student: You got where I wanted to go: to expose this issue of boundary making. Is that, in fact, an information process or information system?

Student: Isn't it also part of a larger set of problems? When we talk about physical weapons we talk about discrimination ability, collateral damage, and the persistence of effects. When we talk about PSYOPs or deception or whatnot, those same effects occur. In other words, can you discriminate your target, and how can you prevent collateral damage so that if you're sending out a message it's not poisoning other people? What's the persistent effect of being disingenuous on your long-term credibility? Those are all, I think, real challenges in figuring out how to use these tools to have a long-term effect.

Oettinger: May I suggest that we defer discussion of this? It's a large and very important question. The closest you're going to get in this course to a thorough analysis of this is in your reading of Ken Allard's book.[5] Almost the whole book is about this question. We're not going to resolve it here today, and I think you will be able to discuss it in a much more enlightened fashion after you've read Allard's book and commented on it. I think it is immensely worth raising, partly because it's not limited to IO but is true of any aspect of warfare and of human affairs. It raises the question of "When everything is related to everything else, where do you cut things in a manner that's useful?" Philosophically it's very hard to argue this because everything is related to everything else, and so you have to get on the plane of practical details. If you're going to hear Greg out, we can't pursue that one today. But it's important enough to have been raised, and one whole book, one whole week's reading, will be devoted to essentially this. Look at Allard with that question in mind.

Radabaugh: IO is also an integrating strategy, because technology has now allowed us to take all these things that are happening at once and integrate them for effect. You have the ability to attack systems of systems and have a cascading effect, so now you might be able just to push *here* and have an effect on the center of gravity out *there*.

Again, what I'm trying to lead to is that the U.S. way of warfare is getting less and less bloody. Now we have capabilities to reach out and touch things or influence them without having to kill a lot of people and break a lot of things. Those of you in the military understand that the bottom line of being in the military is that it's your job to go out and break things and kill people, because you're the people they call when everything else has failed. What IO tries to do is get the commanders, especially the CINCs, to think ahead about their area of responsibility, like the Pacific, and ask, "Okay, where are my likely adversaries? What is liable to be a problem in my area?" and start preparing the battlefield now and influencing it so they don't have to fight there. You start the perception management campaign now and affect some place so that you never have to go to war, because you've come to an agreement on policy issues. They don't want to come attack you, and you don't have to defend yourself, or you aren't honor-bound to go defend somebody because somebody attacked somebody who's protected under a treaty of yours. That's where warfare is driving us: to be able actually to meet Sun Tzu's epitome: "The person who can win the battle without fighting is the true warrior." That's where IO is driving us: to be able to win battles before they happen. Now we have the technology and the ability to make all this happen together and coordinate it so that it has a much more synergistic effect.

---

[5]C. Kenneth Allard, *Command, Control, and the Common Defense*, rev. ed. (Washington, D.C.: Center for Advanced Concepts and Technology, 1996).

We've always done IO. Think about it. In World War II we did deception, we did electronic warfare, we did PSYOPs, we did physical attack, we did civil affairs afterwards, we did public affairs, and we had OPSEC. The only thing we didn't do is CNA. What we didn't do as well as we can today is integrate them and control them as a unified whole. So this is nothing new.

Oettinger: But, as you said earlier, measures breed countermeasures, and the whole emphasis on asymmetric warfare and the potential use of bioterrorism is in a sense a reaction to that. The whole information coordination problem, when you think of it in epidemiological terms, becomes humongous. So it's not the end of the story.

Rattray: I have to add a cautionary note, at least from my experience. Certainly our doctrine and our vision are to be able to integrate all the different things that would happen if we were to apply these little pressure mechanisms against an adversary. However, when you, somewhat as academics, put on your "smart people" hat, the measures by which you decide whether somebody is deceived are very different from the measures by which you decide if a stream of bits is flowing through a computer, or if a signal is flowing through the atmosphere. Integrating those different measures of effectiveness into some whole, where you've actually impeded the enemy's ability to make decisions, is intellectually and practically a very difficult problem, and that's where I think we are right now in the broad area of IO. We're getting increasingly good at each of the different things on the laundry list, but it takes a lot of resources and thinking to bring them together effectively for a commander to decide what to do. It's still pretty challenging. That's my assertion.

Radabaugh: That brings us back to, as you say, resources, and my favorite area is intelligence. If you can imagine what we're trying to do with IO, it's a voracious consumer of intelligence. The real impact is that the amount of detail and depth and breadth of information required to do some of these things is just unbelievable.

The best I can equate IO to is special operations. In the good old days, in World War II, they'd say, "Give me a picture of a house," and I'd send over a bunch of B-17s and I'd blow it up. Nowadays, special operations forces say, "There's a hostage in the building. I need you to tell me what the house is made of. How thick are the walls? Which side does the door swing to? Where are the door hinges? What kind of lock is in there? Where is the hostage kept? How many hostage takers are in there? What are their positions? How is the house wired? What explosives do they have inside? Where are they at any minute in time?" It's a much more difficult intelligence question and problem and requires a lot more resources.

If you compare this to IO, there's a computer in the house, and I need to know if it's hooked up to the Internet, which Internet connection it uses, what speed the modem is using, what operating system it's using, whether it's using any firewalls or any personal protection on the computers, what other kinds of security features might be on there, if there is a password on the system, what the password is, and so on and so forth. By the way, to get to this, I need to know what router it's using, what specific chip sets are on the router so that I can go in and affect it, and what the source code is for that—again, an incredible intelligence problem. You're just sucking up more resources trying to answer these questions.

You can't answer it all, so in the intelligence community you're driven to pick and choose. It requires you to prioritize, because the rest of the community out there—the normal people who like to shoot and scoot and do things like that—are still asking you to tell them, "Is the North Korean army prepared to come across the border tomorrow? Are the Indians about to launch their missile, and what is it made of?" On top of this, people are saying, "I need to know the decisionmaker. I need to know who he is, where he went to school, the psychological profile on this guy, who his circle of friends are, who influences him, how I can get to them, where his finances are, and what I can do to them"—much more depth and breadth of information. So the intelligence community is now stretched even more. You're dumping these requirements on the same intelligence community that has been decreased by 40 percent in the last ten years.

Rattray: Can I just make one quick but fundamental point for those who are particularly interested in the cyber warfare dimensions of this? You can technically lay out that map, which is very difficult and very hard to get, and then there is another whole set of things that have to do with who uses those computers to accomplish what actual operational or functional task, which is almost completely a separate question and as difficult to get at as the operating system and the IP [Internet Protocol] address. Is that the library computer, or is that where they order the planes to take off? Out in cyberspace they just come up as IP addresses. You can't tell, and if they're in a different language that adds just another dimension to it, so there are many layers to this difficulty.

Oettinger: I think it's a fundamental question. One of the aims of Greg Rattray's book is to try to fathom where a reasonable dividing line might be between the equivalent of graffiti on the walls and something that brings down the whole country or gets the leadership or the polity to do what you want them to do. It's easy enough to pilot a plane into the World Trade Center. Is that the same thing as bringing down the United States? How many more World Trade Centers do you have to take down before it becomes a strategic attack on the United States as opposed to a terrorist horror? It's a very important question, because, given what Greg Radabaugh has pointed out about the resources consumed, you don't necessarily want to put all your resources into stopping graffiti or washing graffiti off walls, but you really would like to be there if somebody is going to poison the whole population with smallpox.

Rattray: Since you've raised the issue, I would say we're doing it exactly backwards. Right now most of our defensive effort in cyberspace is about getting rid of the graffiti, and very little of it is pointed toward what happens if somebody comes in with a smallpox virus trying to achieve a strategic effect. That's just one person's comment on that.

Radabaugh: That raises a good point. When you're talking about the cyber domain from an intelligence perspective, it's a killer, because the virtual environment is alive twenty-four hours a day, seven days a week, and is constantly changing. If you think of the computers you use here at Harvard, or that you use back at work, every now and then those information technology idiots change something on the system that screws it up or put on new programs or a patch. After all the intelligence preparation you've done on this target, how do you know somebody hasn't gone in and screwed with it between the time you did the intelligence preparation and the time it took you to do something about the target? So you have to do reconnaissance. You have to go back and

touch things. You have to make sure that what you thought was there is still there, because, like a living organism, it's constantly changing.

You need technically smart people to do that. Can we put your Air Force research fellow down as a case officer and have him go out to find human sources who will get us the information that we need? Probably not, because he hasn't studied computer science and technology. He doesn't know to ask, "What's the source code for that router? Where does that router go? Tell me about the operating system in your networks. What version is it? Who's your network administrator?" What we're finding out in the HUMINT world is that we have a lot of smart case officers who are good at going out and getting at people who sit next to the president of Gambia, but they know zilch about the cyber domain. So now you have to find the people who can translate the requirements into people whom you can reach out and touch to get that information. The big question is, "Do you take case officers and train them over again in computer science, or do you go out and find a bunch of tech nerds and make them into case officers?" Big question. They're still wrestling with it, because HUMINT is one of the best sources for this information.

Oettinger: Let me point out to you, in case it's not already painfully obvious, that in the last five to ten minutes of this presentation we've crossed the boundary between things that the authors of what you've been reading so far, like Zegart and Shulsky,[6] would have recognized, and stuff that's in the world that has not been described in the readings to date. These books have not been written, the articles have not been written, the thinking has not been done. You guys have your work cut out for you.

Student: Greg Rattray's and Greg Radabaugh's thoughts kicked off this notion of graffiti. Last time we were gathered we talked about the intelligence requirements deck and how it's really 55-gallon drums. In looking at the U.S. use of cyberwar, or IO, is that a nimble enough, different enough capability that we're energizing to match some of the more detailed requirements that are coming out of the war on terrorism? If you think about our respective commanders, they have grown up in a different legacy system, and they have physical targets in mind, and a reasonable target set and a reasonable solution set for targeting. Doctrinally, could not IO fill some of these burgeoning antiterrorist requirements with more flexibility?

Rattray: Doctrinally, we'd answer that question yes. The problem practically is very difficult. The intelligence community is not particularly familiar with the information feeds necessary actually to do things: to understand what the threat is and to present new opportunities to us. I would say it's not as easy as you think.

Oettinger: What's more, the technology is not a U.S. monopoly. You're talking here about a set of technologies for which the driving impetus comes out of the commercial world and is spread all over the place. It's dual use to the *n*th degree. Indian software houses are among those that put the fixes for Y2K problems in much of the U.S. financial services industry. Indian software

---

[6]Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Dulles, Va.: Brassey's, Inc., 2002); Amy B. Zegart, *Flawed By Design: The Evolution of the CIA, JCS, and NSC* (Stanford, Calif.: Stanford University Press, 1999).

houses also provided the software for the Arab "Olympic" games played in Iraq. This technology is all over the place, and those who practice it are not necessarily our friends.

Radabaugh: Getting back to how well intelligence and cyberspace get along, let me give you an example of how the two sides think. Some of you recognize what is called a BE number: it's like 0124-00010. BE stands for basic encyclopedia. Every physical point on the Earth's surface that the U.S. military has an interest in or has targeted at one point is assigned a BE number.

Student: That's after a picture has already been taken. There is a difference.

Radabaugh: Correct. Somebody has to go and identify it. So what this does is tie your targeting process, your thinking process, on taking military action to physical things like a dam, a building, a bunker, a missile—things that you go out and physically kill. You know where these are.

What's 129.161.00.124? It's an IP address. You may know by going to "Whois" what block of numbers has been assigned where, but you can't tell me exactly where that computer resides physically, because it's out in the cyber domain. So now the intelligence community and the operational community wrestle with: "Do we come up with virtual BE numbers?" That's where you talk about lethal versus nonlethal attacks, because I don't know where to drop a bomb on this. I might be able to do something electronically. I surely can't put a Mark-82 on it, but I know it exists, I know it's part of an adversary system, and I need to affect it.

Oettinger: It gets worse. It may be on U.S. soil, and the question of whether it is legally authorized for you even to know about its existence is a serious one.

Radabaugh: That's right. One of the greatest lessons you can take out of IO is "Bring a lawyer." For those of you who are lawyers, this is a growth career field. You will love it.

Student: In terms of the BE number, is it assigned to a particular image or to the actual things in the image?

Radabaugh: It's assigned to an actual thing. It could be a facility that has multiple buildings.

Student: So you take a picture of a building and it's got a BE number, but in two weeks they build two or three other things or they dismantle it. Is that BE number still valid for that picture?

Rattray: It's still valid for that facility.

Radabaugh: It's assigned to a physical thing, like a bunker. That bunker has a BE number.

Rattray: It's usually a combination of a facility and a function, like the command and control bunker or the space control center, which may be made up of a group of buildings or a single building. Images can come in on a regular basis and update what's contained within that target, but at the end of the day that BE number usually is equated to a target that may require multiple actions to affect multiple things in that target.

Oettinger: This whole argument is a good illustration of why warfighting, like most professions, is an art and not a science. The commander has to make some decisions, whether it's the CINC or some grunt in the field. They're still arguing, but it's only the beginning of the argument, because these things do not have geographic coordinates in them. If you want to relate that number to GPS coordinates you've got another thing going. Then, if you want to take the coordinates in one service's mapping system and relate them to the coordinates in another service's mapping system you have another set of problems. If you're doing a coalition thing and the other guy has an altogether different mapping system, you've got a lot of art going. The notion that technology solves all these problems and provides instant integration overlooks the artistic and professional components that remain in all endeavors. It's critical to remember that. When the press—and the Congress, for that matter—ask for perfection in intelligence or no collateral damage in military actions, they simply don't understand that things are pretty rough approximations of reality. The surgeon tries not to cut through your nervous system but may not always succeed.

Student: We still haven't perfected communications—radio, telephone, et cetera—among the services, much less nations that we're going to be allied with, much less this portion of it.

Radabaugh: Imagine if I were in Kosovo sitting in the Joint Staff in the targeting directorate, trying to get targets validated through the NATO [North Atlantic Treaty Organization] process. You have to worry about fourteen nations saying, "Yes, I like this target. Yes, you can go hit this target." Imagine the time that took!

Oettinger: George Joulwan[7] said he had better luck with the Russians.

Radabaugh: Yes, honest to God.

One final thing I want to bring up in the intelligence aspect of this is the speed at which intelligence is required. It's getting faster and faster. That's part of the U.S. military's way of doing business. Just for the purpose of illustration, look at the good old days when we had the 18th Airborne Corps on the ground against the Soviets in East Germany and you had the line of contact. As an Army officer, I'm basically worried about a 100-kilometer swath, because that's where my enemy is. That's where my front is, and I'm in contact. I'm peripherally interested in all the stuff that's going on behind it, because these are going to be reinforcements that come up and affect the battle in the next day or two. So when do I need to know information? Usually in hours or days, because that's the speed at which things happen on the ground—unless you're doing air assault, but usually that air assault is occurring in this area. Armies only move so many miles a day, so my requirement for having intelligence and imagery quickly is related to the speed at which I move on the battlefield.

Oettinger: John Keegan's book on World War I[8] is fascinating in this particular respect. The railway made it awfully difficult for folks to know where their own reserves were, let alone the other guy's. You can say, "Oh, well, that was 100 years ago and we've got it perfected," but the speeds keep increasing and so the problem remains.

---

[7]Gen. George Joulwan, USA, Supreme Allied Commander, Europe, 1995–97.

[8]John Keegan, *The First World War* (New York: Knopf, 2000).

Radabaugh: For our Navy brethren it's a little different. If I'm a naval officer, I'm worried about this bubble that goes around my warfare group, so I've got to worry about airborne targets coming in, I've got to worry about subsurface targets, and I've got to worry about surface targets that are affecting my ability to do combat operations. I also have to worry about where I'm projecting my forces. For the Navy, with their concept of littoral operations, the bulk of the world's population lives in the littoral, within 100 miles of a coast somewhere. That means that the fleet can project a lot of power and affect a lot of things militarily in that area, so I need to worry about both the fleet and the littoral. That fleet only moves about twenty or thirty miles an hour, so I'm only moving a certain distance. If I'm a Navy commander, what am I worried about in terms of the timeliness of information? Days to hours, maybe minutes if I see something coming in that might be an airborne target. It's getting a little faster.

Oettinger: If you have an engagement against another naval force and need to stop incoming threats, you have milliseconds or less.

Radabaugh: But you know about that force coming in, so that prepares you.

The Air Force, because one of our core competencies is agile combat, can go anywhere in the world, and with aircraft speeds in the hundreds to thousands of miles per hour, we can basically hit anywhere in the globe in a day or so. That means that our information requirements just jumped up dramatically, because at the speeds at which we're going we now to know things in minutes to seconds to microseconds. Again, it's a push on intelligence: "I need to know it now. I need to know it faster."

Now we get to cyberspace, where somebody on one side of the globe can affect somebody on the other side of the globe in nanoseconds. Imagine the indications and warning [I&W] problem of the cyber domain! I am sitting in the United States, I'm worried about all of my computer networks, and I'm constantly getting bombarded by people over there and people here. They're trying to access my networks. How do I tell which one is the hacker and which one is the terrorist or the state-sponsored person? That is a huge dilemma for us, because until we come up with new and better methods and better technology, every time we get attacked we almost have to treat it as a real-life intruder until we can go back and find out who's screwing with our network. So that raises our I&W problem exponentially, because in a conventional sense, if I'm sitting in South Korea and my I&W problem is, "Are the North Koreans going to come south and ruin my day?" I have certain things I can look for. Are there troops massing on the border? Are they shooting rockets across the border? Are their aircraft coming? Those are things that I can see and judge. In the cyber world, everybody who pings my firewall could be a North Korean or a fourteen-year-old kid in California, and who it is determines my legal rights as to what I can do about it. So, again, bring a lawyer.

That takes me to cyberspace, which is the new, sexy part of IO. It's great, and, as Greg Rattray has written in his book, it presents incredible problems and incredible opportunities. The only thing that I will mention as far as IO is concerned is that the cyber domain now allows us never to leave U.S. soil and still to affect somebody around the world—and vice versa. Let me underline this. There are no borders anymore. In the cyber domain, everything is equally distant.

Oettinger: This is the point in this sort of discussion where I want to commit suicide. I think it would be worthwhile to inject a note of optimism into this, because your last remark prompts me to say this is exactly the situation we were in with nuclear weapons. Fortunately, for a wide variety of reasons, not the least of which was intelligence, no nuke has been fired in anger since we dropped the bombs on Japan. During that period, there was the same kind of concern over nuclear weapons and the metaphor of the ten-foot-tall Russian as the hypothetical enemy that scared us half to death. It's important to remember that every problem that Greg Radabaugh has outlined is also faced by an attacker. So if you think of the ten-foot-tall hacker, you're committing the same error as thinking about the ten-foot-tall Russian who did not in fact materialize. It turned out that the ten-foot-tall Russian had feet of clay and blinked first, et cetera.

There's no guarantee that will happen next time, but one of the reasons for the emphasis that you see in my *Whence and Whither* on being better than the other guy and comparing yourself to real human beings with similar problems is that you can scare yourself into paralysis if you look at this set of problems from an absolute point of view. It is not a game against nature, it is not a game against God, it is a game against other human beings who face the same problems when they look at you. If you look at it that way, it is not nearly as suicidal a problem as it appears to be when you just scare yourself. It's no ground for complacency, I might add, but, then again, no ground for despair.

Rattray: Because these challenges are so new, the tendency is to grab or to base your logic on the fairly extreme or the absolutely challenging dimensions of these things, such as "Cyberspace operates at the speed of light" or "There are no borders." However, when you have to start to solve problems and you don't just throw up your hands, you see that there are ways to get a little bit of traction. First, send an e-mail to somebody across the country, and you'll realize that the e-mail does not arrive at the speed of light and the virus does not propagate at the speed of light. There's a big difference between what you need to do to protect yourself if it's nanoseconds or seconds. People can react in seconds; they can't in nanoseconds, so your response has to be automated. Time is fast, but it's not so fast that you can't do anything.

Borders are an interesting issue. Figure out who a hacker is. This is well known practice in the information security community. One way you can tell if a hacker is coming in from overseas is that there's a little function on all your e-mails that tells you how long it is between each hop, and it is noticeably longer if it hops through a satellite. That is a type of border. It is not a border about political sovereignty, but it's a border in the type of transmission mechanism that an attack is running through and therefore maybe a place at which you can set up defenses. Satellites don't exist in such high numbers that you can't try to control them as places to which these transmissions naturally gravitate or make them become bottlenecks for attacks.

Finally, the book[9] places great emphasis on the challenges to attackers, which are exactly the things you want to exacerbate if you're on defense. The conclusion really stresses that although it's difficult to defend ourselves, because the technologies have a lot of vulnerabilities, it is hard to find the attackers, and the attacks move fast, why don't we make the things that are going to be difficult for the enemy—intelligence, as we've been talking about—hard for them?

---

[9]See note 1.

Make it opaque. Make it difficult for them to know who uses what computers for what purposes, so that they can't attack the things that are most important things to us. All they can do is throw hand grenades and run planes into buildings, which is bad and disruptive, but we can still continue to operate.

Oettinger: By the way, Y2K and the first bombing of the World Trade Center [1993] were in a strange way salutary in this respect. Many of the financial services industry folks who lived in those two buildings diversified and learned the lessons that Greg Rattray is talking about as a result of those prior attacks, and therefore were able to continue operations with far less disruption after 9/11 than would have been possible before those events. So measures and countermeasures work both ways.

Radabaugh: That brings up the problem that we run into from the military standpoint. We don't control the United States. An enemy that wants to come in and exploit our vulnerabilities from a cyber aspect looks at the same centers of gravity that we do: leadership, commercial, power, resources, et cetera. All those are owned by private companies or state governments or parts of the federal government. The DOD has nothing to do with it. All we can do is secure our networks and try to get across to these other people that they should secure their networks. That's why the FBI runs the National Infrastructure Protection Center.

Oettinger: You will hear their deputy director, Admiral Plehal, this semester. He's a reserve admiral.[10]

Radabaugh: Because of what has happened in the past, even the commercial companies understand that there are vulnerabilities. Richard Clarke, the president's advisor on cyber security, has said there are many companies out there that spend more on soft drinks for their employees than they do on security for their networks.

So where is the emphasis? I think part of the problem is that there has not been a huge incident, like the World Trade Center, in the cyber world, which has suddenly gotten everybody to say, "Holy Christ! We've got to defend everything!" It hasn't happened. So to them that's still a threat that's way out there that they can push off or maybe just do a few things about now. There are companies that get burned, like Citicorp in 1995, as Greg pointed out as an example, when a Russian ripped them off for twelve million bucks. If that happens enough times, maybe you'll figure out that you need to plug some holes.

Oettinger: I will put on the course Web site the report of the President's Commission on Critical Infrastructure Protection [PCCIP], which expands on what Greg Radabaugh has just said to the *n*th degree. There is more recent stuff, but if you want to flip through something that will give you a picture of this interaction between the civilian and the military, that's the best source I can think of. If any of you can think of a better one, let me know.

Student: Greg Rattray's conclusion states, "Developing strategic information warfare capabilities requires efforts to identify issues and evaluate uncertainties, not react to individual

---

[10]Admiral James B. Plehal addressed the seminar on March 21, 2002.

events and accept simple answers." I'm wondering, did we not in essence do that post-9/11? Perhaps not necessarily just in the information infrastructure area, but decidedly at airports, et cetera, we took measures to affect things that in all likelihood are never going to happen again. We've gone to an extreme where we've ignored other areas. If I were thinking of ways to screw up the United States, my next move wouldn't be with an airplane. I'd drive a truck laden with explosives to a high school football game in Kansas.

Rattray: Remember a few days afterwards, when the driver of that Greyhound bus got killed? That's what I was thinking: Don't go back to the same well. My study of terrorism shows that terrorists do tend to go back to the same well, which is a good thing for us, because we tend to catch them sometimes.

When I watched organizations move into new areas I learned they tend to be event reactive. In the cyberspace area there were a few critical things. An exercise we ran in 1997 called Eligible Receiver and the Solar Sunrise incident in 1998, which turned out to be two Californians and an Israeli teenager, took us up to that next notch, but a lot of our reactions were tuned to those very specific things, not to what I would expect a sophisticated attacker might go after, such as SCADA [supervisory control and data acquisition] systems or the timing and signaling systems in the phone networks, let's say. So that thought is important. Big events are important, though, to focus attention.

The final thing, because I spent time with the PCCIP and a little bit with Mr. Clarke, the existing legal and policy structures for the roles of the DOD and the U.S. government vis-à-vis the private sector in protecting what is arguably a common national asset—the stock market, the ability of airports to function—have changed through U.S. history. While the book goes a lot into one approach, which is the government's fairly hands-off approach to intervening in the private sector to ensure security for everybody, public and private, it is not concrete. It is not written into the Constitution. It is the result of statutory legislation, in other words, a lot of regulatory decisions that can be modified. We nationalized AT&T in both world wars. The provisions that allow the president to do that actually are still in effect. It would be much more difficult without a national monopoly for the government to intervene in the private sector, but while I agree that is probably the proper approach at this point, because I don't think the threat is that high, that is not necessarily the last word on the subject. If you're a policy and legal wonk, there is a lot of fruitful ground to be plowed regarding a more appropriate structure for the government's authorities in this realm, because they're old. The 1996 Telecommunications Act did not even address national security. The 1934 Communications Act did address national security. I would argue (and have) that we got a little bit too laissez faire in attitude toward the government's role in this regard, given the potential downside risks.

Oettinger: A couple of quick comments. As I said, I'll put the PCCIP report on the course Web site. Just for the hell of it, although it's very thick, but you ought to take a look at it, I'll also put the Patriot Act of 2001 on the Web for you. If you have not eyeballed a piece of legislation before, you really should. If you wonder about the metaphor of a camel being an animal designed by a committee, you'll understand it when you read this. Then, lastly, there's a study of the Homeland Security Authorities of the president that was run by a couple of people at a Washington law firm. Those three items, I think, will take these last few minutes of discussion

and amplify on it in a manner that no other reading or earlier sessions this semester will do.[11] So thank you for stimulating that.

Radabaugh: My pleasure.

Let me wrap up with some thoughts about where IO is today, at least from the military standpoint. The personal views of the U.S. military are kind of ambivalent. On the one hand, you have the U.S. Air Force which says, "IO and information superiority are core competencies." Each of the services has established IO centers of excellence, like the AFIWC, the Land Information Warfare Activity for the Army, or the Naval Information Warfare Activity for the Navy. They understand things are going on and they're trying to get a grasp of them. They've written joint doctrine. Joint Pub 3-13 says, "Here's the way we will fight jointly using IO."[12] The services have written doctrine pubs that say, "Yea, verily, this is how we will fight and support these joint operations." The CINCs have IO cells on their staffs that look at IO and incorporate IO into campaign plans.

On the other hand, those IO cells are usually very poorly manned. There's not a lot of effort and talent invested in those, because the CINCs are of that generation to whom proof is a visually pleasing picture of death and destruction. That's real. That's tangible. You know that when you put a bomb on an SA-3 site and it goes away, it's gone. There's no guarantee that an Air Force commander is going to believe you if you say, "Go ahead, fly through it. I took care of the SA-3." He wants to see a smoking hole, because that's the way he's been brought up.

Oettinger: In the good old nuke days, you put one of those somewhere along the Trans-Siberian Railroad and you didn't know whether you had a garage or a decoy unit or an ICBM [intercontinental ballistic missile]. So what's new?

Radabaugh: From my perspective, we're at the point in IO that air power had reached in the 1920s and 1930s, as Greg has written about in his book. We're in that "a few great captains" era, where you have people who can look at the future and see something that is coming along and the great things you can do with it. But nobody's put it together yet. In Greg Rattray you have before you probably one of the few great captains you'll talk about in the years to come for IO, because of the things he has done to develop this doctrine.

Oettinger: Let's hope he doesn't get court-martialed, like Billy Mitchell.

Rattray: Mitchell was a visionary, not much of a doer.

Radabaugh: Where we need to do better in IO has to do with military cultural changes. You have to get past the people whose whole lives have been built on shooting things and blowing things up. There are legal challenges that Greg alludes to in his book and talks about. As an example to show you how ludicrous the legal situation is in the cyber realm, a certain official at

---

[11]The three reports are accessible on-line at the seminar Web site. URL: http://www.pirp.harvard.edu/courses/ISP482_Spring2002/index

[12]Office of the Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3-13 (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 9 Oct. 1998).

Special Operations Command whom I cannot name said that legally it was easier for him to walk up to somebody at a computer and put a nine-millimeter round through his head than it was to touch his hard drive. Is that crazy or what? Think about that. Think about the kinds of cultural and legal changes that we have to make in order to keep progressing down that road of what the public expects, which is less and less bloody warfare and more and more precise warfare.

That leads me to the IO of tomorrow. The military is going to have to learn to shape the battlespace constantly. The key to success in IO is pre-positioning, because it takes time to get a PSYOPs campaign going and to put perception management measures in place—to shape that battlefield and that culture so you don't even have to fight the battle in the first place.

That's why IO has had a rather poor track record to date, because usually the CINCs get into a battle or a war and they turn to the IO guys and they say, "Okay, give me some of that IO shit! Lay it on!" We have to say, "If you had told us about this a couple of months ago we might have been able to do something, because a lot of the techniques and capabilities are very sensitive, very compartmented, and it takes time to put things into place or to execute things." So unless you're thinking ahead and saying, "Here are my potential conflict areas. I ought to have things in place so if a conflict occurs I can end it as quickly as possible with as little bloodshed as possible," IO is going to keep finding itself running and trying to catch up from behind. We need to get that next generation of officers, the ones who will be in charge ten to fifteen years from now, who have grown up with IO so that this isn't a new deal for them. They're used to thinking in terms of lethal and nonlethal effects and effects-based targeting, and then it becomes an everyday component of the military way of doing things. That's when you start hearing them say, "Oh, yeah, I need to have a campaign plan in place now, before the battle even starts."

Oettinger: Before you go on, there are some balances there, too. As he was talking about all that forewarning and laying down of plans, the name that ran through my head was Schlieffen, and the German general staff's plans for World War I. They were exquisite, down to detailed railway schedules, because this was the generation that finally understood railways. The rest is history. The fact that the Germans managed to stay in France for four years was due to other screwups; it was not due to the glorious operation of the Schlieffen Plan. Everything in moderation. Think of the balances and the tradeoffs.

Student: "No plan survives the first contact with the enemy" really is the direct player here. If, in fact, we haven't done the defensive side, as well as the attack side, we could be in terrible trouble.

Oettinger: The point is well taken: planning is necessary unless it's taken too seriously and locks you in.

Radabaugh: An IO plan is a living organism, because you're constantly going to have to update it and rework it. The decisionmaker whom you're trying to reach some place may change in a heartbeat, and now you've got a whole new set of players, a whole new set of dynamics. The mechanisms to reach that decisionmaker may change. Our relationship with that country may change. Take Iran as an example, and suppose the government falls tomorrow. The people have democracy. Suddenly there is an adversary of ours that is an ally again, potentially. Or, for example, suppose South Korea suddenly falls to North Korea. We're not able to save it in time.

Now we have an entire peninsula of a devastated country that's run by a bunch of maniacs using our weapons.

We're having to think about the battlespace constantly and adjust constantly. CINCs and their staffs in years past have been used to putting campaign plans on the shelf. Some of you military folks may recognize the campaign plan for the defense of Korea. In years past, they'd take that out every couple of years and say, "Yeah, we've got the forces right, we've got the flow of forces here right, this picture is right. Okay, back on the shelf. We know that this is the way it's going to work." The IO effort to support this has to be ongoing twenty-four hours a day, seven days a week, constantly changing, to make sure that doesn't have to come off the shelf, or, if it does, that it has the greatest chance of success as fast as possible, because warfare is moving from the macro down to the micro.

Remember when I said it started off with "Nice hambone, Grog, I'll take it"? We moved up to armies in the field and then started moving down to where you had squads in the field. Right now the special operations forces in Afghanistan probably have as much flexibility and firepower as some battalions had in World War II. You start moving it down smaller and smaller. Has anybody seen the movie *Runaway*, with Tom Selleck? The premise behind it was that somebody had built a bullet that they could program for whom they wanted to kill and it would go directly for that person and not see anybody else. Talk about lack of collateral damage! What we've been doing with our precision engagement, our ability to put weapons on a specific target, is move from a point where we're fighting armies down to fighting a person, and that's the decisionmaker. Is it possible that in the future we may actually push that even further, to fighting the mind of that decisionmaker? Maybe we can go in and affect the mind, rather than kill the person or attack the culture to affect those communities. That's kind of where I see IO in the future: heading down to the point where we can go in and say, "We only want *that* person, because that's the person who's going to kick off the war and make the decision that's going to bring people into the conflict."

Oettinger: There is a so-called kinetic solution to that, which is to kill that person, which is currently prohibited only by a presidential directive. So there are choices.

Radabaugh: Let me finish up with what I'd like you to take away from all of this "gerbil on crank" babbling. First off, the ultimate goal has remained the same. You are compelling your adversary to do your will. You want somebody to do something or not do something.

The second thing is that there is no more peacetime. Militaries are used to periods of conflict followed by peacetime, when you ramp down and wait for the next war or conflict to come. What we now have to do as a military is be proactive, look ahead to the next battle and the battle after that and shape the battlefield and battlespace so that (a) the war never comes or (b) it comes on our terms, so that we can end it quickly and decisively in our favor.

The next thing is that we will still be dealing with first-wave through third-wave cultures. We will still be dealing with the Haitis and the Zimbabwes all the way up to the Serbias, potentially all the way up to countries as technologically capable as France, for example, or somebody else who has a really wonderful base of technology and the same ability we've got to put it together. We haven't faced that yet. The closest we came was when we were facing the Soviet Union, but, hypothetically, if relations between us and China, for example, became very

bad in the next ten to fifteen years, they would be an extremely formidable opponent because they would have the same technology, the same outlook, the same ways of dealing with us that we would have of dealing with them. We have to prepare for that as well as for the stone-throwers at the other end of the spectrum. So we're still faced with having to run the gamut with our military of reacting to all these things.

In the information world, all aspects of an adversary are fair game. If you're trying to influence decisionmakers, you're now looking at influencing them through financial networks, infrastructure, and people. Your military has now become the society and the culture, because in most of the places that we face there is one person who decides whether or not to push the button. That is the leader, and that leader is usually a civilian. Under that guise, as a U.S. military, we can target that person, because that person is in essence the commander in chief. All the things you can bring to bear on that individual to influence him to do something or not do something are now fair game, whereas in the good old days all you had to worry about was, "Do you shoot his army or don't you? Do you sink his ships or don't you?" In World War II it was, "Do you blow up his infrastructure or not, to affect his will?"

The next thing is, IO is pretty much in its adolescence. I know I said we've been doing it for a long time, but the technology gives us capabilities to do so much more and we're trying to deal with that environment and that universe of the possibilities. We're in that "great captains" stage that air power was.

Next, remember that IO means more than computer networks. Most people, when you say "IO," say, "Oh, yeah, CNA." Remember, IO includes things like deception, PSYOPs, public affairs, physical attack, electronic warfare, and OPSEC.

We've gone from just bombs and bullets to effects-based targeting. We are now looking at what effect we want to achieve, not at how we kill or blow something up, so now we're forced to think of lethal and nonlethal means.

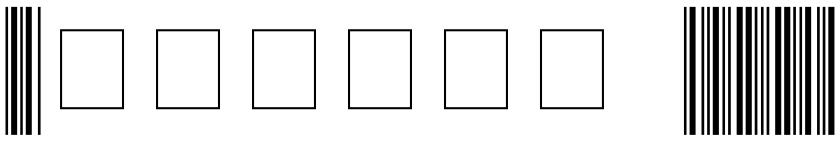
This is nothing new. We have always done IO in parts. Now we have the capability to bring it all together into a synergistic whole.

My last point is: the ultimate capability that we may eventually achieve is to affect the actual mind of our adversary. With that, I say, "Welcome to the twenty-first century, because that's my world."

Oettinger: I want to thank our guest and present him with a small token of our large appreciation.

Acronyms

AFIWC	Air Force Information Warfare Center
BE	basic encyclopedia
CINC	commander in chief
CNA	computer network attack
CNN	Cable News Network
DIA	Defense Intelligence Agency
DOD	Department of Defense
GPS	Global Positioning System
HUMINT	human intelligence
I&W	indications and warning
IO	information operations
IP	Internet Protocol
IW	information warfare
JDAM	joint direct attack munition
NSA	National Security Agency
OPSEC	operational security
PCCIP	President's Commission on Critical Infrastructure Protection
PSYOPS	psychological operations
SIGINT	signals intelligence
USAF	U.S. Air Force



Seminar 2002

ISBN 1-879716-81-X