INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

The Evolution of Intelligence and the Public Policy Debate on Encryption

John M. McConnell

Guest Presentations, Spring 1996
James R. Clapper, Jr; Mark M. Lowenthal; Richard T. Reynolds; Julie J.C.H. Ryan; Arthur K. Cebrowski; John M. McConnell; Albert J. Edmonds; Martin C. Libicki; Robert A. Rosenberg

January 1997

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

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

The Evolution of Intelligence and the Public Policy Debate on Encryption

John M. McConnell

Vice Admiral J. M. (Mike) McConnell was the thirteenth Director of the National Security Agency, a position he held from May 1992 to early 1996. When he led this discussion, he had just become a partner at Booz-Allen & Hamilton, Inc. From July 1990 until May 1992, he served as Director for Joint Staff Intelligence (J-2), and was a member of the Defense Intelligence Agency. His first tour after commissioning with the U.S. Navy was as damage control officer aboard the USS Colleton *in Vietnam. He next worked as a counterintelligence analyst and command administrative officer for the Naval Investigative Service in Japan. VADM McConnell became an intelligence specialist while attending the Defense Intelligence College (now Joint Military Intelligence College) in 1970, and then served in the Pentagon as an analyst and supervisor of CNO Undersea Warfare Intelligence Watch and later as Force Intelligence Officer for the Commander of the Middle East Force on the* USS LaSalle. *In 1976, he became Operations Officer for the Fleet Ocean Surveillance Information Facility in Spain, providing 24-hour real-time intelligence for the Sixth Fleet, and became the intelligence officer for the Commander of the Pacific Fleet (CINCPACFLT) in 1981. Beginning in 1983, he served for two years as Fleet Intelligence Officer for the Commander of the Seventh Fleet. After graduating from the National Defense University's Industrial College of the Armed Forces and earning a master's degree in public administration at George Washington University in 1986, he served for a year as executive assistant to the Director of Naval Intelligence, and then as Chief of the Naval Forces Division at the National Security Agency, prior to becoming Assistant Chief of Staff for Intelligence for CINCPACFLT.*

Oettinger: The last time we had the pleasure of hearing Admiral McConnell speak at this seminar was four years ago, when he described his work as the current intelligence officer for the Chairman of the Joint Chiefs of Staff.

McConnell: First, I find it a little suspicious that I'm invited back. I'm not a real admiral, so I can't wear my sailor suit, and so I wore my navy blazer. The second thing is that I'm speaking on the due date for term paper drafts for which there are no extensions. If I don't make a really good pitch, maybe I can talk Tony into giving whoever is late one more day.

In all honesty, I had a busy last 30 or 40 days, and I really focused on what I was going to do and say on the airplane ride up here this morning. I refreshed myself on who you are, what you do, and read a little about you, some of your projects, and what this course is all about.

I want to spend some time on the public policy debate on encryption. That may sound a little esoteric, but many of you will spend a lot of time and energy thinking about this, so maybe we'll get into some of the issues. But in fairness to Tony's course, and its focus on intelligence, command, and control, and their evolution since World War II, I thought I'd try to share with you the little insights that would be gained by a director of NSA (National Security Agency), someone who is a career professional in intelligence, and how it looks from my vantage point. If you want to dwell on that or ask questions, we'll stay there for a while, but I basically want to do three things. I want to pitch you on the public policy debate on encryption; I want to talk about the evolution of intelligence since World War II; and then I want some good, sharp questions and debate—some give and take. I want to talk about what you want to talk about.

Let me start with World War II and the evolution of NSA. The Brits like to take great credit, and do, in every public forum. But the great success is told by Dr. David

Kahn, in the book *The Codebreakers.** I recommend it to you. It's a fascinating account of what transpired.

The Brits take great credit for having broken Enigma, the German code. If truth be known, we would not have been successful without the Poles. The Poles were codebreakers in their own right. They actually obtained the Enigma machine, or a copy of the machine, and because they knew what was coming, they smuggled it out of Poland and got it to Great Britain, and you know the story of Bletchley Park and the attack on the German codes.

As it turned out, the Germans continued to evolve the technology, and they went from three rotors to four rotors, and basically a robust algorithm that just added more complexity. Now, what do I mean by a robust algorithm? Robustness is defined as: there are no shortcuts. If you're going to break this code, one of two things has to happen. You either have the keys—you know what the combination of the lock is—or you run it to exhaustion.

The attack on Enigma was basically a "run to exhaustion" attack. The first computer was invented in America by cryptographers trying to help the war effort. It was something that was called the Bomb, B-O-M-B. It was done at Nebraska Avenue, and it was operated by women sailors, WAVEs (Women Auxiliary Volunteer Enlistment), as they were called in those days. So as it transpired, what was happening was that the Brits were successful in some of the basics, with the three rotors and even some of the more advanced things, but they couldn't keep up. The requirements for brute force attack to break the code were so massive that they didn't have the appropriate mechanical resources. They needed America's brain power, and its resources, and its wealth and its know-how for success on the attacks.

Now, this is interesting, because in those days America was a target for the Brits. They were attacking our communications. They were breaking our codes. They were trying to know what the President of the United States was doing and thinking and saying to provide advance warning and inside information to their leadership. You may remember the famous Zimmerman telegram, a World War I story, when the Germans were attempting to bring the Mexicans in on the German side, and that subject was addressed in the Zimmerman telegram. The Brits intercepted it. They were successful in breaking the code, and the dilemma they had was sharing it with the Americans. So they falsified the process by which they obtained the telegram and shared it with the Americans to bring the Americans in during the World War I era.

Now, here we are later, in World War II. They're enjoying some success and they are being pounded by the Germans. The convoys, the lifeline that America had established to Great Britain, were losing incredible amounts of men and materiel. Enter America on the scene, the secrets were shared, the Bomb was built at Nebraska Avenue in Washington, and we were enjoying breaking German codes for the remainder of the war. The Navy then had great successes in defeating the German U-boats, after we tried every possible other avenue. When we finally read their communications, and we knew where they were ordered to go and at what time, it narrowed our effort to be where they were at the right time.

It's kind of like precision bombing in the Gulf War. If you look at the history of bombing, we needed thousands of bombs to get some level of damage in World War II, a lesser number in the Vietnam era, and in the Gulf War, it was one bomb, one target. So it radically changed how we have viewed bombing in the history of warfare.

The same can be said for something as esoteric as antisubmarine warfare. If you knew where the submarine was going to go and when he was going to be there, it limited your field of search.

Oettinger: Last year, Bill Owens was speaking of how the dilemma was addressed in that particular situation of using that information over and over again with-

* David Kahn, *The Codebreakers*. New York: Macmillan, 1967.

out endangering the sources.* That must have been a major consideration.

McConnell: It was a major consideration. The folklore—what you will be told by the professionals on the inside—is that Churchill had an incredible dilemma because he knew that the Germans were going to attack a city, and he knew that if he reacted to protect that city, it most likely would tip the Germans off that somehow the Brits were reading their codes. I asked David Kahn, the historian, if that was true. He said, "No, it's totally false. It's without foundation." Now, having said that, as director of NSA, I was frequently confronted, as you'll see in my remarks about public policy on encryption, with questions on the sources and methods we used. What I've found is that there are really serious things that you need to be worried about.

I'll give you some insight, because this was a public effort. In the mid-1970s, NSA had access to just about everything the Russian leadership said to themselves and about each other. A new technology had come along, called a car telephone. The way the technology worked at the time was with a transponder somewhere in Moscow, and everybody talked to the transponder, and the transponder talked to the other party. Well, if you're in the line of sight, it's a pretty simple matter to be able to collect that information. So we knew Brezhnev's waist size, his headaches, his wife, his wife's problems, his kids' problems, his intentions on the Politburo with regard to positions, his opinion of the American leadership, his attitude on negotiations, and on and on and on it goes.

Jack Anderson became aware that we were enjoying that level of success. Virtually every important person in Moscow had a limousine with a car phone, and every time they spoke, we listened. We had people at NSA who knew voice inflection, voice recognition, and it was an amazing opportunity. Jack Anderson published it on Tuesday and it was gone on Thursday, never to be recovered.

So there is a very serious worry about sources and methods. Although I'm told the story about Churchill and the dilemma of the city (Coventry) that was going to be attacked was not true, you always have to factor in how much you are revealing by reacting to this capability. Now that our code-breaking success has become public, historians are starting to rewrite the history of World War II. Some of you Army guys know this better than I. In the famous forced march by Patton, in the Battle of the Bulge—the 100-mile march—he knew he had to be there, or we were going to suffer a tremendous defeat. We knew that because we were reading German communications.

Let me flip to the other side of the war area: Japan. A group of sailors were successful in breaking the Japanese code, called JN-25. We had broken some others, Purple and so on, but JN-25 was the one that was so beneficial to the Navy. The dilemma that Nimitz faced, after Pearl Harbor, was that we knew the Japanese fleet was underway. They had left Japan, and we knew that they were going to strike a major target. That much had been learned through the normal intelligence process. The problem was that they were EMCON. If you're not familiar with that term, it's from "emission control," meaning you don't radiate. The sensors that we had were what is called HFDF, high-frequency direction-finding. If you're not familiar with the technology or with the phenomenon, a high-frequency transmission will be trapped between the surface of the Earth and the ionosphere. It bounces around and so on, and that allows a radio transmission to go around the world. The kinds of communications you're mostly accustomed to today—FM radio, cellular phone, satellite link, and so on—are all line-of-sight communications, so when you use them they go off the Earth's surface and into outer space. HF is how you would communicate with a ship at sea in the days before you had satellites. So when ships went to sea and communicated, you did two things. You would try to hear them, even if you couldn't break the code. By hearing them

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

you could DF—direction find—and know where they were located. If you were successful in breaking their communications, even better.

The Japanese were practicing a kind of emission control that made it very difficult for us to be successful in direction-finding their fleet. We knew they were going to attack again, and the range of targets were from the Philippines to San Francisco and several places in between. So Nimitz faced some hard decisions. He had a fleet that was crippled. He could amass enough firepower to be pretty potent in a very isolated specific case, but he couldn't cover the entire Pacific Ocean. If you haven't looked at a map, the Pacific Ocean is almost half the world's surface. From San Francisco to the Philippines, on a ship, would take you about three weeks if you're steaming fast.

So his dilemma was: "Where are they? Where are they going?" A young cryptologist said, "Sir, I think I have a way to figure out where they're going. Although we're not being successful in our HFDF effort, if we can just get them to talk about the target, they'll say something that will let us understand what it is. Then you can put your force in the right place at the right time. I believe the place is Midway, because I think they're going to start there, and then they're going to work their way back to Hawaii. There is no fresh water in Midway. Any water that comes to Midway is either processed by desalinization, or they've got to ship it in." So he said, "Let's instruct the commander at Midway to communicate in an unprotected, open way that he has a critical water shortage, and request a water supply ship with great urgency." Within 48 hours (actually I think it was 24 hours), they heard the Japanese say, and now as I understand it, this is the way the transaction happened: "The fleet's at sea; it receives an information broadcast from ashore. Therefore there's no HFDF vulnerability in communicating to the ships." But the exploitation effort in Japan and in the islands around Japan heard our commander at Midway say, "I have a water shortage. Send water quickly."

That information was then broadcast from Japan to the ships at sea, saying, "Target X suffering water shortage." Nimitz knew that the answer was Midway. So if you now go back and read about the Battle of Midway, it will tell you about the brilliance of Nimitz in committing his entire Navy at the right spot at the right time, and there's great detail about the torpedo droppers being, basically, a diversion. Most of them were slaughtered, and then the attack by our bombers was right out of the sun and directly overhead. The Japanese had about four carriers, and I think they lost maybe three of them. That was the turning point of World War II in the Pacific. The Japanese never regained momentum for all the men and materiel, airplanes, and ships they lost in that battle.

Now, why do I tell you all that background and all those stories? At the end of World War II, communism was obviously going to be a problem that the United States was going to have to face. Help me, Tony; was it Kennan who did the containment draft?*

Oettinger: Yes.

McConnell: After we debated, the basic word was "containment." The capabilities that we had enjoyed, that had been developed during World War II by OSS (Office of Strategic Services), which became the CIA, and this code-breaking effort (not SIGINT; I haven't used the word SIGINT, which stands for signals intelligence, but COMINT, communications intelligence—and I'll tell you a little bit about the difference later) was challenged because our history had been pretty spotty with regard to intercepting other people's mail. You'll recall the famous statement made by the former Secretary of State** saying something to the effect that "gentlemen don't read each other's mail." Even the successes that we enjoyed in World War I were sustained by only a very small number of people in the intervening years between World War I and World War II. So, at the end of World War II, the State Department

* George Kennan authored the so-called "X Article," published in *Foreign Affairs* in July 1947, in which the doctrine of containment was proposed.

** Secretary of State Henry L. Stimson made this remark in the 1920s.

had an effort, the U.S. Navy had an effort, the U.S. Army had an effort, and each of them said, "We will grow and the others should go away." The first effort was to establish the Armed Forces Security Agency, an amalgam of Army and Navy, and that was a failure. It was basically a fight between the Army and the Navy over who's in charge.

The President had received the benefit of communications intelligence, knowing the stories of World War II. He asked a man named Brownell to lead a blue-ribbon panel to look at the issue. It took him a relatively short period of time, and he came back and said, "Mr. President, this effort is so important that it should be preserved, and it should be maintained at the cabinet level." That's a very interesting conclusion. Most people look at Dr. John Deutch, the current Director of Central Intelligence, as the absolute top leader for intelligence. Brownell said, "This codebreaking can only be the responsibility of a cabinet member." In most administrations in the past, the Director of Central Intelligence has not been a cabinet member. In this case, in John Deutch's situation, he has been made a cabinet member for the same reasons that you and I both read about in the press.

The decision at the time, 1952, was that this person would be the Secretary of Defense. To give the Secretary of Defense the wherewithal to run this thing called the COMINT effort, the United States created an agency and named it the National Security Agency. It was an amalgam of the Army and the Navy efforts, a little bit of what the State Department had, and some civilian corps that had grown up around each of them. Basically, the division within NSA, over its lifetime, has been half civilian, half military. The interesting part of what has made NSA work is what the imagery agency—the thing referred to as NIMA, National Imagery and Mapping Agency—is wrestling with now: it's the construct of their future. What I have recommended to them is to take the NSA model, and at least consider it, because it's a method that has worked. Here's the construct.

In the NSA structure, for the people that they're budgeting for and managing, it's half military, half civilian. If you add up all of the SIGINT expertise in the United States government, you could break it into three pieces. A third of it is military that belongs to the Army, Navy, Air Force, and Marine Corps; a third of it is military that belongs to NSA; and a third of it is NSA civilian. So, I've confused you, probably, with my numbers. NSA budgets for a 50-50 split, but if you look at all the resources, it's one-third, one-third, one-third, with the last third being funded and managed outside of NSA by the services.

Now, why does that work so well? Because a SIGINT soldier who's out with muddy boots with his troops in the field one day, for one tour, in his next assignment will be resident at an NSA field site, or NSA headquarters. He learns a lot about the business of SIGINT. In his next tour he goes back to the Army, or back to the Air Force or Marine Corps, and it's a very beneficial rotation to allow expertise to be learned and used.

I got to be the director of NSA at the end of May 1992. The Cold War ended, for most purposes, in August of 1991, and the thing on everybody's mind was the "peace dividend." The message that I took to the NSA bureaucracy was not warmly embraced. If you look at our history throughout the Cold War, NSA was the fount of knowledge on what's really happening internal to the Soviet Union. If you tracked and understand the Ames case, then you understand what really happened during Ames. By his compromising most of the high-level, well-placed sources in the HUMINT arena, they were either taken away, killed, executed, or they were turned to provide information that the Soviets wanted us to have.

The aspect of communications intelligence that is very difficult to replace in any form is that you are listening to someone speak. You are listening to leadership make decisions and debate issues and so on. So the policy of containment, the experience of World War II, made NSA one of the most protected and coddled bureaucracies in the entire history of the United States government. It was very big: thousands and thousands. It was very expensive: billions and billions. It was protected by a

veil of secrecy. Most people would tell you that NSA stands for No Such Agency, as opposed to National Security Agency. And it had good friends in very powerful positions.

So, an attitude grew up in NSA that I would describe as arrogant. We *knew*, and if you wanted to know, you came to us on our terms, and we would decide what you needed to know and if you had a "need to know." My message to NSA was, as I said, not warmly embraced because, basically, what I had to say to them is, "If we do something useful for the nation and believe that we're doing something useful for the nation, we're going to lose in the budget battles unless we take away the veil of secrecy, unless we open the doors."

So what we decided to do, after some great debate, was a number of things. One was opening a museum. We invited David Kahn, whom I mentioned earlier, in as a resident historian to look at some of the historical data. We took our argument to Capitol Hill and spoke plain English to answer their questions fully and make sure they understood. To make a long story short, in about two-and-a-half to three years of that effort, finally, after eight years of decline, the budget began to turn upward again. The debate now is focusing on what *is* the right level, not "Let's just slash it till it hurts, and take the peace dividend."

The debate now mostly revolves around: What are the future security interests of the nation? What do we need to protect against? What do we need to have early warning on? How many linguists do we need who speak Persian, speak Urdu, or speak Abkhazian or whatever? I'll tell you how many linguists available to the entire U.S. SIGINT system speak Abkhazian: zero. I got a call from the Vice Chairman [of JCS], who was in a heated debate, "What are we going to do about Abkhazia? I really need to know." I said, "I'll get right on it." I said to my staff, "Send in the Abkhazian linguist," and they said, "We don't have one." Then I said, "Well, ask the Army, the Navy, and the Air Force." We asked them, and they didn't have one either. We put it out to the universities like Harvard and other places. They didn't have any either. So we're still looking for our first Abkhazian linguist.

Were we successful in changing bureaucratic behavior? A little bit.

Oettinger: Where the hell is Abkhazia?

McConnell: Oh, it's part of Georgia. Didn't everybody follow the Abkhazian civil war? I thought that was a topic you'd be really close to.

Oettinger: Thank you.

McConnell: I've handed off NSA to one of the right guys at the right time: to Air Force Lieutenant General Ken Minihan. There are some very important issues on the horizon. We have stabilized where we are, and the debate really is not about protection of a bureaucracy. The debate is that there's a service that we provide to the nation, largely unknown to the nation, and we have to answer the question: Do we want to preserve it or not? Should we preserve it?

Let me give you just a couple of examples of what I mean. Americans were at risk in Rwanda. Americans and foreign friends were there when the slaughter was occurring. The commander in chief (CINC) responsible for saving the Americans, for what we call the non-noncombatant emergency evacuation operation, is, of all places, EUCOM (European Command). Stuttgart, Germany, is responsible for Rwanda. So the phone call came in the middle of the night. It took us 10 minutes to get the call, to understand what the requirements were, and it took us about another 30 minutes to start focusing the great sensors of the U.S. intelligence system on the issue. Within 30 minutes we were producing intelligence, and within the first hour we started saving American lives. That's one isolated incident. I use it because it's in the middle of nowhere. But everybody remembers the carnage and the slaughter. There were some Americans there who could have been involved in that if NSA had not been available to answer 911 in the middle of the night.

Bosnia, the Gulf War, Panama, Haiti, international commerce, Middle East peace

negotiations, Russian nuclear weapons, Chinese policy on supporting alien immigration—all of those kinds of issues, regardless of what they are, that the national policy makers or military commanders may be faced with—NSA makes a contribution toward answering the questions. The effort is to get the information, wherever it originates in the world, move it to the person who needs it, at his location, in the form that he needs it, and do that in minutes, if not seconds.

Having had the opportunity, as a Naval Intelligence officer, to use NSA systems for about 26 years and then be the director of the agency for about three years, I'll tell you, it is unequaled anywhere on the globe in its capability. There's tremendous capability that we want to protect—not to the exclusion of making it answer the questions and being subjected to rigor in defending itself and so on. But it is a marvelous capability.

Where is it going today? Where is the future of intelligence? Where is the U.S. intelligence system going?

Oettinger: Before you go on, you made a point that sounded very bland and simple, but I'd like to ask you to elaborate on it the way you did over lunch, about making the information available to anybody who needs it. Also, please elaborate on the question of what that means to folks who might be bypassed when that is interpreted literally.

McConnell: The information revolution, basically, has flattened U.S. business. In the company I just joined, if I want to talk to the CEO, I just hit my e-mail buttons and it's in his office in a couple of seconds, and I frequently will get an answer back in 30 minutes. Now, that is a job security issue. A lot of people who were there before are now gone. There's no staff of secretaries reading and processing all the mail. I went from seven people worried about everything I did—to get me where I was going, informed, and on time. I now share a secretary. I'm probably not as efficient, but I'm either going to learn to get that way or I'm not going to be working there very long. But it's amazing what's happened because of the information revolution.

In the context of information flow, we get some questions from the White House: "I need it faster, because I've got to respond to the press." In the amazing, wonderful system we have, my experience has been that the more senior the people, the first thing they want to know every day is what is being said in the press. I observed this in the Gulf War with the Secretary of Defense and the Chairman and a couple of times in and out of the White House. So, recently, the National Security Advisor had a few of us in, and he said, "How do I make this work?" One of your colleagues here in your class was previously in the Situation Room and can share some insights about how they did it then. Basically, they used e-mail to get information delivered, as I understood it. That went away with the change in administration. The computers went away. And guess what? E-mail's back.

So now young Lieutenant Jones down on the watch has been told by the National Security Advisor, "Here's what I want to know and here's how fast I want to know it." So if you're in Tony Lake's office at any time talking to him, that little chime keeps going off, and he'll look around, and he gets about two sentences so that he knows what's happened, and what he needs to know, and if he's interested, he just hits a button and he'll get the full disclosure. That means it goes from NSA to the White House Situation Room, to Tony Lake, and it takes maybe five minutes. Most of that's brain time, not processing time.

We ran into a situation where I got a call from the Chairman of the Joint Chiefs and he said, "Mike, I know you're the National Security Agency, but why are you getting to the White House ahead of me?" I said, "Sir, I don't understand what you mean." He said, "I'm constantly getting phone calls from the National Security Advisor asking me questions about things that I'm not witting of yet. And so, you're obviously telling them before you're telling me." I said, "Sir, not true; not guilty. We *are* the National Security Agency. We have a lot of customers, from the President to the

Secretary of Commerce, State, DCI, the commanders in chief, and as far as I'm concerned, the soldier in the field, in the foxhole." (We like to advertise that "from the White House to the foxhole.") I said, "When we push a button, it goes to everybody at the same time." And I said, "I'll give you some insights to what's been arranged in the White House. They have empowered (strange word) a watch officer. Now, when it gets there, it goes right to the guy who wants it. Now, sir, there are a lot of people between you and the watch officer in the Joint Chiefs of Staff, in what you call there the NMJIC, the National Military Joint Intelligence Center. There are a lot of filters, and every time you inject a filter, you slow it down."

It was a dilemma for the Chairman because there's the Secretary of Defense, a Deputy Secretary of Defense, the commanders in chief, the JTF commanders in the field, the White House, the State Department, and they're all reacting to the press perception of breaking events. There are hard decisions on very complex issues, and it's hard to get them the same sheet of music and get it coordinated.

What I have found is that the more you use this technology, the less control those down the chain have over the information that goes directly to the top. We have had Russian generals and politicians tell me that what they knew most and understood the best about the old Soviet Union is what they read in the American press. They couldn't get it on the inside. It was always controlled.

So the point that Tony raises, I think, is a good point. For years we were focused on containment; we had "snail-mail," as Tony calls it; and we had a very sharp pyramid. There was the press, but the inside information at the classified level tended to be managed in a way that there was a pace for making decisions. CNN has changed all that. You saw it in the Gulf War. You saw it in Somalia. In my view, we went to Somalia for one reason: the television cameras. We never would have gone there without those horrible pictures of the children who were starving to death. They drove us there. Once we got there, the supposed leadership in Somalia figured out how to get rid of us. Aidid had the same mindset that Saddam Hussein had: "If I can kill 10 Americans, I'll win this war." In his case, he killed 18. In Saddam's case, he couldn't quite pull it off, so we were able to benefit there.

Let me give you just a couple of comments on the Gulf War, and then I'll go into what I want to talk to you about: the policy debate on encryption. I'm a sailor and I grew up doing maritime things. I had an advantage over my Army and Air Force colleagues. The reason is: the U.S. Navy is forward deployed, and our number-one priority was submarines. Antisubmarine warfare is a very esoteric, hard problem. What it meant for me as a sailor was that my number-one target was active seven days a week, 24 hours a day. What I knew about it came from information sources that I did not own and did not control. So it honed my skills in being able to task and use other people's information. From my vantage point, all I did was to try to fuse and correlate data.

There's a term that goes around: "sensor-to-shooter." That's sort of a buzzword for, "All you guys get out of the way, we don't need you. We're going to go from satellite to the guy with the gun." There is a need for that. But it occurs about one-tenth of 1 percent of the time. The other 99.9 percent of the time, you are making a decision. You have to have context. That's what I grew up doing: trying to give context to disparate and varied pieces of information. If you are flooded with data, which is real, which correlates? If you have lots of bits or hits, how do you string a track to get some information? That gave me an advantage. I was forward deployed. I used sensors I did not control. I tracked Russians, which caused me to use those sensors aggressively. I always shot at somebody else or pulled Americans or allied personnel out of somebody else's embassy, but we learned the intelligence business on the Russians.

So it gave the maritime professionals an advantage, because if you think about an army's approach—a ground approach—to the intelligence process, you had two modes of operation: garrison or field exercise. How many senior commanders

have you ever seen subjugate a field exercise with lots of force to intelligence objectives? Ground commanders didn't grow up doing intelligence; they don't like intelligence; and, oh by the way, they controlled the sources and the guys simulating the intelligence part. So, while they had more important things to do, my view is that it caused my Army counterparts not to have the same opportunity that I had as a sailor to make those sensors work.

The reason I'm giving you this background is that we go back to Desert Storm. Major General Jack Leide was the J-2 for CINCCENT in Saudi Arabia. I think he spoke to your class recently.

Oettinger: Yes, he did.*

McConnell: I relieved as the new JCS J-2 five days before the invasion into Iraq and Kuwait, and Jack relieved about the day of the invasion. When I called Jack he was down in Tampa, and I said, "Jack, I know a lot about antisubmarine warfare. What do you bring to this equation?" He said, "I speak Chinese." And that was, literally, how we started this effort. What I found out was that Jack was a great HUMINT, human intelligence, guy. He did super in speaking Chinese and all those sorts of things, and he knew about grunt stuff, but he didn't have any background and know-how on how to make all these national sensors focus on his problem. So we sort of cut a deal. I said, "You take care of the grunt stuff and I'll take care of the national sensors, and we'll try to work this in a collaborative way."

In the joint arena, I went to the intelligence chiefs of service for help, and I was then a Navy captain. I'd been selected for flag, but I had not put it on. Most times when you say "Captain" in the Pentagon, they think Army, Air Force, or Marines, and that makes you the O-3 level. So when I would call somebody, like the Director of Central Intelligence, and say, "Hi, this is Captain Mike McConnell calling," they'd say, "Well, we'll have him call you back." Frankly, the phone never rang. I was learning the ropes.

But here's Mike McConnell, the captain, going to the Air Force intelligence senior leadership, Navy, Army, and Marine Corps, and what I told them was, "I want your best two or three people," and they looked at me like I had two heads. "We're about to go to war here, and you want my best two or three people. You're crazy. You've got all of DIA, you've got 6,000 people. Pick your own people." I said, "No, you don't understand what I'm trying to do here. Remember where I came from—all-source fusion without ownership of any sensor. What I want to try to do is put together a team that will pull the information together to come up with the best picture. Therefore, I want your best two or three guys. Here's my game plan. That person is going to work about 18 hours a day. I'm going to come in at four o'clock in the morning. They're going to make me smart on what they know, after they came in at two o'clock in the morning, and when I go see the Chairman to tell him what's going on, this same person who's gotten me smart will come over and get you smart so you can go speak to your chief. We at least get all the chiefs on the same sheet of music."

With the backing of the director of DIA, that logic prevailed. We finally got it established. We got something we called the JIC, the Joint Intelligence Center, and for those of you who are in the military intelligence business, this will be probably a little more meaningful, but the big change was to make the intelligence community follow the model that had been dictated in the law called Goldwater-Nichols. The operators had been directed, by law, to embrace jointness. It took this crisis in a war to force it on the intelligence side. We established the Joint Intelligence Center and now there are JICs across the CINCs that

---

* See John A. Leide, "Intelligence Analysis in Coalition Warfare," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1994*. Cambridge, MA: Program on Information Resources Policy, Harvard University, January 1995; and "Coalition Warfare and Predictive Analysis" in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1995*. Cambridge, MA: Program on Information Resources Policy, Harvard University, January 1996.

are being rationalized for manpower and so on.

In the old days, you had commanders in chief, CINCs, who were the "have-CINCs" and CINCs who were the "have-not CINCs." If you controlled nuclear weapons, you had lots of resources. If you did not control nuclear weapons, you were in the backwater. So if you looked at an intelligence center like SAC out in Omaha, or folks down in the Atlantic, or out in the Pacific, they had control of nuclear weapons, and their intel support numbered in the thousands. If you looked at CINC-CENT, intel support was numbered in the seventies. Maybe you can get it up to 100. That's a big difference.

So, here's Jack Leide going to war, and he speaks Chinese. He doesn't have the needed robustness, and he's going off to Riyadh. We did a lot of things to establish a JIC, train the manpower, start shipping it out to the Gulf, and so on. The big lesson for me was that the magnificence of the national intelligence effort and all it produced was not received, displayed, or understood by the senior Army leadership. General Schwarzkopf we were able to take care of reasonably well because we had people there who could talk to him. They could sort of force the issue. He was not a pleasant person to brief. We had more than one person thrown out of the room, and some different debates that went on. But the information that was generated from the NSA mission and imagery and all this sort of thing was not getting to the field commanders in a way that they could receive it, understand it, display it, and act on it. Remember I told you the opportunity the maritime guy had that was not shared on the ground side; the Air Force was kind of somewhere in the middle.

We had to make some fundamental changes. At the conclusion of the war, we started changing the character and the nature of how we did this business. That process (without crossing over the border here with some of the more sensitive information) is now underway. The Army has now taken ownership of more of the national resources; so has the Air Force; the Navy had some previously, and they still do. I think we will see better use of information at the point of conflict in the future than we have in the past. I don't know what the 8,000 mile-screwdriver article had to say, but I want a copy when I leave. I suspect what it might say, but I want to take it and read it.

If you read the books on the Gulf War, there was a big schism between Schwarzkopf and Lieutenant General Frederick Franks, VII Corps commander.* Schwarzkopf wanted to go fast. The reason he wanted to go fast was because we were telling him what the intentions of the opposition were. His primary target was going to escape because General Powell had helped construct the debate in a way that caused the President to decide what "success" was. Success was "Iraqis out of Kuwait." So there was a decision, early. We're not going to chase them to Baghdad. We're not going to slaughter them on the highway. So, if they were out of Kuwait, or that area just north of Kuwait, then they were off limits. The Republican Guard was the primary target.

Schwarzkopf was informed in no uncertain terms that they, the Republican Guard forces, were leaving. General Franks had access to the information, but it was never given to him or displayed for him in a way that he could understand it and use it. It was the same for General Funk, who had the Third Armored Division, and General McCaffrey, who was 24th Infantry Division, and on and on. The information was disseminated, but it wasn't received and understood. Therefore, the debate between Schwarzkopf and Franks was over what the Army guys call "deliberate attack," as opposed to going fast. Franks was of the mindset for deliberate attack. Schwarzkopf knew he had to go fast. He ordered the attack 13 hours early. He ordered it to continue, not refuel, and the reason for it was never explained to General Franks.

When I went to see General Franks two years after the war was over, in his office down at TRADOC (Army Training and Doctrine Command), and I explained the

---

* Michael R. Gordon and General Bernard E. Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf.* Boston MA: Little, Brown and Company, 1995.

reason to him, he turned pale. He said, "Nobody's ever told me that before." I said, "Sir, this is what we were telling Schwarzkopf, and why." He said, "Why didn't somebody tell me at the same time?" That's the reason that we changed the character and nature of the Army intelligence support system, and the Air Force, and, to some extent, the Navy, too: to make those folks understand all the national sensors and how they could contribute to the work of commanders in the field.

Student: Was it technology problems or was it just bureaucratic?

McConnell: It's very simple. I grew up using national resources. I knew what it was, how to task it, how to evaluate it, how to depend on it, and how to insist on it. Quite frankly, I was a real pain in the ass as a customer, because if I didn't get what I needed, I'd use my two-star or three-star or four-star, whomever I was working for, to whip up on the system. The system is very sensitive to a four-star saying to his bosses, "They're not supporting me." I knew how to do that, and I was reasonably effective.

My Army counterpart never was put in the situation even to know what it was. He may have had a course; there was Army TENCAP (tactical exploitation of national capabilities). But it's not like being at sea saying, "When are the airplanes coming? I have to launch my ready," or "We've got to find that submarine and counter it."

I remember a discussion when I was working for Admiral Watkins in the Pacific. I was a young officer at the time (this is going back a few years). He turned around, and he said, "Gentlemen, the United States Navy is going to give the President an option that is somewhere between unconditional surrender and all-out thermonuclear warfare." We stood there just waiting for great wisdom to come down on us. We were looking puzzled, and he said, "Think about it. If we're in a showdown nose-to-nose with the Soviet Union, we've got two choices: we either surrender or we go to nuclear warfare. I want to hold their nuclear forces at risk." Now, you know this better than I: about a third of Russian nuclear weapons went to sea on submarines. He looked at me and the other intel guys and said, "You find them." Then he looked at his operators and said, "You counter them. Hold them at risk. And demonstrate that we can consistently do so." So, all of a sudden, I had very clear exercise objectives, only it was not an exercise. It was a noncooperative, real target that I did not control. And the measure of merit was ... I'll change it from submarines, now, to airplanes ... that if Russian airplanes approached a carrier and got within 200 miles, and they were not being escorted, the battle group commander got fired.

Now, on this carrier, do you want to bet the ops and intel guys weren't working this together? Because you were not about to be the guy who got your boss fired. I used to think that the admiral who made that decision (firing the battle group commander for unescorted Russian airplanes near the carrier) was the meanest son of a bitch I'd ever heard of, but later on, I started to think about it. What he really did was to set up a construct that forced us to work together. We talked about it over dinner. We talked about it at the briefing the next morning. We talked about it that night after the movie for the few who had the opportunity to watch the movie.

So, when you think about the maritime context, when the ship sinks, all is lost. So everybody was involved in this effort to make it work and make it work well. I asked my Air Force counterparts on the base, "Where are the operators?" "Well, it's a squadron down on this end." "Okay, where are the intel guys?" "Well, they're over on this end." If you're not right together, then you're in trouble.

Student: I know my boss worked in the "real world" before. He was involved in Panama. He was involved in Grenada. He was involved as the 18th Airborne Corps G-2, and so he's used to tapping into national systems and all that. Despite that, that still didn't sink into him or the VII Corps G-2.

McConnell: For the support structure, and him, in what you just named, Panama, there wasn't that much national contribution. Grenada? The same: no national intelligence resource contribution. We had to use ESSO road maps.

What I'm talking about is a big war, half a million on one side, and half a million on the other side, and how you know where all those tanks are. You've got to know how often I can take your picture, what the system can "see," and what you can expect from the national SIGINT system. For all of that process, not only can you task it, but what do you expect it to do for you? Once it does it, how do you digest it, and how do you hold the system accountable? That's the part that was missing. My maritime intelligence community was judged on it, and, quite frankly, held accountable. I'll say it a different way. One acronym grew up in the community I came from: OPINTEL. That meant operational intelligence. If you grew up as a Navy intelligence officer, and you did not go to sea and identify with an operator, probably knowing about as much about operations as the operations guys, you weren't going to make grade. In the U.S. Army, if you don't command, you don't make it. It's a very different model for Army intelligence. You command as a platoon guy, as a company guy, as a battalion or brigade, and so on. Command. If NSA was a command, it was my first one.

So, do you see the difference in how we just approach life? Where I lived, what I did was use resources I didn't own against a target I didn't control. It's a different culture on the other side, where the success path is command, and you are in a field environment often against a target you do control—again, using sensors that you do own.

Student: Did Schwarzkopf understand the system or were you just force feeding him?

McConnell: A little of both. We offered up his former G-2 as a division commander (now an Army two-star), Chuck Thomas, a good friend of mine, as an assistant to General Leide. Thomas is a guy who kept getting thrown out and kept going back, and he's a general now because of his success. He was picked for that reason.

I'll give you the inside story on General Schwarzkopf's comments after the war. If you remember the headline, it said: "Schwarzkopf says, 'Intelligence was flawed'." That was driven by two things. Just at the crucial hour, it was discovered in an imagery pass that there was what appeared to be a 100-square-mile minefield, and it was smack in the path of where he was going to send 3rd Armor and 1st Armor. It was discovered at two o'clock in the morning. We had "empowered" the imagery analyst to put that information out fast: don't sit on it, get it out there. So, it's out there. Now, he's about to start his attack, and there's a 100-square-mile minefield. When we looked at that imagery over the next couple of hours, we realized, "That's not a minefield, that's a seismic exploration area, and it's only been there for five years." So we quickly cleared that up. It did not leave a positive image in the minds of the field commanders. That was the first thing.

The second thing is that we were having a great debate about battle damage assessment (BDA). Now, there was a big debate among leadership out there. The Air Force leadership (they're all friends of mine), General Glosson and General Horner, were determined to win this war without a ground phase. But the two guys in green suits decided early on that you don't win until a guy with a gun is standing on the dirt. That's Army-speak. They believe that's how it works. So I'm watching this play out. The issue was: Have the Iraqis suffered enough damage so that we can be effective in the ground war, the ground phase of the campaign, without losing a great number of American lives? The Air Force argument was that we can win without the ground phase. At the national level we had some vision of the battlefield, but it was limited. Our vision was mostly driven by imagery and 50 percent of the time the cloud cover prevented one from seeing the ground.

So the construct was that you would have better information forward because

you're flying; we still had the RF-4s there, and A-10s were down low. We were getting a variety of different inputs. Some of the Army Rangers were outdoing recce. So there's lots of stuff coming in, plus anything that could be generated at the national level could be instantly shared at the tactical level. So the arrangement we worked out with Jack Leide was, "We won't try to second guess you. We'll give you the best of everything we can do for you from the national level. You meld it with what you have in the tactical area, and you make the calls, and we'll swear by it."

There was one analyst at CIA who said, "They're lying." It probably was being fueled a little bit by the guys who wanted to win this with just bombs and not ground troops. So this big debate started, when one guy, who had the input to the President's Daily Briefing (PDB), started the trouble. (I don't know if you know how this works, but the President gets an intelligence briefing, put together by the CIA, each morning; it goes to only a very select number of hubs, more today than it did then. Back then it was more restricted. It was probably eight people at the top.) What the little item in the briefing said was, "We cannot confirm by national means the damage levels being reported by the CINC." The President read that and said, "What the hell does that mean?" So he turned to General Scowcroft and he said, "Ask Colin to come over here and explain this." So my phone rang, and General Powell said, "Get your stuff and get up here. We're going to the White House." I took my charts, since I had an inkling what was going on.

So I went in with General Powell. I believe Cheney was there, Judge Webster, the senior military guy at CIA at the time, the PI (the photo interpreter) who made the call, and Scowcroft. So our mission was to explain this. The PI made his case, concluding, "They cannot prove the level of damage claimed. They're going to get a bunch of people killed." And I said, "Now, wait a minute. We don't know that. There's lots of information out there. We've got some information back here," and I flipped out a map and I said, "This is what we can see, which is pretty small, and we can't see that half the time because of the clouds. So you can't make that judgment." General Powell basically let this play out because he was telling Scowcroft that this was not an issue. "I know ground warfare. That army has been sitting there for months. They haven't fired their weapons. They haven't moved. They haven't maneuvered, and they cannot be effective. We're going to go over the top of them."

Everybody was sent away except Scowcroft, Cheney, and Powell. I went back to the Pentagon. As you might imagine, I was somewhat interested in the outcome. My phone finally rang and General Powell said, "You can keep your job. We're going to go with the way it's going now, and CIA is out of the battle damage assessment business for now."

Now everything's copacetic. Schwarzkopf had been made aware of the PDB. He'd been made aware of the discussion with Scowcroft, and then the President. So he was kind of okay. The next day it was on the front page of the *New York Times*. They literally had to pull Schwarzkopf out of the overhead. He just went nuts. I didn't blame him, because here he is trying to make a decision; he's worried that the Marines are going to go fast; he's worried about a flanking movement; he's worried about being second guessed on the loss of American lives. There's debate in his own circles about whether it's even necessary or not. He is committed to this ground war, and he's getting second guessed on his battle damage assessment. So he was very unhappy, I guess justifiably so.

For the rest of the war, that colored his judgment. "You damn intel guys just get away from me!" Then we'd have Chuck Thomas run in and we'd say, "Please, General, listen to this part," and he'd use it, and we'd go on. When Schwarzkopf came back, there was big testimony in front of the Armed Services Committee. Everybody was commenting about how wonderfully our equipment works, and how we made the right investment, everybody's a hero, let's make him a five-star, da, da, da, da. Schwarzkopf was talking about how wonderful everything was, and somebody said, "General, tell us how your intel support

went." And he said, "I didn't think it was very good at all. I had some real problems." That's the only thing that got kept in the press.

Now the two intel committees said, "Hey, if that's true, you've got to come back. Please come up and talk to us." He said, "No." They said, "Well, maybe you didn't hear us. We *really* want you to come talk to us." He said, "No." The third time, they said to Secretary Cheney, "Tell him to come up here or we're going to subpoena him and you." So Cheney said, "General, ..." We had two weeks. So Jack Leide (I helped a little, but mostly Jack Leide) sat him down and did Intel 101: What is a sensor? How does it work?

So, we went back, and Schwarzkopf was gracious enough to ask me to go with him, even though I'd been identified as the "enemy." Remember when he was shown on television blowing up the Scuds? There was this huge secondary explosion. Those were Jordanian tankers, carrying fuel. I took it up to show General Powell. I said, "You know, he was just on TV and he said that he blew up Scuds. These were trucks, not Scuds. Here's the before. Here's the after. They're not Scuds." So General Powell picked up his phone. He had a button for direct dial. And he said, "Hey, Norm, how's it going over there? Har, har." Schwarzkopf is always growling. Powell said, "Well, I just saw you on television. Great show. Mike McConnell says you're all wrong." Here I'm crawling through the floor. So my stock was not real high with Schwarzkopf.

When Schwarzkopf came to Washington, he came by my office and he said, "I'm going to the Hill and I want you to go with me. You don't have to say much. You can chime in. I'm going to testify, but I want my J-2, Jack Leide, on one side, and I want you on the other side." I said, "Sir, I'd be honored."

So, we went up there, and for four hours—two hours in the House, an hour break, and two hours in the Senate—he talked about how wonderful the United States intelligence was. "Never in the history of warfare has a battlefield commander enjoyed such a commanding view of his battlespace. I knew where they were, what their intentions were, how their weapons operated, and what their movements were. I detected them." He just went on and on and on.

At the end of all that, Senator Warner, who's got an interest in intel, said, "General, I appreciate what you're saying. Since this is a closed session, we've been all over the map. We've talked about great secrets. But, we've got a misperception out there that is a disservice to the intelligence professionals in the United States government. I think it would be very helpful if you would make a public statement, unclassified, and we will make sure that it gets in the public record, and we'll try to make it available to all the newspapers that ran the stories." Schwarzkopf said, "I'd be obliged. I'd be very pleased to do that." And he did. I watched every major newspaper for the next two weeks. Not a word. Not a blink. That's just the way it goes. Bad news sells, but good news doesn't.

Now, with that said, I testified probably 40 times as director of NSA, and I would say that in two-thirds of those testimonies a Senator or a Congressman, at one point in the testimony, would say something to the effect, "But General Schwarzkopf said ..." So, you know, once you get that negative image it's hard to reverse it.

I'm rolling along here. Can I switch to the next part?

Oettinger: Yes. Please do.

McConnell: Are there questions or comments or debate? I mean, if you guys hear it and don't agree with it, that's when to speak up.

Student: Sir, I have a question about your telling us about the White House and the watch officer sending off e-mail to Mr. Lake. The problem with that is you have a vast amount of trivia, unless the policy maker actually makes a collection decision: if something comes in on this, this, and this, please tell me. But that seems to be more the exception than the rule.

McConnell: The apparent rule of thumb for Tony Lake was, if it's on CNN, I have

to know. What drove him was the Russian White House affair. The intelligence community was saying, "We're watching it. Nothing is changing, they're not mobilizing. There is no change in the posture of nuclear weapons. They're not bringing troops to Moscow." Lake kept looking to CNN. "Well, for Christ's sake, they're shooting holes in the White House." The intel guys were saying, "Everything's okay. Nothing's happening." There was a big debate at the embassy in Moscow. The ambassador sent a message saying, "Everything's safe here. We all hunkered down in the basement." Lake said, "Well, get out of the basement and look around." What the intel guys were looking at was the traditional, normal military indicators. All the interest was on: "What are we going to do about the Russian army shooting holes in their congress?" And so, Lake said, "I've got to have a way to know what's going on." My response to his request was, "Sir, no disrespect intended, but you're relatively new at this. Those of us who have been doing it for all our lives know how to ask the questions, and the answers are there. We'll tell you a lot of the information or, with confidence, tell you the information is not available." He said, "How do I do that?" We said, "You get a smart, young, watch officer and you tell him what the bounds are."

Does he get them all right? No. Is there a lot of stuff? Yes. But if you do this, over time you develop a feel for it. How long did it take you to get proficient at the White House?

Student: A minimum of a year, sir.

McConnell: And you [speaking to a student] came out of a similar situation in the CNO's office, working it for the Navy. But once you had a year under your belt, you saw the ebb and flow, crisis. You could do it. You must have. Didn't you get promoted?

Student: Yes, sir. I mean, the only difference there was that we didn't send it electronically to General Scowcroft. We ran it up. Paul [Clarke] was there with me* and it was an awful, I don't want to say burden, but it was a tough call. I mean, you could only go to the well so many times, and you didn't want to run up those steps ...

McConnell: Right. The intel professional who can separate the important from the unimportant is what separates the winners from the losers, or the guys who make it and the guys who don't. That's not to say you're always going to get them right, but you develop a sense of confidence in what you know. You know what's knowable. Has Keith Hall spoken to you this year?

Oettinger: Two years ago.**

McConnell: Did he use his argument about the ability to know?

Oettinger: I don't recall it.

McConnell: In the big debate about resources, Keith framed it in the context of the "ability to know." The United States intelligence system has an amazing capability. If the President really cares, or if a tactical guy could command what the President could command, we can tell you the answer with confidence in most of the cases. So it's a matter of getting a feel for it and making it happen. Plus you've got to know well the person you're working for.

The toughest guy I ever worked for, ever, was Colin Powell, because it was too hard to keep up with him. The guy was just too smart, too fast. He just had so many sources of information. I usually would show up a little bit late. He already knew. Now, I was useful to him because I could

---

* David A. Radi, "Intelligence Inside the White House: The Influence of Executive Style and Technology on Information Consumption." Cambridge, MA: Program on Resources Policy, Harvard University, 1996, forthcoming.

** Keith R. Hall, "Intelligence Needs in the Post Cold War Environment," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1994*. Cambridge, MA: Program on Information Resources Policy, Harvard University, March 1995.

tell him that we turned on all the sensors and is there any more we can do? I must have answered that question six, eight or ten times during the Gulf War.

So, you're right, that is a judgment call, but what's the alternative? Not to make it?

Student: I'm curious about your comment about his [General Powell] having many sources of information. Would these sources of information be through the normal channel of information flows or were these ad hoc, informal? Can you describe these informal means of communication?

McConnell: I mounted a great intelligence effort trying to figure it out, but I was not successful. He had a lot of well-placed sources around the government, the press, and others.

Oettinger: There are a lot of histories of the ways of Franklin D. Roosevelt that outline a good deal of that. So you'll get a feel for it by going through good histories of Roosevelt's era and how he played multiple sources.

McConnell: Powell is an amazing man. He's got probably the fastest, most comprehensive, and broadest human mind I've ever been around. He just gets smart people and working with smart people gets them elevated several notches. He could sit in a room with the television on, somebody briefing him, and reading, all at the same time. I used to go in and start briefing and noticed that he's reading and his television was distracting. I'd stop and he'd say, "Go on, go on." Three days later he knew more about what I was saying than I did. He's just an incredible guy.

So there are lots of places, lots of sources, and they were all phoning in. He had several direct lines. The phone would ring, he'd say, "Later," and hang it up. Somebody with a hot tip. He'd pick it up sometimes and say, "Go!" and they'd tell him whatever they had to tell him. People he knew, he trusted, and took inputs from.

Student: Sir, let me ask how you came to terms with your balancing act? We talked earlier about there being more and more information, and getting the information out there. As we go towards more and more combined types of operations, how do we reconcile getting more and more information out and keeping some things secret? I know you go through sanitation processes and those types of things, but historically the intel community wanted to protect their little wickets and dole little parts out ...

McConnell: I hope that the last part of what you just said is not true. It's not true in the world I come from. It's the last thing you'd ever do. You try to create the perception there is no green door. There are sources and methods you have to consider, but the effort is to make it transparent to the user. What you just described, in my view, is the essence of the future success or failure of the United States intelligence community. I describe it in very simple terms: information management.

There is a construct for sensor-to-shooter. I've got a weapon. There's a sensor that can tell me where the target is, and there's no real need for analysis—if the President has placed us at war, and if the beeps meet the criteria and so on. When you're rolling in your tank, and the bad guys are on the other side of the hill, and you come over the hill, and you see them, you're going to shoot them. That's sensor-to-shooter.

My contention is that 99 percent of the time you're not shooting. You've got to manage the information. That's the challenge you're raising. Out of the flood of data, which piece are you going to bother the National Security Advisor about? You're going to be wrong a limited number of times, because they'll get somebody else if you're wrong too often. It comes down to that.

Oettinger: Before you move on to the next topic, just one last gloss on this. I think you also talked about the coalition situation. Who knows what, et cetera? Hold that until the session when "Rosie" Rosenberg will be here. He was in Bosnia recently, and he's noted for telling some

stories on that.* So we can come back to that topic.

McConnell: The technology exists, and it's just like when you lose your credit card. You dial 1-800 and say, "Someone stole it or I lost it," and they wipe it out of the system. Now if somebody uses it, it says, "Reject." The technology exists for us, today, to do that with coalitions. Remember we fought the Gulf War with the Syrians. You've got to talk to them if they're on your side. You don't want to talk to them under different circumstances. So you can turn them off, turn them on. That's being developed in an electronic rekeying kind of a situation where you can dial in, dial out. The big decisions, the tough decisions, today are: How do you share this codeword information? Unclassified level is available to the United Nations. Today, as we speak, the wrestling match we're having is: How do you share it with the Russians in Bosnia? So, whoever is coming can probably can give you some insights.

Oettinger: Rosie Rosenberg.

McConnell: I know a different Rosie Rosenberg, who is retired.

Oettinger: Yes. That's the one.

McConnell: Okay. I know what he means. He did the "go over and take a look" review for Dr. Perry.

Oettinger: Yes, that's him. So why don't you move on to your other topic?

McConnell: Okay. I'll do it. I'll wear you down here a little bit.

I want to introduce the subject you probably thought about in terms of debate just a little bit. In essence, I'm going to give you the same graphic at the beginning and the end.

We're having what I call "the great debate of the next age." If you buy the Tofflers' arguments, there was the agrarian age, the industrial age, and now we're about at the start of the information age. They go on to make the point that you fight with what you use to make your living, from agrarian implements in historical terms to the tanks of the industrial revolution. How you control information will determine your success in future warfare.*

So, as we go down that path, we're going to have to make some hard decisions about what I call the equities debate, and here's what we're trying to reconcile (figure 1). America is grounded on the principle of personal privacy. The government cannot invade your privacy except under very controlled conditions. Those conditions are that you have to be a criminal, or a terrorist, or somebody doing harm to society. You've got to be able to convince someone in the judicial branch—a federal judge or some appropriate judge—that you have probable cause, present your evidence, and get a warrant, and then you can go invade that person's privacy, either by a physical search or by listening to their communications.

So, the issue is personal privacy. Now there's a business case to be made. Did I talk with the larger group about Boeing, or was that at lunch?

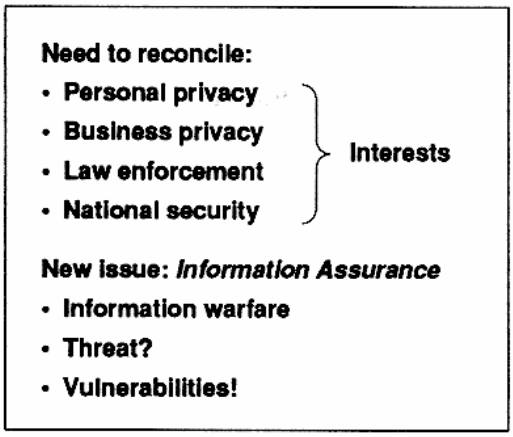

Figure 1
Policy Dilemma

* See Robert A. Rosenberg's presentation in this volume.

* Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston, MA: Little Brown & Co., 1993.

Oettinger: At lunch. You haven't mentioned it here.

McConnell: Let me just give you a quick sea story. Boeing is the largest exporter in the United States. They make, of course, airplanes, among other things. When they built the 747—one of the most successful airplanes ever—one of the most important objectives was to make sure that when the airplane is finally rolling off the production line the front end is aligned with the back end. For every inch that you're out of alignment, you have to counter. As you're assembling the airframe, for everything that's out of balance, you have to use shims. The 747 rolled out about a foot off with about 2,000 pounds of shims.

That was designed on mylar, the modern version of blueprints, and it had a lot of folks measuring it and so on, and that's about as good as they could get it. They decided with the 777 they were going to do it all in CAD, computer-assisted design, in a way that would allow them not only to do the finite measurements, but also to measure a space to see if a human body could fit into it to do maintenance, etc.

Recently I had a chance to visit Boeing, and I asked the integrator of wings and engines, whose database had all this information in it, whether he worries about the protection of that information. And he said, "I don't have anything classified here. We conduct classified business, but that's over in the space division. I have nothing worthy of protection." I said, "When we visited another part of the plant earlier, they told me that you use General Electric, Pratt & Whitney, and Rolls Royce engines." He said, "Yes, sure, we do." I said, "I assume you have all that proprietary data in your system for the integration process." He said, "Sure. It's right here in the database." I said, "If I worked for Rolls Royce, would it be beneficial for me to know what the leading edge technology changes are in a GE or Pratt & Whitney engine?" He said, "Wow, I hadn't thought about that!" Then I said, "Now, a second thing is, if I'm a terrorist, and I cause every fourteenth equation to change a one to a zero, or if I shave everything a certain percentage after a certain number, does that cause your airplane to fly right side up or upside down or crash?" All of a sudden, you could see him get very concerned that this is valuable information. The only difference is that it used to be in a filing cabinet that was locked, and had a guard out front. Today it's digital, so there's nobody in the way of someone reaching in electronically and either changing, degrading, stealing, or just copying the data.

So, there's an argument to be made that businesses have to protect their data. When I grew up, in the industrial age, it was information on paper, locked in a safe, or at least in a secure facility with a fence around it. Today it's digital, and I, as a penetrator, can reach in electronically riding the Internet.

The second part is what I described earlier, called law enforcement. The law enforcement argument is less important to me as a professional, because I never worried about that. As a citizen, yes; but as a professional, all of my interests are foreign. They're all overseas.

Louis Freeh (Director of the FBI) led the charge to enact digital telephony legislation as the phone system went from copper to fiber and computer switches. The ability for the FBI to get a warrant to tap the telephone of a suspected criminal started to deteriorate because the carrier could not provide that service. You couldn't single out the line that the suspected criminal would be using. The FBI asked the carriers to please factor that capability in, put it in up front, and at minimal cost. The carriers said, "We're not required to do it legally; therefore, we're not going to do it." The previous administration started, then decided it was too hard, and handed it off to this administration. Louis Freeh got the job, and he successfully maneuvered through Congress a bill which requires the public switched network (PSN) managers and carriers to put in their software the ability to tap a phone when it's duly authorized by a judge. So there is a requirement for law enforcement to have access under the law of the land.

These issues at the top (figure 1) are the national security implications of this debate. They are what I've been talking to you

about mostly this morning: NSA's role, what we meant in World War II, and what's been happening over the more recent time frame.

What has started to evolve is what we've been debating for about three years. I tried to get Tony Oettinger to take this on as a champion of my solution, and he said, "Do you think I'm nuts?" Now I understand much better, after being involved in this debate for some period of time, why he was reluctant to do that. I'm not sure anybody's got the answer yet. It's going to be the subject of a long, heated debate. But the new issue that's evolving is information assurance. This means just protecting our ability to function as a nation.

Let me ask you kind of a basic question. What's more important, classified data or unclassified data? What would your normal reaction to that be? Guys who have self-selected this class are generally interested in national security affairs, international policy, and that sort of thing, and there are capabilities and things that are protected—nuclear weapons, those kinds of things. So, what's more important, classified or unclassified?

Usually when I ask that question in a military audience, they say, "Classified, no question." I'd say, "Oh, that means it's more important for you to have that secret than it is for the banking system to work? Banking is all unclassified."

If you think about this nation, it cannot function without its unclassified databases. It can function without its classified databases. When you start asking yourself, "What's the more important of the two?" the argument that I would put forward is that I understand the vulnerabilities. I know that because of the world I came from. There's less definition of the threat. One of your colleagues here is writing a paper on the threat, and if his experience is similar to mine, he's having a hell of a time. Is that about right?

Student: I'm definitely having a hell of a time.

McConnell: You're not getting a whole lot of good solid information.

Student: Right.

McConnell: I would offer that there's a reason for that. I came from a world where I focused my time and attention and effort on the Soviet Union. I told you how much time we spent on those submarines. Another part of the mission may be, "Well, if we can't physically kill them, can we cause their system not to work?" and so efforts were mounted to have some influence, to create some confusion, some impact on nuclear command and control. So I have some insight as to what kinds of efforts, energies, and successes might have emerged in a previous life, but that is probably the most sensitive, compartmented, tightly held capability in the U.S. military-industrial complex. Therefore, it's very hard for guys like you, or even a guy like me, with all the sources and resources, to obtain information on this subject because it's very tightly compartmented. My CIA colleagues went out to mount this effort, and they didn't come back with very much data. That does not mean it does not exist, it just means it is difficult to prove.

I understand the vulnerabilities, I know what we can do, and we are not omnipotent. I can only surmise that someone whose interests are inimical to the United States might have similar brain power to come up with the ability to interfere with things that we hold dear. This is the main thought that I want to leave with you (figure 2). If vulnerabilities are real, then threats will grow. I know today what was on my previous slide; this is what I believe about the future. Terrorists are going to figure this out. There was the blind sheik and his terrorists working to blow up the World Trade Center. If the blind sheik had a computer scientist working to do bad things to America, I think the result would have been devastating.

Here's my premise (figure 3).

Oettinger: Let me play devil's advocate, if I may, for a moment. Massive networking, I would say, may or may not make the United States vulnerable, and let me make the argument for the "may or may not" on a logical basis. I haven't the vaguest idea

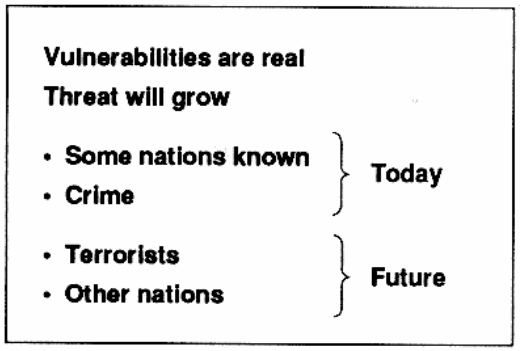

Figure 2

Main Thoughts

empirically which of those statements is true. If you have a very tightly integrated, nonredundant network, then "may" has a high probability of being true. If the network is a very, or relatively, inefficient, highly redundant one with loose coupling, then "may not" is more likely to be true. So it seems to me that this question of how tightly coupled, how redundant the network is, is an important empirical element to see whether that first point is hypothetical or a reality.

McConnell: I had similar worries, and I did some research with some people from NSTAC to look at this.

Oettinger: National Security Telecommunications Advisory Committee?

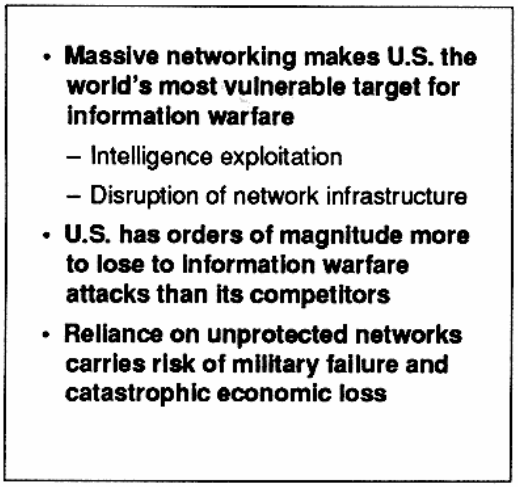

Figure 3

How Vulnerable Are We?

McConnell: Correct. What I learned from them, when I started to dig into this, is that 95 percent of the classified information that drives the U.S. military, that sends their orders, that launches the ships, moves their pay and medical accounts, rides the public switched network. The ability of the nation to conduct commerce rides on the public switched network. So my "massive networking" here is the public switched network. The public switched network is very vulnerable. You will recall that some years ago, on the U.S. East Coast, what was alleged to be a computer glitch (at least that was the way it was described) caused the whole system to go down for some long period of time—I think it was 12 to 20 hours, something in that range. The loss of revenue in that one time frame, only from lost 1-800 service, was $180 million.*

If we were attacked in a way that would take down segments of the public switched network, my view is we couldn't even detect it. The first question we'd have to ask, and we can't answer today, is: Do we even know if we're being attacked? And if we suspect, we don't know who's doing it. That's what I mean here by massive network vulnerability.

Student: Sir, that goes back to the previous question about how vulnerable we really are to terrorists, because my impression of terrorists is that they like high body counts. They like visuals, and they have to have public disclosure of their actions.

McConnell: It would be visible if the stock market collapsed, à la 1929, or if U.S. banking were to suffer that kind of loss, say $300 billion in round numbers, just because somebody scrambled the database. Or, let's take one day's transactions of the U.S. banking system, $1.7 trillion, and most of that flows through New York. If you had the ability to change all the ones to zeros or somehow disrupt it, you could create a situation where confi-

* Francis W. A'Hearn, *Northeast Power Failure and Lyndon B. Johnson: An Interview with Donald F. Hornig, June 30, 1983*, Incidental Paper I-83-3. Cambridge, MA: Program on Information Resources Policy, Harvard University, October 1983.

dence in the ability of the nation to function would start to deteriorate.

Let's make it personal. You put your money in a bank account somewhere. You probably have some kind of electronic transfer. You probably deal very seldom with dollars. Some of you do, but most of your transactions are by credit card or check or something like that. Is that about right? All of that is digital. It's all ones and zeros floating around electronically.

The confidence you place in writing a check to buy goods, or to get some service, is based on confidence in the banking system, and that it will behave the same way you expect it to behave. Now, with 90 percent of the wealth in the banks, there's nothing there except an accounting entry. So if you create a sense of uncertainty, or lack of confidence, the normal behavior for most people is to rush down to the bank and draw their money out. "Give me dollars! Something I have confidence in." There aren't enough dollars. So the only premise I'm making is based on two things. You can impact banking, and you can have a catastrophic economic loss that could carry over to Wall Street and so on. If you could just impact the public switched network, it could cause you to have a massive military failure if you were trying to do something—mobilize, carry out an exercise, or whatever—because 95 percent of our stuff is flowing on the standard public system.

I'm not sure I got all your questions, but maybe as we go through, I can reinforce others as we continue.

Student: What about the DISN (Defense Information Systems Network) and that sort of thing? Are these independent networks, or are they also run on top of the PSN or something like that?

McConnell: That's why I say 95 percent. There are a couple of things that are operated by the DOD, but most are just the standard MCI, AT&T, and Sprint telephone lines.

Oettinger: I think it's important just to clarify a technical point. You have to be very careful about what you interpret as a network. When people say we have this network or that network, most of the references will be to a virtual network. They see this as something that they hold and operate, but the physical infrastructure may well be the PSN. What Mike is saying, quite accurately, is that only a small fraction of all these virtual networks are truly physically independent networks. Most of them are things that are logically built on top of the same physical infrastructure. That was more true of the old-fashioned system than it is now with local area networks and so on, which is one of the reasons why I raised the question of the shifting nature of networks. But that takes us too far afield from where we are at this point.

McConnell: If I could just follow through for a second. When I made this argument that most of our DOD stuff flows on the public switched network, one of the people in the audience said, "But you don't understand. Those are all leased lines." Now to that person, a senior person in the current administration, a leased line meant something physical. He leased a line in Timbuktu and it ran to somewhere else. I had to explain that the only thing you get with a leased line is restoration priority. The phone call may go via Ottawa to San Francisco or via New Orleans to San Francisco. You have no control over that. It's going to go by the path of least resistance. If there's a disruption here, it'll go around. The argument I'm putting forward is that on the public switched network part of the control, the maintenance ports, are vulnerable. One who is properly skilled could go in and cause havoc to perpetuate itself throughout the PSN service.

Student: Sir, I understand everything you're saying there, and I think that my question, and what I heard Professor Oettinger ask, would be whether the systems themselves are now built with any robustness in them. My thinking, without ever studying it, would be that if Ma Bell put this thing together, they were thinking economic efficiency, and they would not necessarily build it with robustness because

nobody told them to build it with robustness, and it makes no sense to build it with robustness because we didn't build this for a terrorist not to break into it. Now, that's just my belief that you're on target.

McConnell: That's exactly right.

Student: But my question would be: Has Ma Bell come back, or is that probably not anything that they really want to talk about right now? Or has the telephone company come back and said, "No, in fact, we did not build any robustness into this, and, yes, in fact, if you did attack this public switched network, we don't see a way that it would be able to back itself up." Or is that classified and you can't talk about it?

McConnell: There are several levels of answer. There was some level of robustness built in. When you say Ma Bell, you're really talking about the old AT&T, and there was a thing called divestiture that caused a total shift around. Remember, not long ago, the secret hideaway for Congress was revealed somewhere in the West Virginia mountains? They had a place to go in case of nuclear attack, and this was called "continuity of government." There was a whole government continuity program. It was laid out. It worked pretty well. We controlled everything.

Divestiture happened. "Oh, my goodness, what are we going to do?" I'm going to give you two acronyms. The first is NCS, National Communications System. The executive agent is the Secretary of Defense. The Secretary of Defense keeps showing up in those because he's the guy for defense. He was given a mission: "If we have a nuclear exchange with the Russians, we still have to communicate. Go make sure that will happen." He looked around and said, "Everything that I depend on is commercial." So he established a group called NSTAC, National Security Telecommunications Advisory Council. They report to the President. The Secretary of Defense reports to the President. So, there is some carryover from the old continuity of government to this collaboration, which has gone on since right after divestiture to make it work.

Enter the information age, when it is less a physical system and more networking with the software and fiber and management of the process with computers as opposed to people in the loop. No more operators.

The advantage I had, in the jobs I've had in the past and the one I had at NSA, was to see what is doable, and understand what one can do today. So I felt an obligation to go make that point to the Secretary of Defense, who sent me to the NSTAC. We made a pitch to the NSTAC about a year and a half ago, similar to what I'm doing today, but I went into more detail. NSTAC has put a lot of energy into this. They are going to try to address those points: Where to from here? How do you provide this level of protection?

Student: It would seem to me that they have a responsibility to the customers to have a little bit of backup in the system, obviously.

McConnell: And they do. There is some.

Student: But there's only a certain level at which they would want to provide for their customers. Obviously, we don't build a bank to keep a terrorist organization out of the bank; we build it safe enough so that an armed robbery wouldn't necessarily happen.

McConnell: Great analogy.

Student: When we're getting up higher here, beyond what our customers expect, and we're trying to build this thing for national defense, then I would expect the national defense to help out a little bit in making this system work.

McConnell: All very good points. You would expect the bank to have a vault and a guard to protect our money. You would not expect a bank to protect your money from a terrorist attack. That's government's role.

Student: Yes, sir.

McConnell: To go back to my first graphic (figure 1), the debate that we're trying to reconcile is balancing what the role of government should be. The money is now stored as a one or a zero in electronic form, and it's accessible right around the guard and right through the vault, so whose role now is it to put up a barrier of protection?

Student: If all of the guys at the table are NSTAC people, folks from civilian infrastructure, without necessarily a focus on national security, but on the common problems that they have as civilian infrastructure, are they going to build paths, are they going to build to a point of national security? Do you understand what I'm saying?

McConnell: That's the debate. It costs money.

Student: How come we don't have defense representatives on NSTAC?

McConnell: We do. The chair is DISA (Defense Information Systems Agency).*

Oettinger: They report to DISA.

McConnell: The executive agent is the Secretary of Defense. The NCS guy is General Edmonds, the director of DISA. I think he's coming to speak to you and you can talk to him.

Oettinger: He's coming next week.

McConnell: When NSTAC comes together, he's sitting at the table. When the NSA guy showed up, my role was to set my hair on fire and say, "Hey, all I'm doing is putting the disparate pieces together to say, 'There's a potential problem here.'" I've been sort of the catalyst to say, "Here's the problem," and not give them the answer.

Oettinger: We're running a little late, so let's move on.

* See Albert J. Edmonds' presentation in this volume.

McConnell: Here's what I think is at risk (figure 4). Others have taken different hacks at this, but my bottom line is that if you do bad things to any of these, it does have a national security connotation. My basic premise is that we're a free-market society, and we depend on a global financial system that works. If the free markets don't work, or the money system doesn't work, then it will impact our ability to sustain ourselves as a nation.*

Figure 4

What is at Risk?

Now let me start making this real (figure 5). I have some classified examples, but I can't use them in this pitch. This appeared in the *Wall Street Journal* on September 12 last year. There was a Russian hacker, Citicorp was the target, and he used international folks. They were successful in moving millions. They actually got out some hundreds of thousands. There's no law against it in Russia. There's no extradition treaty from Russia to the United States. They used Holland as an intermediary point, because the Dutch will not extradite for financial fraud. What it tells me is that if you are in the banking business and your total customer base will bank with you only on the condition of

* How the global banking system protects itself against certain disruptions is sketched in Ethan B. Kapstein, *Governing the Global Economy: International Finance and the State*. Cambridge, MA: Harvard University Press, 1994.

- **Details of CITICORP raid**
  - Russian hacker
  - International actors and venues
  - Millions of dollars moved
  - Hundreds of thousands of dollars lost
- **No wire fraud laws in Russia**
- **No extradition treaty with the U.S.**
- **Dutch won't extradite for financial fraud**
- **Implies problem is widespread**

Figure 5

Wall Street Journal (12 September 1995)

confidence—that it works, my money is in there, I know it's in there, and it will be there when I want it—banks are not about to advertise if people are moving hundreds of millions of dollars (figure 6).

So, a great deal of this problem is that what's known about this problem is in the private sector, and how do you get them to share it? It's like telling your friends you've got AIDS or Alzheimer's or whatever. That may be something you're not willing to share. We're trying to look at this issue in the context of the Centers for Disease Control. How do you set up rules of confidentiality so that anybody who's experiencing a problem can put it in a databank to let us understand how big the problem is?

The Air Force, the Navy, and DISA have attacked government systems to test them. They were successful at about a 90 percent rate, and of all the successful penetrations, they were detected about 2 percent of the time and they were reported about 1 percent of the time. The last time I looked at the numbers, for every 400 penetrations there was one reported detection of penetration. When we started counting the penetrations, it went from hundreds on the first look, to thousands on the second look, to hundreds of thousands on the third look. The Army, Navy, Air Force did about 10,000 each, and they were successful 90 percent of the time.

This is just what I said, in bullet form (figure 7).

This is how I would recommend that you try to think about this problem, because it gets very confusing (figure 8). You all have spent some time and effort on it, but I have found, particularly if you're talking in a public forum, that it gets convoluted very quickly. The issue is information. Most people say information warfare; that's kind of the buzzword right now. When you are saying information warfare, usually you mean you want to control or destroy. We're spending money on building a capability to attack. The Joint Staff's

- **Probably seeing only a small fraction**
- **Incentives to protect banking "confidence"**
  - Suspect banks under-reporting the problem
- **Less urgency felt for R&D, power grids, individual information protection, etc.**
- **We don't know what we don't know**

Figure 6

Tip of the Iceberg

- **Organized crime looting U.S. firms via computer**
  - Russian and others
  - Drug cartels
  - Terrorists
  - Over $5 billion per year estimate
- **International legal structure inadequate**
  - Computer crime not always illegal
  - Cooperation a problem
  - Extradition agreements lacking
- **Risks go beyond financial loss**

Figure 7

Observations

doing the operational part. The services are developing it. But we're spending almost nothing on the ability to protect ourselves from somebody else hurting us. The responsibility for protection, if the information is classified, belongs to NSA. If it's federal unclassified, it belongs to NIST (National Institute of Standards and Technology), and no one has responsibility for commercial or private information. So the issue is protection.

Let me make a point and I'll come right back to you. I'm back to what I showed you to start with: your privacy, your company's privacy, law enforcement when duly authorized, and don't forget the national security context, and we're trying to balance that effort.

Student: Admiral, going to the balance of protection of private resources, the whole debate about the Clipper Chip and the proliferation of private encryption software so that they can protect their own information ...

McConnell: Right. I'm coming to that. I'm going to go quickly here so we can get to these questions.

There are apparent legal limitations (figure 9). I won't say they are limitations, but from the chair I did sit in, and what I think at the moment, the National Computer Security Act of 1987 defines the responsibilities, but the law says that NSA cannot provide support here. It says that NIST may, but NSA cannot. NSA worked to make a contribution by establishing a memorandum of agreement with NIST to lend some expertise to the protection effort.

I'm coming to the Clipper Chip. Part of the political reality facing NSA was the claim that we spied on Americans and, in fact, we did, by the order of the Attorney General, in the mid-1970s. Somebody here in the group had a special interest, which I read about in your backgrounds, in the dilemma of distinguishing between national security, intelligence, and law enforcement. There's a very sharp difference. It's codified in law. The intelligence community can only focus on a foreign target or an agent of a foreign power. The law enforcement people are the only people authorized to target Americans, and they can do that only when they have probable cause and they get a warrant. So there is no spying on Americans by NSA. That occurred in a previous life, at the direction of the Attorney General, and the context was the Weathermen —U.S. citizens—blowing up reserve centers and recruiting centers. The decision

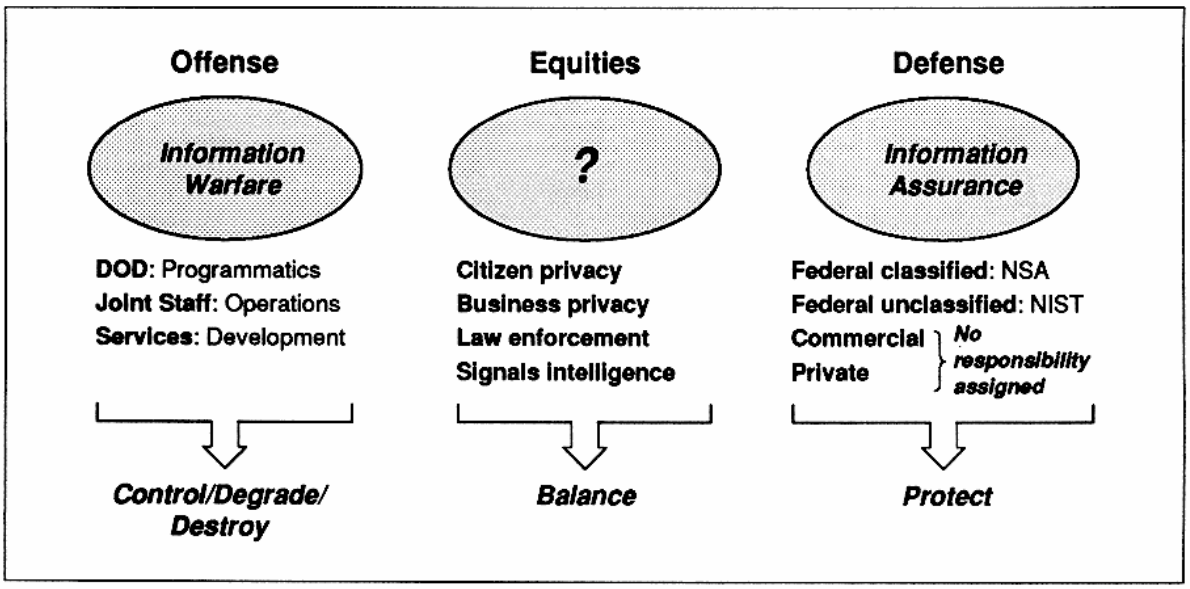

Figure 8

Information

- **PL 100-235, National Computer Security Act of 1987**
  - NSA protects classified and national security information only
  - NIST responsible for all other federal data
  - Does not address protection of critical *public or commercial systems*
- **Political realities**
  - Lingering mistrust of NSA from Church/Pike investigation
  - Negative publicity/reaction to Clipper Chip

Figure 9

Political and Legal Limitation Issues

made by the Attorney General, rightly or wrongly: "That has to be sponsored by a foreign power; therefore, they are agents of a foreign power; therefore, NSA, do this." NSA saluted, as expected, and did it.

I will make a point. I think the tendency of the American people not to trust a large bureaucracy is well justified. It is in the framework of the Constitution and the intent of the founding fathers. A large bureaucracy, left unchecked, without oversight, will do bad things.* Over time, it will eventually make bad decisions. I've witnessed it in lots of places. The fact that we had the Church/Pike Committee hearings in Congress, and it resulted in two oversight committees (as a matter of fact, it turned out to be six oversight committees), is the best thing that ever happened to the United States intelligence system. It holds us accountable. Sources and methods arguments come into play when you can't just go out and tell the public, but you can and you must tell the Congressmen or Senators—in great, excruciating detail. That's what keeps us on the straight and narrow.

The CIA has had its problems recently, and they've gotten the hell kicked out of them because there was somebody holding them accountable. The NSA has had problems going back further and it resulted in Church-Pike. Laws were passed, and that got us back on the straight and narrow.

This is a SIGINT fact or cryptography fact (figure 10). Basically, if you're going to make a cryptographic product, you've got three choices. You can engineer it to be exploitable, or maybe you didn't engineer it to be exploitable, but you made a mistake, and there is some exploitable feature, or it's robust. What do I mean by robust? You've got two ways to get to the raw text: you either have the keys, or you run it to exhaustion. The complexity of the algorithm will determine the work factor to run it to exhaustion. With today's cryptography, it would take about a billion years on the best equipment to run something to exhaustion—on things classified by the United States it would take only about a billion years to break (run to exhaustion). That's what I mean by robust.

Another option is to make it robust, but then escrow the key. You can make an argument for escrowed key in a business sense. If you're a bank, and your employee who's got the keys to what's scrambled got hit by a train, you now need to recover that data. So the argument that is being made today is for key archiving: recover the key, so you can recover the data.

Once you understand this, and you're going to make cryptography, you've got two basic choices: hardware and software. If you make it in hardware, you can escrow the key, and you can do it with confidence. If you make it in software, there's no way currently to bind the algorithm and the escrow feature. We haven't been able to that. Why is that?

These are facts (figure 11). If I'm going to attack something, as the director of NSA, and it's in hardware, it will cost me millions and many man years—usually 20 or 30, something like that. If I attack something in software, we call it a pizza after-

* David Seipp documents this across all American institutions. For instance, the Congress itself at one time put the president of Western Union under arrest in the Capitol for refusing to turn telegrams over to a congressional inquiry. David Seipp, *The Right to Privacy in American History*, Research Report P-78-3. Cambridge, MA: Program on Information Resources Policy, Harvard University, July 1978.

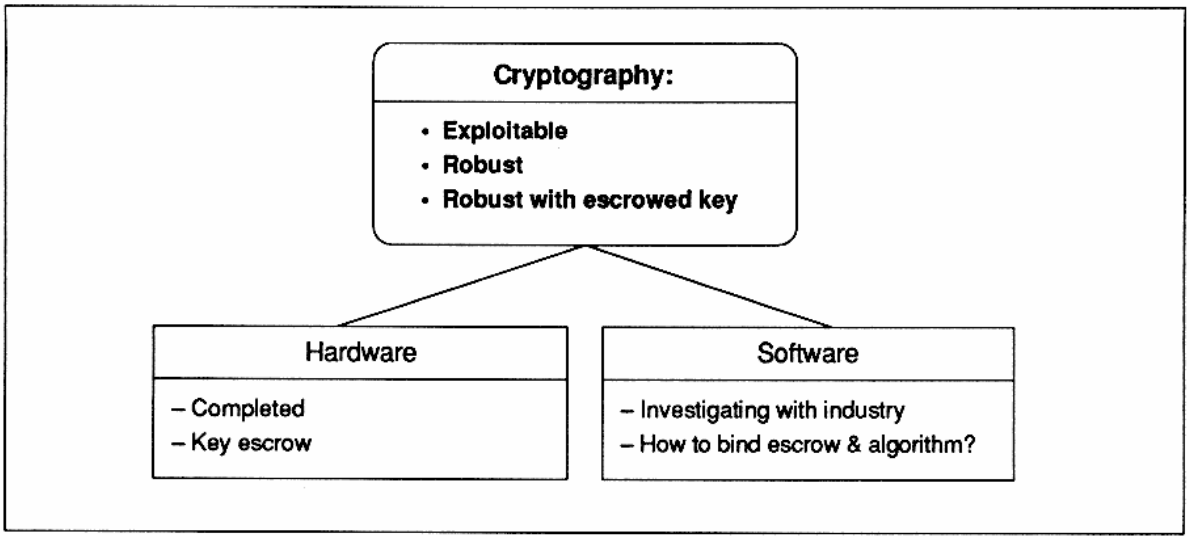

Figure 10

Cryptography

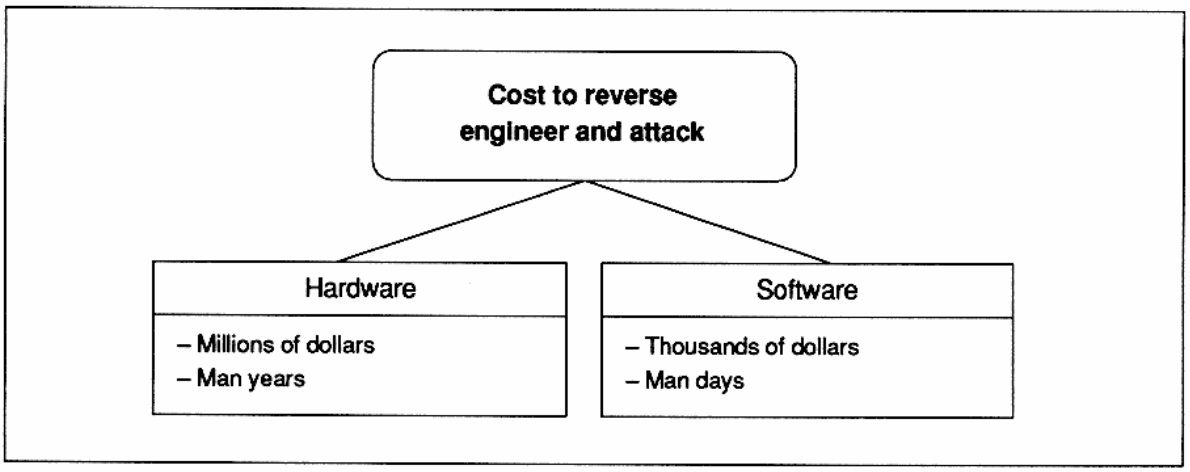

Figure 11

Costs

noon. A pizza, a six-pack and about a thousand bucks and I can reverse engineer it.

When I talked to the Boeing engineer about the hardware versus software debate, I said, "Do you want to protect it on this side (software)? Because I've got people who could penetrate you very easily." It would be just like the 10,000 attacks by the Air Force, 9,000 of which were successful.

Student: Sir, wouldn't you consider that an attack against Boeing to get their proprietary data, by the French or somebody, would be a national security issue because of the economic loss?

McConnell: Yes. You're now getting into the heat of this debate. What the Clipper Chip was intended to do was to start the argument, the debate, on the efficacy of escrowed key. It turned out that the advocates of this seized upon the privacy argument and made this a *cause célèbre* to say that Clipper is evil. Ask those who were

most vocal where they work. Most of them trace their revenue back to the software world. The guys on the other side weren't fussing, because it was a hardware solution. So, when you listen to this debate, always establish the bona fides of the guys making the point.

Now, let me go back to the very first slide (figure 1). The thing I hold most dear on this slide is personal privacy. That's Mike McConnell, the citizen, here. I really believe it. But I also believe that these other things are important, and whatever we do, we have to balance it.

All right, I'll give you just a couple more and we'll quit and take questions.

If you're going to discuss this issue, in my view, it's essential that you capture the first four terms on the slide (figure 12), because if you talk to INFOSEC (information security) professionals or cryptography makers and so on, you quickly go to a level of description and language that's hard to capture. They will use the terms "data integrity," "authentication," "audit" (or nonrepudiation), and "confidentiality," expecting you to understand. So when

Term	Definition/Analogy
Data integrity	Absolute verification data has not been modified *(detection of a single bit change)*
Authentication	Verification of originator *(signature on check)*
Audit Trail	Undeniable proof of participation *(sender/receiver in bank transaction)*
Confidentiality	Privacy with encryption *(scrambled text)*
Availability	Assurance of service on demand *(guaranteed dial tone)*

Figure 12

Security Terms

I've been to the Congress or talk to a large group, I say, "What is data integrity? It is absolute verification that not a single bit has been modified." We can do that today. It's done with cryptography or mathematics. It's a mathematical formula. It's basically the detection of a single bit change.

Authentication. When I am communicating with someone on the other end, can I have confidence that they are who they represent themselves to be? When I call up to the Air Force logistics system and say, "Send the F-117 parts to San Francisco," when we need them in Saudi Arabia, how does the receiver of that know that I really am a legitimate authority? So the cryptographic concept of authentication, like a signature on a check, is very important.

Audit trail and nonrepudiation mean that once you've done this, you cannot deny having taken part in the transaction. The above is doable with mathematical certainty. The technology exists. If I'm in the banking business, or the stock market, or the securities exchange, in my view, the first three are the most important.

All of the debate, all of the fuss, the public debate, has been over confidentiality, which means scrambled data. You can have the first three very easily. If you add this confidentiality or privacy feature, it becomes very emotional. Of course, the last term the cryptographers always use is "availability." But if you're going to address this issue, I'd strongly recommend that you get very familiar with those terms, and when you're talking to someone in a debate, make them explain to you what piece of the argument they're using, and what it is they really are after.

With all that said, this is what the Vice President approved in August 1995 (figure 13). We started with Clipper. Now we've evolved to this stage. The argument we made was that if the information value goes up, the level of protection needs to go up, and at the top would be nuclear weapons. You want to have very high confidence and authentication that it is really from the President. You need data integrity to make sure you've got the right coordinates for your target. Nonrepudiation means that now that you've done this, you can't say,

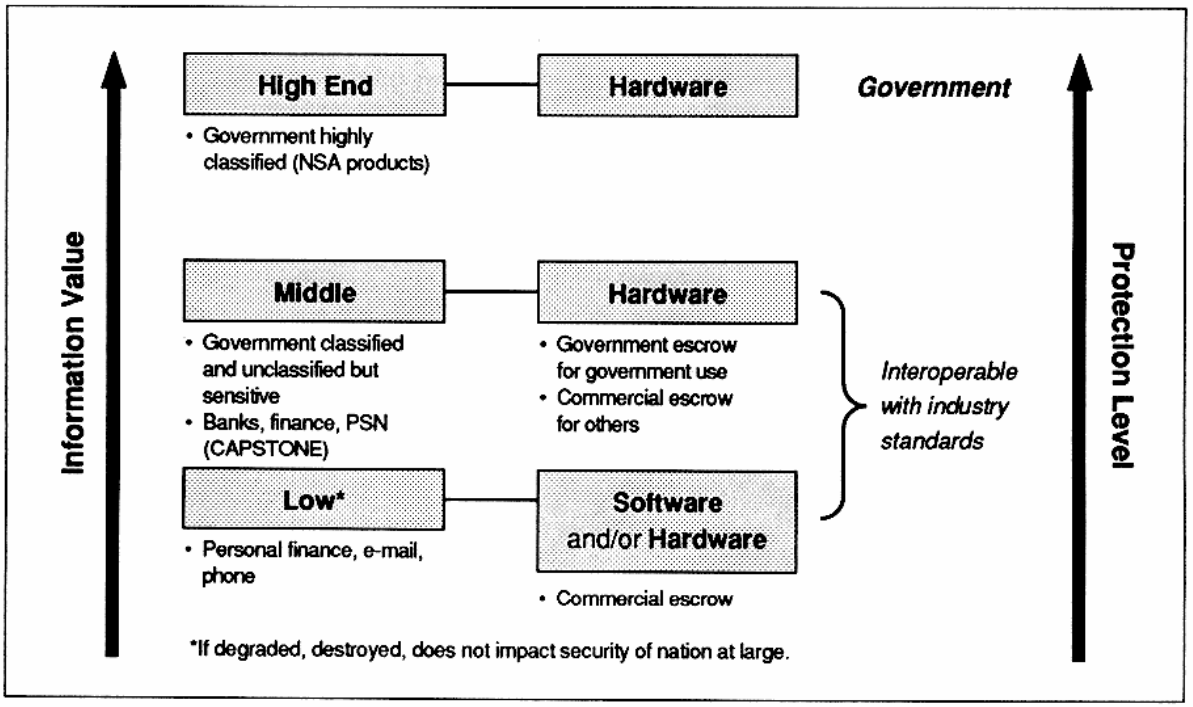

Figure 13

Information Security and Protection

"It wasn't me." And, of course, you need scrambled text.

If it's high end, government classified, NSA produces it. It will be in hardware. There's no argument.

Let's take the middle ground: if it's government classified, or the regular kind of business we are engaged in, or unclassified but sensitive, like the Air Force logistics database. If I'm going to do business at that level, I want to have confidence that the person is who he says he is and so on. So the argument we put forth was that if it's government classified, we want government escrow for government use.

Here's the mistake we made in the Clipper Chip. The Vice President said, "I don't want the executive branch to be the holder of all keys. Heaven knows, we might go through another Watergate. So we want to make sure that some portion of the key, a piece that would be required to break the communications, is held beyond the reach of the President of the United States."

The argument that we made was that for the banking system, the public switched network, whatever, there should be commercial escrow for commercial use. That appeals to hardware makers. Next we said, "We cannot stop this freight train called software. As much as we might like to, in a bureaucratic sense, it is coming. We have to learn to deal with it." So the argument we put forward is that if it's software and/or hardware, some combination, there should be commercial escrow, and it would be used to protect things of lesser importance—my bank account, not my banking system. If my banking system, transferring trillions, is very important to the nation, and I believe it is, we should protect it with hardware. If it's down to me just making a transaction, software is probably good enough. If my business is Boeing, I'd probably want a hardware solution. If my business is providing Boeing with cleaning supplies, software is probably good enough.

When I made this argument, the White House senior person who was working it said, "If NSA will make these two (levels 2 and 3) interoperable, then we've got a construct we can work with." What I asked my technicians was, "Can we take the industry standard, whatever that turns out to be, and make it interoperable with what we call

'Capstone'?" The answer was yes. You can put any number of algorithms on a hardware device. So if you are a citizen calling the Internal Revenue Service and you want to order tax forms, the first questions your devices ask are: "Who are you and what encryption are you using?" If the lower order is software, say DES—the data encryption standard, the industry standard today —it says "DES," and the hardware says: "Thank you very much. Let's engage in a transaction using DES." We've established a key; we have a confidential transaction.

If it were the same IRS computer now talking to another IRS center, exchanging important data, it would revert to the higher-order algorithm. That was what was put forward. That was what the Vice President agreed to.

If we can bring up the lights, I'll tell you what's happened since then. The *Washington Post* carried an article in July of 1995. Basically, the title was something along the lines of "Are We Headed to an Electronic Pearl Harbor?" That caught the attention of Senator Kyl, a Republican from Arizona. He decided to attach to the national defense appropriations bill a requirement for the President to submit a plan to Congress that tells Congress what the President intends to do about what I just tried to describe here.

The President signed it on the 10th of February. It's due the middle of June. In the meantime, those of us who feel passionately about this issue—the potential vulnerabilities and the need to do something about them—have been talking about the importance of it. We've worked it with the director of the FBI. We've worked it with the Attorney General. We've been to the White House. We've been to the Congress. And for some reason (Tony asked me to tell you my views on why that might be, and I'm still searching around for the right answer), all of a sudden, the nation is starting to pay attention. It's appeared in *Time* magazine. It's been written about by Tom Clancy and by Winn Schwartau, *Chaos on the Internet.** A lot of people are starting to focus. I think the nation has matured a little bit in the last couple of years to start to work this issue.

In the White House, there's a big debate over what we are going to do. They started by making a list of how many agencies are working this issue. When they started to make the list it was a line diagram, and it got to 37 feet long. They said, "Maybe there are too many people trying to work this issue," and they called a group together in the White House for a debate on what to do. The decision was: a presidential appointee. The first order of business is to draw a staff from each of the agencies that has a competing interest, and establish a liaison to the private sector— NSTAC, or some representative sample. When we briefed NSTAC recently, we asked them to do it. They deflected it to the Business Council, established in the thirties by President Roosevelt, I think, to bring in industry views. They're trying to establish a forum to bring in the software vendors and other people with different views. But the intent of the presidential appointee is twofold: answer Kyl by the middle of June,* and take about 12 or 15 months to come up with a strategy that says how we're going to address this as a nation.

The issue, bureaucratically, is who's in charge. The Secretary of Commerce is normally in charge of the information infrastructure; OMB is normally in charge of security on the information infrastructure. The big debate within the inner circle has been about the software argument that export controls are making us noncompetitive, and that we have to establish a global,

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

* Editor's note: President Clinton issued Executive Order 13010, *Critical Infrastructure Protection*, on July 15, 1996. Among other provisions, it established the President's Commission on Critical Infrastructure Protection. "... Section 1. Establishment. There is hereby established the President's Commission on Critical Infrastructure Protection ("Commission"). (a) Chair. A qualified individual from outside the Federal Government shall be appointed by the President to serve as Chair of the Commission. The Commission Chair shall be employed on a full-time basis. (b) Members. The head of each of the following executive branch departments and agencies shall nominate not more than two full-time members of the Commission ...."

interoperable standard. What I ask you to consider is that France passed a law that says that no encryption can be used in France that is not approved by the government, which means the government can read it.

What we're trying to solve, what Louis Freeh is trying to solve, in this country about terrorists using unbreakable encryption is the same concern they have in Japan, and I think we had some questions earlier about the group that was doing the terrorist acts. Should they be entitled to unbreakable encryption? Some would argue yes; some would argue no. So, there's a part of the argument that says we're not going to solve this issue by getting rid of export controls and sending our problem abroad.

So this debate is going to go on and on for a while. Is what I call the three-tier approach that I put up here (figure 13) the answer? No. The way the administration has looked at it up to this point is that this may not be it, but it's the only thing I've got, and if a better one comes along, I think I'll know it when I see it. And the debate continues.

Oettinger: Thank you very, very much.

INCSEMINARS1996

ISBN-1-879716-39-9