INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Relationships Between Law Enforcement and Intelligence in the Post-Cold War Era

Philip B. Heymann

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

April 1998

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

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

Relationships Between Law Enforcement and Intelligence in the Post-Cold War Era

Philip B. Heymann

Philip Heymann was confirmed by the Senate and sworn in as Deputy Attorney General on May 28, 1993. He resigned on February 14, 1994, and returned to Harvard University to resume teaching at Harvard Law School, where he is the James Barr Ames Professor, and at the Kennedy School of Government, where he has taught in the Program for Senior Managers in Government. As Director of the Center for Criminal Justice at Harvard, Prof. Heymann has in recent years managed a number of projects designed to improve the criminal justice systems of countries seeking to create or preserve democratic institutions, including Guatemala, Colombia, South Africa, and Russia. In earlier government service, he was Assistant Attorney General in charge of the Criminal Division of the U.S. Department of Justice from 1978 to 1981, Associate Watergate Special Prosecutor from 1973 to 1975, and, in the prior decade, held the following posts in the U.S. Department of State: Executive Assistant to the Undersecretary of State, Deputy Assistant Secretary of State for International Organizations, and head of the Bureau of Security and Consular Affairs. After clerking for Justice John Harlan of the U.S. Supreme Court, Mr. Heymann represented the U.S. government in the Solicitor General's Office from 1961 to 1965. Prof. Heymann was also independent counsel to the National Football League in the investigation of allegations of sexual harassment by the New England Patriots, and he chaired the panel of international experts proposing to the Goldstone Commission new procedures for conducting and handling mass demonstrations in South Africa. He has written extensively on the subjects of management in government, criminal justice, and combating corruption.

Oettinger: We need not say much by way of detail about our speaker's background, since you've all had a chance to look at his biography. I will only say that I'm delighted that my long-term colleague and friend agreed to come and talk to us today on a topic that kind of deals with the hybridization of a lot of issues that in the good old days were somewhat separate. Since he has been not only a scholar, but also a practitioner in this area, his views on a lot of this will be particularly valuable for us.

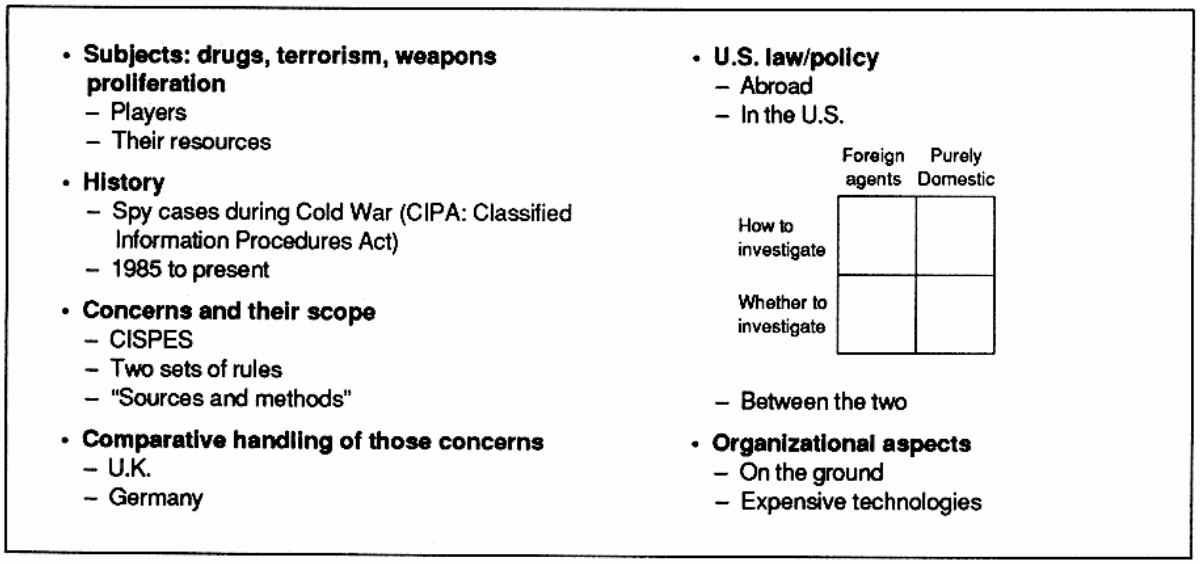
He has agreed, and indeed is eager, to be interrupted with questions and comments anywhere along the line. So saying, Professor Heymann, it's all yours. We've got until four o'clock.

Heymann: Thank you, Tony. I am comfortable with anyone interrupting whenever you want. Some of it's likely to be confusing, so I'd actually prefer that you interrupt if at any point I confuse you.

Professor Oettinger described the subject right, and what I'd like to do with you is take you through the six subjects on the board (figure 1). Maybe I'll walk around as I talk to you. I'm sure that will be more fun for me.

The first subject is the new areas of intelligence: the major areas that have grown up post Cold War. In particular, they are drugs, terrorism, and weapons proliferation. There may be one or two others in there. The National Security Council staff and the CIA would have those things listed now as major intelligence areas along with whatever more familiar national security topics there would be, which would include Iraq, Iran, et cetera.

As I'm going to describe, what's interesting is what Professor Oettinger flagged in his introduction: that these subjects have worked a merger or an overlap of what has traditionally been law enforcement, carried out by one set of organizations under



CISPES = Committee in Solidarity with the People of El Salvador

Figure 1

Agenda

the supervision of one set of cabinet-level officials and under one set of rules, with intelligence agencies that have their own reporting channels and their own set of rules.

Student: Just so that everyone's clear, although these may be subjects that are relevant to other nations, we're specifically talking about these areas within the United States?

Heymann: We're talking about American organizations. For the intelligence agencies, we're talking about the Central Intelligence Agency (CIA), the National Security Agency (NSA), and Defense Intelligence Agency (DIA). For law enforcement agencies, we're talking primarily about the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), and Customs.

Let me take a step back. It's useful, in the broadest way, to think about the country as having two official vacuum cleaners: two official sets of organizations, whose responsibility it is to snatch up information and then to organize it, more or less, for use. Those would be the law enforcement community and the intelligence community. If you wanted to be complete (and it's interesting), you would say that the media are a third major private information-gathering organization that is now working in both of these areas. I know that law enforcement, which I've worked with for a very long time, is very often led by information that comes out of the press. I was at the White House after a military operation and watched them wait for CNN to tell them where the bombs had dropped. So I take very seriously this third great vacuum cleaner of information.

Oettinger: I might add to that a fourth, because it's a little bit early to tell whether it's a fad and populated by trend surfers or something new, and that is open source information with databases, the Internet, and so on.

Heymann: Oh, absolutely.

Oettinger: A lot of folks—the intelligence agencies and others—at least to make a living in that area are claiming that they need to pay attention to that. How much of that is real and how much of it is froth? Do you have a sense?

Heymann: I think it's immensely real. I think it's getting very big, and I think it poses a substantial threat to the bureaucratic interests of intelligence agencies in the United States. Now, the amount of open source information about economies, agriculture, production is very important. It has to be analyzed by government analysts, but it doesn't have to be developed by government operatives in many cases. I think it's a very good addition.

The major sources of information for our intelligence agencies, as you probably know, are photo reconnaissance; signals intelligence, which would mean gathering radio signals and phone signals of various types; human sources, mainly spies; and liaison with foreign governments. The major sources for our law enforcement agencies are not so different in the United States. They would rely on electronic intelligence in a major case, particularly a case that rose to the level of national security in some way: terrorism, weapons proliferation, and drugs—a very big drug operation. They would rely very extensively on informants, the equivalent of human sources. They even have, on a minor scale, the capacities of photo reconnaissance. Law enforcement today would use various airplanes and helicopters and devices like that as part of surveillance, much more than has ever been done in the past. And they, too, are rather actively involved in foreign liaison.

The Drug Enforcement Administration probably has close to 300 agents abroad in the world dealing with the law enforcement agencies of Colombia, Bolivia, Peru, Burma, and Thailand. The FBI would have around 100 or 120 agents. As we're about to see (that's what we're talking about today), the CIA would, at the same time, be meeting with the same law enforcement people, perhaps not telling the FBI and the DEA when they were doing it, as long as the subjects were of equal interest to the intelligence world, which has lost its main target with the end of the Cold War, and to law enforcement.

But let me move to the history.

Oettinger: Before you do—and perhaps it's a question you may want to note on the board, or develop later—you've indicated that the FBI might be doing this and the CIA might be doing that without either of them knowing what the other one was doing. During the period when, say, J. Edgar Hoover was director of the FBI, there was a fairly general belief that noncommunication between these agencies had to do with personality, and God knows there was plenty of justification for that, given the personalities. But it has persisted, and in your paper[1] one gets more of a sense that it's kind of endemic: that it comes with the territory and is not that much a matter of personality. I'm wondering if you could either now or later comment on that.

Heymann: Let me comment on it a little now and then get back to it at the end. I think relations between these organizations and between their leaders obviously do have their ups and downs, but they're different types of people, and there's a lot that's endemic. Police officers generally come from working-class backgrounds. They generally have a very conventional and a quite good sense of values. They believe that it's very important to keep right from wrong and separate them and deal with them differently. Traditionally, intelligence people have had much more education; they're more likely to come from universities. They have been more middle class or upper middle class. What happens is that there's a certain amount of resentment that flows back and forth in a situation like this, as there's a certain amount of resentment that flows between prosecutors and law enforcement people. They've also sniped at each other. There's been a certain amount of fighting for territory.

The history begins with the birth of the CIA in 1947. It seems to me to be a great victory of civil liberties that in the charter of the CIA, amended last year, it was written that it would undertake no action in the interests of law enforcement at all. Now I thought that was rather nice, as a matter of

[1] Philip B. Heymann, "Domestic Intelligence Gathering and Processing Within the United States," chapter in his forthcoming book on terrorism.

civil liberties: keeping our intelligence agencies out of our domestic hair. But the fact of the matter is that it was J. Edgar Hoover writing in a provision that said the CIA should not go near the FBI's jurisdiction, and he was powerful enough to get it in. So, sometimes bureaucratic self-interest works well.

At the time of the Aldrich Ames affair, relations between the two organizations hit a temporary nadir. The CIA had been shamefully negligent as he operated as a mole/spy for years before that, but in the years 1993 and 1994 they were working very well and very closely together with the FBI to catch Aldrich Ames. But no sooner was he caught than the FBI turned over to the congressional intelligence committees a very long book of what the CIA had done wrong to allow this to take place—hundreds of pages of a book that the FBI had been writing all along. The CIA was very resentful of this. The CIA was on its knees and about to have people hit it on the head with a baseball bat, and the FBI was providing a whole new set of baseball bats to the Congress.

We'll go back to that topic of relations between the agencies. It depends a lot on who the directors are, and things like that.

So, let me get you into the history. The CIA, having been forbidden to work in the law enforcement area, had no desire to work in the law enforcement area in the years between 1947 and the collapse of the Soviet Union. It saw its job as protecting the interests of the United States abroad against national security threats, at a time when the national security threat was quite easily identifiable, and that was communism.

The FBI had the responsibility for the internal security of the United States. Unlike almost every other country in the world, we have no separate internal security agency. The British have MI-5; the Germans have something called "The Committee for the Protection of the Constitution." We just have a single law enforcement agency, which also is responsible for espionage and terrorism cases. That's the FBI. They had that responsibility but, basically, the subject of law enforcement was within our borders and, other than an occasional spy case, law enforcement was about matters that were exclusively for the FBI: thefts, murders, kidnappings, robberies. The CIA was required to work only abroad, so there was a jurisdictional separation. Its subjects of interest were the military capacities of the powerful communist nations. So, there was no overlap, except for espionage cases in the United States, and there the overlap always created immense trouble.

CIPA (figure 1) stands for the Classified Information Procedures Act of 1980. I get the credit for that, and it turns out to make me very popular in the intelligence world. When an espionage case would come up, the investigators, having put a lot of work into catching a spy, would very much want to have the spy tried and punished. The intelligence agencies would be a little bit embarrassed by the spy who was caught, but more important than that, would fear what the criminal justice system would do in terms of revealing secrets at the trial of the spy.

They had very different purposes. The purposes of the intelligence agencies were to protect our national security and give policy advice to the President.[2] Their purpose was not to arrest and punish, and they saw a distinct threat to "sources and methods"—the crucial words. That's what they care about. They don't care about the substance of what they've learned. That's not a terrible secret. Let's say they've learned the Iraqis have a new weapon. It doesn't matter that anybody finds out (they could, but they don't, generally) that we know that Iraq has a new weapon, but it matters *how* we found out. The intelligence agencies care very much about protecting that, and that was always at risk whenever there was a spy case.

Oettinger: By the way, this is with good reason, because, among other things, revealing sources and methods is a crime. No

[2] Philip B. Heymann, "Law Enforcement and Intelligence in the Last Years of the Twentieth Century," *National Security Law Report*, Vol. 18, No. 1, Winter 1996.

intelligence officers would want to put themselves in that position.

Heymann: Yes. I'm sure that some of you have been through this, but this is like a powerfully held religion for the intelligence people: the protection of sources and methods.

When I was head of the criminal division during the Carter Administration, we were having a fight about a very big corruption case—Congressmen taking money from a foreign country—which we could solve by revealing that we had broken a code. Now, that's very secret sources and methods stuff. My boss, Deputy Attorney General Ben Civiletti, suggested that I should be the one to meet with Admiral Inman, who was then head of the National Security Agency, in the floating secret room of the Justice Department, which can't be bugged. What do you call one of those rooms?

Oettinger: SCIF (special compartmented intelligence facility).

Heymann: SCIF. He sat sort of in the background, and Admiral Inman and I sat next to each other, and I said, "So, why don't we reveal this? They almost certainly know that we've broken this code." The Admiral thought I was absolutely insane, and he thought I was a living, breathing danger to the safety of the nation. It's like a religion. I can't tell you ... he could be sputtering with anger.

Oettinger: I can't resist it. Admiral Inman on that score is a moderate. He's a three-time comer to this seminar, and you can see the record of some of his sentiments.[3] He's really quite rational and balanced on this. So you can imagine what the interview would have been like if it hadn't been Bob Inman, but somebody who is really crazy.

Heymann: That's correct.

Student: Do you have a feeling of how much of this conviction is justified, or is it just something that's part of the organizational culture and doesn't have any real basis?

Heymann: It's both. It's obviously very important. As a mystique it goes back to World War II. The ability of the Allies in World War II to crack the German code and the Japanese code resulted in immense military, tactical, and strategic advantages. A variety of stories have grown up around it that are part of the mystique, part of the religion. It's a little bit like talking about biblical stories of some sort. One is of Churchill being told that they could tell from the broken German Enigma code that the Germans were about to bomb Coventry out of existence, and Churchill saying, "Do nothing." And the Germans bombed Coventry out of existence. Another is about, I think, Leslie Howard, who played in "Gone With the Wind" and "The Scarlet Pimpernel" (nobody remembers these things anymore, Tony), who was flying from Portugal to Britain. He was a British movie star like Tom Hanks at the time, and they knew from the broken code that the plane would be shot down and he would be killed. They did nothing, and let it be shot down, and he was killed.

Oettinger: The latest word I have on the Churchill story is that it is apocryphal, but the debate continues.

---

[3] Bobby R. Inman, "Managing Intelligence for Effective Use," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1980.* Cambridge, MA: Program on Information Resources Policy, Harvard University, December 1980; "Issues in Intelligence," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1981.* Cambridge, MA: Program on Information Resources Policy, Harvard University, December 1981; and "Technological Innovation and the Cost of Change," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1986.* Cambridge, MA: Program on Information Resources Policy, Harvard University, February 1987.

Heymann: It's part of the mystique, but it's also very important. Of course, it depends on whose code and what you're picking up on it.

Oettinger: I'd like to insert a couple of citations, if I might, because it's a really important point. There is a book by a man named Gordon Welchman called *The Hut Six Story*.[4] The guy was a Brit, a first-hand participant in the process that led to the breaking of the Enigma code and so on, who then moved to America and wrote this book, and believes he was persecuted for having prematurely revealed sources and methods. There's also Nigel West's book, and I will, for the record, get the exact name of it. He is a guy who wrote chapters and chapters about the persecution of Welchman for revealing sources and methods.[5]

What is at stake in those two books is that Welchman described the German stupidities that provided the leads to the British decrypters. The debate over what Welchman did lay in revealing methods that had to do with using the enemy's weaknesses rather than the strength of the decrypting algorithms, and the folks charged with protecting the sources and methods didn't want that revealed. The Welchman book and what West wrote are open literature. You can form your own judgment, then, about whether the facts alleged are true or not true, but it illustrates, in the open sources, the flavor of the kind of debate that Phil is telling you about.

Heymann: When there's real hostility and it's a dangerous opponent, sources and methods have to be taken very, very seriously. If it's not a real opponent—for instance, if we broke the Canadian code—it would be less serious.

Student: Can't it be taken to extremes, though? If I use the example of Ultra, it was 30 years before they released information on it, and by then we had devastated Germany ...

Heymann: Germany was probably not using the same code for 30 years; not likely.

Student: Is there some line of reasonability that they're using?

Heymann: I don't think so. I think you do something like this very much by trying to hold a line rigidly. As you all may know, both our intelligence agencies that break codes and the FBI, which likes to be able to engage in electronic surveillance with judicial orders in the right case (we know the number of times: 500 times a year in a country of 260 million—that's not much), are extremely concerned by what looks like a hopeless problem. Technology has now developed encrypting machines the size of the tape recorder you're using that you can attach to your telephone or computer and seem to produce almost unbreakable codes. It's just the brilliance of the mathematicians who have devised new codes. We may be living in a world in which it's not going to be possible to break codes, at least for a while.

The fears that the intelligence agencies had about spy cases in these years lead up to about 1985. The two agencies were working in different parts of the world on different problems. The only overlap was in a spy case where the spy would have turned over some Defense Department secrets. I remember one was about satellites and things like that. Those were very difficult cases. There was an immense amount of anger associated with them. Then, with the help of a brilliant young lawyer (more him than me), I invented what's called the Classified Information Procedures Act, which is a new set of procedures that are used in the courts. The procedures prevent people who simply want to practice what is called "graymail"—threaten to reveal secrets in order to prevent their trial—from making an idle threat.

Whatever source or method they propose to reveal if you take them to trial (because all trials in the United States are

---

[4] Gordon Welchman, *The Hut Six Story*. New York: McGraw-Hill, 1982.

[5] Nigel West, *The SIGINT Secrets*. New York: William Morrow and Company, 1988.

public; we have no secret trials), the CIPA statute has the judge ask in advance: "Why do you want to reveal this secret?" and explore whether it really has to be revealed; whether you couldn't get away with a substitute. "Instead of saying: 'Professor Tony Oettinger is the deep-cover CIA agent at Harvard,' couldn't you simply say, 'There is a deep-cover CIA agent at Harvard.'" Something like that. The judge will explore all the alternatives to revealing a secret about sources and methods. That turns out to work very well. It's now been copied in Britain, and it ended almost all problems of agency conflict for a very long time.

Then the world suddenly changed dramatically in about 1985. It crept up on us, and you'll see the change. First of all, along came both terrorism and the crack epidemic, and growing fears about cocaine coming in from Colombia. With those, we started passing laws, or interpreting laws, that made it a crime for people abroad to do things that were going to be harmful in the United States. These are called extraterritorial statutes. There's a set of international law rules that tell you when you can do this and when you can't. So we can't simply say, "When a Frenchman kills a Spaniard in Portugal, we're going to try him if we can get our hands on him." You can't do that, but there is a considerable reach. The reach is far enough so that if somebody is dealing with drugs in Colombia or, more to the point, if it's Manuel Noriega in Panama, aiming them to come into the United States, it's perfectly all right under international law to make it a crime (and the United States has done this) for that person to be dealing in Panama with drugs intended to flow into the United States. We interpreted that activity to be a crime, and we went to Panama, and arrested him with a large military operation.

In the field of terrorism, it's perfectly all right (for a variety of reasons that I'd be happy to tell you if anyone cares, but I don't think you should care for the moment) to make it a crime in the United States to blow up an American plane abroad, to take Americans hostage abroad, to do a variety of things that are terrorist activities abroad. Beginning in the mid-1980s we started passing laws making activities of foreigners abroad, aimed at the United States, crimes against the United States. What that meant was that suddenly the line at our borders that separated the FBI from the CIA had disappeared, and from now on, the FBI was going to be investigating terrorism and drug dealing and weapons proliferation in foreign countries. It started getting more and more agents abroad, and taking that seriously.

The other half of the separation collapsed. Remember, from 1947 to 1987, if you want to take those 40 years, part of the separation was that one agency—law enforcement—was working at home; the other agency—intelligence—was required to work only abroad. The other thing that happened is that the Soviet Union collapsed. With the collapse of the Soviet Union, we found ourselves in possession of very substantial intelligence-gathering assets: human beings, satellites, analytic capacities, and no likely use for them. To put it differently, if you imagine a set of uses that you could make of such capacities, and it goes, in order of importance, from A to F (indeed, they have some such order of importance), suddenly A and B were cut off. We weren't concerned about A and B anymore, and suddenly you were looking at C, D, E, and F. I actually think they just wrote C, D, E, and F on the board at that time. But the intelligence agencies started saying, "Well, we can tell you an awful lot about drugs in Colombia. We know a lot about that. You want to know about terrorism in France? You want to know who tried to bring down that plane? We know about that."

So, the typical subject matters, which had been separate—one was the military capacity of the Soviet Union, the other was a bank robbery in Detroit, Michigan—suddenly started to duplicate quite completely. The Soviet Union was off the list. Drugs, terrorism, and weapons proliferation had moved right up on the intelligence side. In terms of territory, we had developed extraterritorial jurisdiction for our law enforcement agencies, so they were interested in drugs, terrorism, and weapons proliferation wherever they took place in the world. So, we've got both of those agencies now working abroad on the same

subjects, and they don't like each other very well.

Student: Do you think there's going to be a rise in disinformation to justify the existence of some of these?

Heymann: I don't think anybody lies about the amount of drugs, let's say, or a terrorist event, but I think there's a tendency to exaggerate. I think problems become more serious when they justify your existence. I think you start taking them more seriously instead of talking about them. The one that strikes me most is one that I don't have up here (figure 1), which is organized crime. I don't have any reason to believe that either Russian or Nigerian organized crime is what I would call a national security threat to the United States, but you'll find it on the President's list of national security threats. This is a list the President signs off on, which then becomes a legitimate target of intelligence gathering.

Student: Being specific, does that explain something like the amount of effort on the TWA bombing ... ?

Heymann: I don't think so. I think they believed it was a terrorist event. Just to stay on that for a minute (this is a footnote, unrelated to what everybody's talking about), we've been very fortunate in the United States in the very small amount of terrorism that takes place here. One possible explanation is that we have so quickly succeeded in solving the cases that have taken place. If I were the director of the FBI or the Attorney General, and something like TWA 800 came, I would pour resources onto it just because I'd want to maintain the reputation of our ability to resolve any terrorist event that takes place in the United States. It probably has effective discouraging tendencies with would-be terrorists.

Oettinger: Let me add another comment, because the questions you've raised in your responses are a very important element that we'll return to from time to time during this semester. Corruption can happen anywhere, but the notion of disinformation—lying in order to protect turf—to my mind, and, I gather, Phil's, is fairly rare, whereas what he describes as the sort of exaggeration of one's favorite threat, over which one has charge and budget, is fairly natural and fairly pervasive and is sometimes even true. And so, it's a difficult thing to sort out.

One of the current themes, which you will see all semester and I therefore give you an opportunity to pursue this, is the current information warfare thing, where, since a lot of the A and B have vanished, we now have: "*They* are going to screw up all our information systems and bring the United States to its knees by virtue of lousing up our vital information infrastructure." That has gone from nobody paying any attention in 1970, when Nelson Rockefeller pointed publicly at some threats that the Soviets were posing,[6] to today, at the other extreme, where the doom of the Republic is predicted. It's rather difficult in that area to make a coherent assessment. We'll talk about that more during the semester, but I think it would be derailing to assume that there's deliberate lying. There may be now and then; everybody gets corrupt now and then. But the fundamental problem is really a much more pervasive and understandable one, which is that it's your turf and you fervently believe in what you're doing, and you tend to exaggerate it, even almost unintentionally.

Heymann: Professor Oettinger's examples are wonderful ones, because we've got a brand new terrorist threat now, which is "breaking into our information infrastructure," and an immense amount of resources is going and will go into that. It's probably just sincere, often exaggerated, fears.

Student: I wonder if the military has a role to play in solving the conflict between the FBI and the CIA beyond our borders. I'm thinking specifically now of Mexico, and an effort to include Mexico in

---

[6] Commission on CIA Activities Within the United States, *The Nelson Rockefeller Report to the President*. New York: Manor Books, 1975, pp. 7-8.

SOUTHCOM (U.S. Southern Command). There are some advantages to that, particularly in relation to the drug problem. Could a major command in the military provide that kind of bridge? Could they separate the two or coordinate their activities?

Heymann: We'd probably have a three-way split. My successor [as Deputy Attorney General], Jamie Gorelick, paid an awful lot of attention to trying to deal with what I've so far described as both natural and psychological conflicts. When we get to organizational aspects, I'll tell you a little bit about it. I think that at the moment the situation is relatively good between CIA and FBI, in part because the CIA is so weak and the FBI is so strong now. You don't see two bulls butting heads; I think you see a bull butting heads with a bulldog, and the bull generally wins.

I want to put on the table, then, some of the concerns that are there in the background as the world comes to change, as I've described it. These are concerns that are there in any event, but they're part of the background. You'd better get them.

We've already talked about sources and methods. It's a matter held with almost religious fervor by the intelligence agencies.

The people in the United States worry a lot about spying on their political activities, and, indeed, we should. What every nation has developed as a consequence of that has been a separate set of rules, to some extent, for its intelligence agencies as opposed to the set of rules for its law enforcement agencies, which are designed to give citizens more protection by keeping intelligence out of this business of arrest, search, and immediate interference with citizen's rights. This doesn't relate closely to anything we've seen before, but we'll now see it start to come up. There's always been a sense that you'd better give your intelligence agencies more generous powers: less restrained, less guarded in by civil liberties protections, because you think it's necessary in the name of defense of the country. As we go along, I'll tell you rules for our intelligence agencies. But you generally give them very broad powers because you think they're operating abroad and not involved with your own citizens—this is a worldwide system—and because you want them to have broad powers to deal with foreign adversaries.

So one big worry is what happens when, with the change in the world I've just described, you suddenly find your intelligence agencies dealing with things that have a lot of important domestic consequences. Your intelligence agencies are dealing with drugs, and there are Americans at the other end of the Noriega line, and you've given the agencies extensive special powers to deal with drug production in Colombia. Does that become dangerous as you move it into the United States?

So, we've got to watch out now, as I take you further, about how you protect your citizens from your intelligence agencies when your intelligence agencies are starting to come home in their interests. As long as they were interested only in foreigners, and only in national security matters, and only abroad, you could give them much broader powers than you would trust your law enforcement agencies with. But when they start to come home, they bring those powers home with them. That's one thing I'll sort of describe to you as we move on.

Let me move to how other countries handle this (figure 1). Almost every country in the world has a separate internal security agency. Almost every country in the world has a foreign intelligence agency—the equivalent of our CIA; usually a defense intelligence agency in addition—a defense capacity to gather intelligence; a law enforcement capacity; and also (except for the United States) a separate set of internal security agencies (or usually one). In Britain, it's MI-5; in Germany, the Committee for the Protection of the Constitution; in Spain, GAL, which you're reading about in the papers these days. Israel has Shin Bet, the General Security Service. These organizations often come into conflict with law enforcement because all these agencies like to fight with each other.

The general way it's handled in the world is that these agencies are freed from almost all of the general legal requirements for searches, wiretaps, interrogations, questioning. They're left quite free. How-

ever, they're not allowed to arrest citizens and no information that they develop can be used directly at trial. So, if they develop information, they're likely to give leads to the law enforcement agency, which will then sort of know what the facts are, but they will have to find their own way of proving those facts. That's the general way.

As you're about to see, the United States does all of that quite differently. We don't have an internal security agency. We use the FBI for both law enforcement and for internal security. We have a quite complicated system of rules for intelligence gathering: a system that, I think, leaves us with less to worry about than other countries have because we give our FBI, as an intelligence gathering agency, considerably less power than other countries give their intelligence gathering agencies.

Oettinger: Let me try out a sort of statement, but I mean it as kind of an introduction to the question to you, which will be: Is that statement a reasonably accurate representation of the development of things as you see it? My own reading of U.S. history in this field is that, for the reasons you've mentioned, nobody gave much thought to controlling the intelligence agencies because they were abroad and so on, and that it was in the first place more important to regulate the FBI, et cetera. That became more of an issue, leading then to an increasing differentiation between the practices in the United States and those abroad, kind of based on almost a textbook demonstration of a fundamental U.S. premise, namely, that government is not to be trusted. Therefore, that whole distrust in the basis of the U.S. Constitution was manifested in greater restrictions compared to what you've just described with regard to, let's say, the U.K. or Germany. Is that a reasonable description?

Heymann: Yes. I think that is an accurate description. A lot of these rules come out of the period after the Vietnam War, when there were congressional hearings on our intelligence operations, chaired by Senator Church. There were lots of shocking revelations, including six or seven attempts to assassinate Fidel Castro, one more clumsy than the next. He was never in any real danger. As a result of that, a whole set of rules emerged. I said the Vietnam War, but it's also the Nixon period. Nixon was very concerned about internal security. He had the FBI doing a lot of information gathering about people in a general way.

I'm about to give you a set of rules that (I think Professor Oettinger is absolutely right) emerged out of a rejection of what was going on between 1965 and 1975. These are post-1976 rules. Having said that, I'm just anxious for you to have a sense of what the rules are for intelligence gathering.

First of all, abroad. Since the time it was discovered that the United States had tried to assassinate Fidel Castro, there's been Executive Order 12333, which forbids assassination of anybody by any U.S. intelligence agency or any other government official abroad. It's simply an executive order, signed by the President, but no one has changed it since 1975. Late in Judge Webster's tenure as director of the CIA, there were a lot of complaints about whether we shouldn't have done something to prevent a particular event and Webster said, essentially, that to have done that would have been to support a local group abroad that might have assassinated a leader abroad, and we can't do that. So, it's obviously taken quite seriously.

The law abroad is very complicated, but sort of fun to get a sense of. So, let me tell you about that. All of our constitutional protections apply only to everybody within the U.S. borders and American citizens or resident aliens—people who are going to become citizens—abroad, but they don't apply to foreigners abroad. It makes some sense to me. So, the protections travel with the American citizen or the resident alien abroad, and your foreign students enjoy them while in the United States; anybody in the United States enjoys them. But they don't travel abroad otherwise. So, in terms of U.S. law, an intelligence agency could break into someone's house in Peru and it wouldn't be a violation of U.S. law in any way.

Oettinger: Of course, getting caught in Peru is another side of it.

Heymann: That's right. Then you have to ask two other questions, which Tony asked right away. One: Is it a violation of Peruvian law? And the answer is, obviously, yes. It would be a violation of Peru's law, and very embarrassing, so not much of that goes on. The second question is: Is it a violation of international law, and what's the effect of that? And the answer is: Any policing done abroad, any law enforcement done abroad, without the consent of the government abroad, is a violation of international law. It can be done; this is going to be important as we get down to figuring out what we want the FBI to do and what we want the CIA to do now that they're both located in the same embassies around the world. But even just asking questions of people whose doorbells you ring, and who answer voluntarily, is a violation of international law. It doesn't matter who does it, the FBI or the CIA (well, maybe it will matter a little bit).

In the U.S., the law breaks down into . . .

Oettinger: Before you move on to the U.S., a question about when you say it's a violation of international law, for those of us who are, as I am, quite ignorant of it. International law is what? Agreements? Bilateral treaties? Sort of common law evolved informally? Or is there no single answer for that question?

Heymann: Yes. There is a very simple, single answer to it, and that is: all of the above. International law is generally considered to consist of multilateral treaties, including the U.N. charter; bilateral treaties, for instance, between the United States and Mexico; and customary international law, a little bit like what we think of as common law. When I said that it was a violation of international law to engage in policing activities in anybody else's country, that is customary international law. When people talk about what international law is, customary international law is supported by the opinion of (I don't know what they call them) sort of the academic experts. It's the only place where academic experts get all the credit they deserve. In international law the opinion of the commentators is given great weight, too.

Student: I had a question along those lines. Earlier you mentioned that there is a set of rules in international law regarding extraterritorial application of national law. Is there a codified body of rules in that regard, or is that just generated out of customary law?

Heymann: I can tell you what they are, and you're going to see they're nice and clear. It's simply generated out of customary law. The rules are that you can regulate the activities of your citizens anywhere in the world, so we can say an American who kills somebody in Tibet is guilty of a crime in the United States. You can regulate anything that takes place in your country, and that includes Manuel Noriega shipping drugs into the United States. You don't have to have all parts of the activity in your country, you just need some parts of it in your country. You can regulate anything that is an attack from abroad on your national safety, or your national institutions, in some way, and I think that rather sensibly has been stretched by the U.S. to include the activities of terrorists when they specially target Americans. If they seize a plane and kill only the Americans, I think you could make that a crime.

Finally, there are certain international activities that have been called universal crimes, mainly in treaties, but sometimes it's customary. That means anybody can make it a crime, and anybody can punish it. Piracy is the oldest one; that means it's 100 years old. But now there is a whole set of treaties that have emerged, largely since 1985, that say hijacking planes, attacking diplomatic personnel, engaging in hostage taking, are forbidden activities. Under those, we're free to pass statutes that make what the treaty forbids a crime in the United States, no matter where it takes place.

Now, we break the rules in the United States down into intelligence gathering with regard to foreign agents, and intelligence

gathering about people who are purely domestic. This is what we do instead of having a separate internal security agency. We have no internal security agency, but we tell the FBI that it can do different things if the target of its investigative activities is an agent of a foreign country. An "agent of a foreign country" includes anybody working for any political party in a foreign country (it could be the opposition), and he or she has to be not just an agent, but also has to be involved in espionage or terrorism. So, if somebody—including an American citizen—is working for a foreign country and is engaged in espionage or terrorism on behalf of that foreign country, rules apply that are special in only relatively minor ways. Without more, if you can just establish that he's working for a foreign country and that he's engaged in espionage or terrorism, the FBI is authorized to engage in electronic surveillance and physical searches. They do that in secret, so they have to go to a court. There's a special court that's specially cleared to handle this type of information. It has special safes where they keep all the documentation very secure. The Ames case was of that sort. In the Aldrich Ames case, once a court agreed that he seemed to be working for a foreign country and engaged in espionage, then the government was free to place cameras in his workplace, to go into his house and search for information, and to engage in electronic surveillance.

Student: Is the purpose of that surveillance to gain evidence for trial, or is it to prevent any terrorist activity?

Heymann: Two wonderful questions. It is theoretically to prevent any espionage or terrorist activity. The intelligence side is always to prevent something, or to allow the administration to develop different policies. Since Aldrich Ames is spying for Russia, we're going to do something to Russia: for instance, we'll close up a Russian consulate. The intelligence side is always for that.

Because it's the same organization that does it, the FBI, we don't have an organizational problem. Because the information can be used in a criminal trial, sometimes the courts say you should have used the non-foreign agent rules, the ordinary American citizen rules. It's not a big problem. It's a little problem.

Those are the only differences in rules. If somebody is working for a foreign country or a foreign party and engaged in terrorism or espionage, if there's reason to believe that and it's brought to the attention of the special court of judges (they're regular federal judges who do this part-time) and they agree, then there's a freer hand in searching and in electronic surveillance.

Oettinger: Your earlier statement that no trials in the U.S. take place in secret, I guess, still holds true: these special courts do have, essentially, secret proceedings, but they are of an administrative kind. Is that what you meant?

Heymann: It isn't that they're administrative. No trial where someone's guilt or innocence is determined takes place in secret. We can't do that. I think that when sexual abuse of a child is alleged, we allow the child to be out of the courtroom and things like that, but it is very rare and we don't do it any national security case. Every case has to be tried in the open. But getting a warrant to search, in every case—national security, foreign intelligence, or ordinary automobile theft—is done in secret because it's not much good searching after the other guy knows you're about to come and search. All the evidence disappears.

Student: Are they actually federal judges that issue the warrants, or are they administrative?

Heymann: They are federal judges selected by the Chief Justice of the Supreme Court. The court is called the Foreign Intelligence Surveillance Court.

Oettinger: Your summary makes it sound relatively easy, but then, as I read the guidelines that were part of your handout,[7]

[7] "The Attorney General's Guidelines on General Crimes, Racketeering Enterprises and Domestic

one of the questions that arose in my mind (you may want to hold it until you get more into the organization) was: What does this imply for training? Because by the time I was done reading the rather simple-sounding summary that you gave, elaborated in those guidelines, I said: "Gee, if I were an FBI recruit and then I figured out these guidelines are only the beginning, and there must be a lot more detail someplace, I'm going to be either very well trained or I'm going to be unable to act in a particular situation because by the time I figure out where to pigeonhole this, the guy may have gone away." So, would you elaborate?

Heymann: It's a little bit tough, but I'm going to make it. I have, so far, not told you the difficulty. I mean, you're saying it's already getting very complex.

Oettinger: Because I'm not an expert, it sort of overwhelmed me.

Heymann: I'm about to make it more complex, and it's a very good question.

Student: In cases where you put a subject—for example, Aldrich Ames—under surveillance, and you use this special court to obtain a warrant to do that surveillance because it's more of a national security issue, I'm going to go on the assumption that from a criminal standpoint, a typical domestic law enforcement standpoint, the issues of probable cause are not really fulfilled.

Heymann: It's awfully close, but apparently it's a little bit easier. You're right, They're not quite fulfilled.

Student: In a criminal trial, would the defense be able to exclude that evidence by the exclusionary rule?

Heymann: No, it would not. It would be legal. I don't know that the Supreme Court has reviewed one of these, but I'm close to 100 percent sure they would say, "That's an adequate basis for a search," even though you're right, it's just a little bit less than probable cause. By the way, I think the main difference is that if you were going to do a criminal search—in other words, if this were a purely domestic group, like the three people who blew up the Murrah Federal Building in Oklahoma City—and you wanted to get authorization for a wiretap or a search, you'd have to establish that they were conspiring to engage in arson, in a bombing, or whatever. If it's a foreign group, like the group that blew up the World Trade Center, which has some foreign ties, you have to establish that they have foreign ties and that they're engaged in international terrorism. One doesn't seem much easier to me than the other, but when I asked the people who work on these issues on a daily basis, they say it's easier to establish foreign agents engaged in international terrorism than it is to establish domestic conspiracy. So, you're right. There's a little bit of difference in how hard it is to establish.

Student: I would think that any good defense attorney would try to exploit that.

Heymann: They would try, but I think the Supreme Court would simply say, "It's sensible to have slightly different rules for national security cases." Let me tell you exactly what they have done.

In the days of Richard Nixon, in the days before we developed all these protective rules, the FBI was spying on people without getting a warrant, on the grounds of internal security. It was often purely domestic (no foreign involvement), but it was internal security. They said these people looked like they're dangerous people who are likely to blow up buildings or kill people or something like that. That case went to the Supreme Court, and the Supreme Court said: "No, you can't do that. If it's domestic security, if it's a totally domestic group with no foreign ties, you have to use the regular system and have probable cause, and it should be just like any other crime." But in saying that, they strongly suggested that if it had foreign ties, the

---

Security/Terrorism Investigations," Office of the Attorney General, Washington, D.C., 21 March 1989.

government would be free to go further. At that point, the law was written that gave them the power to search whenever there's a foreign tie.

Student: How loosely is that defined? Does it mean that you have actual official contacts, or you have a cousin in Algeria, or ... ?

Heymann: Oh no. I said "foreign ties," but you're supposed to be an agent of a foreign country. That means you're working for them either for pay or with a clear understanding of what you're doing for them. Again, it doesn't have to be a country: if you're working for Hamas or for the IRA, and you're in the United States, you would be a foreign agent. But it's not that you have a lot of friends in Germany or have a lot of friends in Jordan or something like that.

I've really talked to you about the rules for investigating when there's an investigation going on. The very big issue—this is an immense issue, and it's largely in the domestic case—is: When should the FBI be free to investigate at all? Forget about electronic surveillance or searches. When should the FBI be allowed to attend meetings, even public meetings? If there's a public meeting of the Michigan militia, designed to recruit people to stand up to the federal government and its oppressive tendencies, should the FBI be allowed to send an agent, and should it be allowed to keep records of what was said? If it's a private meeting, should it be able to convince or bribe a member of the group to report on what was said? It's not a search. That doesn't take a warrant or anything else. When should it be able to investigate political activities at all? When should it be able to open an investigation of political activity?

The World Trade Center bombing was preceded by highly inflammatory speeches in, I guess, New Jersey by the blind Sheik, Abdul Rahman. Should they have been attending those? Should they have been seeing who was there? Should they have been monitoring the group if there was a lot of talk about the necessity to use violence? The suspects in the Oklahoma City bombing were not militia members, as far as anybody knows, but the bombing was preceded by speeches by militias in the West demanding the flow of blood to free us from oppression by the federal government. Should they have been attending those meetings? If they attend those meetings, people aren't going to feel very free to meet because they don't like being spied on. If they don't attend those meetings, buildings are going to blow up that could otherwise have been saved. It's a major, major issue.

When it's a foreign agent, I think there's not too much trouble with the rules for when you can start an investigation. Among other things, I'm going to describe the CISPES (Committee in Solidarity with the People of El Salvador) investigation, which began as a foreign agent investigation. There's an act that makes it a crime not to register if you're a foreign agent. So, if they have some reason to think somebody is even working for a foreign country, they could open an investigation and monitor his activities without searches and things like that.

Student: Just to clarify, when you say "investigate" you mean "collect intelligence." Is that an important distinction?

Heymann: I meant "collecting information." The FBI calls the type of investigation that I'm about to describe "being allowed to open an intelligence investigation."

Student: It precedes a crime.

Heymann: Yes. The intelligence agencies aren't allowed to work in the United States, so they're all out of sight. We're now talking about activities in the United States by groups that are largely American. When can you monitor their activities? The FBI calls this a criminal intelligence investigation.

Oettinger: I trust it's clear to you from the reading, and it may be worth underscoring to check my understanding of it, that the countervailing thing that's at stake here is the chilling of normal legitimate political

discourse, by virtue of having sort of police, the FBI, whatever, come in. That, presumably, is the balancing act.

Heymann: Exactly. There'd be a substantial chilling. If I told you that there is a federal agent in this room now and he's not interested in much, except he does record what you're saying or takes notes afterwards, all of you would, I take it, feel inhibited in what you say.

Oettinger: And, by the way, lest you think that's a very academic, hollow kind of argument, in the era of Joseph McCarthy in the 1950s, that would have been a very reasonable concern about a classroom in this university, and it did have chilling effects. So the notion that it can't happen here and so on is absurd. For those of us who lived through McCarthyism in this university, one can only appreciate the efforts made at balancing this concern over national security on one hand with civil liberties and political freedom on the other. It's not an empty argument at all.

Student: If I could, too, refer to the readings, which I thought were very clear in the distinction between probable cause and reasonable suspicion, is that the distinction we're talking about here or are we leading up to that?

Heymann: I've been leading up to it, but there's no reason to lead up any more. Let's just go there. Immediately after Nixon, Attorney General Levi, working for President Ford, promulgated the crucial rules here. They're like the Presidential order that says that you can't assassinate. These are simply the orders of an executive official, but they've barely been changed for 25 years, so they're starting to get some status.

The rules are that the FBI cannot open any investigation, including an investigation that is what they call a domestic security investigation, unless they have reasonable suspicion, and here are the words. A domestic security/terrorism investigation may be initiated "when the facts or circumstances reasonably indicate [that's less than probable cause] that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States."[8] So, it has to be several people, political or social goals, through force or violence, and committing a crime, at the same time.

When you think about it, that's really quite protective. It's a little worrisome because it's so protective. It leads you to ask the question, "Well, could the FBI attend speeches in New Jersey by Sheik Rahman? Could they say that the facts reasonably indicate that "two or more persons" (that's easy) "are engaged in an enterprise for the purpose of furthering political or social goals" (that's easy—they're actually religious, but that's fine) "wholly or in part through activities that involve force or violence"? He sort of preached force or violence, as did some of the militia leaders. But could you prove that they were engaged in activity that involved changing the social structure through force or violence in violation of the laws of the United States?

Worried that the guidelines were just a little bit too tight, FBI Director Freeh and my successor, Jamie Gorelick, have interpreted that (I gave you their interpretation) in such a way as to allow what's called a "preliminary investigation": a short 30-day investigation, on less basis than reasonable suspicion that they're actually engaged in violence, of any group that is preaching violence and has the capacity for violence. They've changed it in that way.

Let me say one last word about this. CISPES is fun and interesting. In the CISPES case, large numbers of the American people were meeting under the banner of CISPES, in opposition to our national security efforts in Salvador. We were supporting right-wing regimes in Salvador, and large numbers of people were meeting, demanding that we support left-wing regimes. An informant came along and said, "You know, this organization is really an agent of a foreign power. It's really working for the revolutionaries in Salvador.

---

[8] Heymann, "Domestic Intelligence Gathering," p. 19.

What's more, it's planning bombings both in Salvador [where the revolutionaries were bombing and shooting people for sure], and in the United States," where there were some bombings and shootings. Now, the guy was lying through his teeth. There was no basis for believing him. Nobody ever should have believed him. After years of investigation, nothing was found to confirm any violence attributable in any way to the organization, or any tie between the organization and the revolutionaries in Salvador.

But, in the meantime, we had done all the following, which gives you a sense of what we're worried about. "The FBI investigated CISPES over a period of five years, from 1981 to 1985. ... [T]he FBI used photographic and visual surveillance of rallies and demonstrations (22 field offices) [that means 22 places in the country], undercover operatives attending meetings (five offices), informants, interviews of people going to Central America, trash examinations [looking at people's trash] (six field offices), examination of bank records (six offices), study of telephone toll records (14 field offices), and the use of a number of quasi-public records [Tony had mentioned those earlier], involving licenses, credit, employment, utilities, et cetera."[9] They added retrievable information about 2,375 individuals and 1,330 groups to their files.

It's a tough world out there. If you become even a little bit paranoid, you find that your domestic intelligence people are doing what was done in CISPES, which was a mammoth investigation threatening to lots and lots of people's feelings of freedom to engage in political dissent. If you are a little bit too cautious, which they were immediately after CISPES, you find that 230 people are blown up in a federal building in Oklahoma City.

This crucial line is drawn in terms of the words (it's all done in terms of words, and you have the words there), which are that it's the FBI director's interpretation that they're free to investigate organizations if the organization is preaching violence and seems capable of violence, at least for a limited period of time.

Oettinger: A couple of comments, if I may, for purposes of the course. The class knows, Phil, about my foible for balancing acts resolving tensions.[10] You've been given here, both in the readings and in what Phil has been telling you, the exquisite anatomy of a balancing act right at the point where two very important things—civil liberties and the need for self defense against criminals or whomever—confront one another, and when that adjustment is exceedingly difficult.

Just to anticipate a bit from the rest of the semester, Professor Heymann pointed out that a ban on assassinations is not the only place, in terms of covert operations and so on, where there are limitations placed on U.S. intelligence agencies. He's been focusing on law enforcement. The same kinds of dilemmas apply even in the international sphere, in the intelligence sphere, on going beyond civilized norms, whatever they might be at the moment, and reasonable prudence in defending oneself.

Now, traditionally, some of that, especially in the intelligence realm, goes all to hell when you have a wartime situation. You do things in wartime that you would not do in peacetime, including killing. All right. But when you have a situation like the present one where it's not cold, it's not hot, et cetera, a lot of the stark distinctions—killing is permitted, indeed encouraged, when you are "at war," but it is a crime when you are not at war—disappear, and you have a much murkier situation, which Phil has illustrated admirably in this realm.

I'm putting you on notice we're going to have a lot of these in the intelligence realm as well throughout the rest of the semester. It's kind of the heart of the dilemmas that Phil is pointing to in that watershed of 1985. As the Cold War evaporated, so did some of the certainties that the older

[9] Heymann, "Domestic Intelligence Gathering," p. 24-25.

[10] Anthony G. Oettinger, *Whence and Whither Intelligence, Command and Control.* Cambridge, MA: Program on Information Resources Policy, Harvard University, 1990.

regime of clear distinction between war and peace permitted us. The whole intelligence, law enforcement, and policy communities are still wrestling with that. These are live, active, balancing acts and issues.

Student: If I could just take you to that balancing point in the CISPES case, did a federal judge see the evidence and make the decision to allow the investigation to continue?

Heymann: No. You only need a federal judge if you are going to engage in a search or an electronic surveillance or an arrest, and in CISPES they never did any of those things. They simply wrote down license plate numbers, attended meetings, searched trash, engaged in physical surveillance from planes and cars, and made records on 2,300 people.

This is much more, I'm sure, than any of you ever wanted to know. But that's why you have to break the questions into what it takes to initiate an investigation, and what it takes to engage in intrusive steps. For intrusive steps, there are special rules for foreign agents. They're not much different, but they're a little different for searches and warrants. But they're no more important than the question: When can our internal intelligence agency, the FBI, initiate an investigation without intrusive steps? Just following people, picking up their trash, looking at their license plates, see who meets whom, opening files?

If you can't open an investigation, if you can't satisfy those guidelines I just mentioned, you're not allowed to open any files. The Privacy Act forbids the FBI from keeping any files, even on public meetings, unless there is a legitimate investigation. An FBI agent couldn't come to this class, make notes, and have them filed at the FBI. You can't do that unless an investigation has been opened properly and efficiently.

Student: That's the whole entrapment issue?

Heymann: It's not entrapment. This is simply record keeping. It's just a protection, again, all starting with ...

Oettinger: With Nixon, the "enemies lists." Think about it.

Heymann: The Freedom of Information Act and the Privacy Act were passed at just about the same time, all, I think, in the 1970s. The Privacy Act says they can't keep files unless they've properly opened an investigation. The Attorney General says you can only properly open an investigation of an organization like CISPES or something else if you have reason to believe that it encourages violence and has the capability, and you can only keep it open for a little while before you have to close it, unless you can be satisfied that, in fact, they're planning violence.

Just in case this has been too clear and not confusing enough, here's what you got so far in terms of what the rules are. The rules are that there's basically a sort of free hand for intelligence abroad, although you have to worry about violating foreign law and international law because of its diplomatic consequences. The structure of intelligence laws—rules for activities overseas—by the way, is largely one that requires higher and higher levels of approval for activities that are more and more dangerous or questionable. The only flat prohibition that I know of is the one on assassination. But, as you do more and more questionable things, it requires a higher and higher level of approval. That's the way they do it.

Oettinger: Ultimately, there are things called "presidential findings," and you'll hear about that later on this semester.

Heymann: "Between the two" under "U.S. Law/Policy" (figure 1) is very interesting. A certain number of intelligence activities pick up activities of foreigners abroad and activities of U.S. citizens simultaneously, or you could target them in the same way. It could be technological or it could be nontechnological. You could target somebody abroad, where there are no rights (basically a foreign citizen abroad has no rights under U.S. law), knowing and hoping that you're going to pick up a lot of information about the person whom that

drug dealer in Bogota is dealing with in the United States.

So there's a very interesting category. We have elaborate protections for Americans at home. We have very few protections for foreigners abroad. That's all very sensible. But there are investigative techniques that allow you to learn a great deal about U.S. citizens, just sort of through the rules of nature. Nature allows you to find out an awful lot about Americans in a smaller and smaller world, a world where there's more and more international traffic, by focusing intelligence gathering on their associates abroad. If we believe that an American is a major drug dealer in Chicago and is getting his drugs from Burma, we can find out an awful lot about the American in Chicago or Detroit or wherever by focusing either FBI or CIA (because we're about to get to the fact that they're both hanging out there) on the Burmese guy.

I'm not going to tell you what the answer is there. But that remains a difficult question because, remember, one of the important problems is to keep the free intelligence rules from entering into the life of your democracy at home. We've done a pretty good job of that. We've got an elaborate set of rules here; Professor Oettinger says they're so complicated that the new FBI officer is going to go home and decide he wants to be something else. We have practically no rules for foreigners abroad. And we have this funny little relationship where you could aim for the "no-rule" category, knowing that, without having to comply with the rules, you're going to pick up a lot about U.S. citizens who are associated with those people.

Oettinger: That realm, again, is getting larger and larger. All you have to think about is international satellites, the Internet, et cetera. You can be abroad, and if you have a wiretap someplace you can pick up, you don't know what you're getting. So this, again, is hardly an empty issue. It's a large and growing area of this tension between civil liberties and self defense.

Heymann: Just so I don't take up all your time, the last thing is organizational problems (figure 1). We now have the law enforcement agencies abroad (maybe I'll pretend it's just the FBI) worrying about drugs, terrorism, weapons proliferation, under extraterritorial statutes. We have the CIA abroad worrying about the same things, theoretically with a preventive objective or an "advice to the President" objective. We've got satellites overhead picking up information that was designed to be used for preventive purposes, but that could be very useful to law enforcement. Maybe it falls into this third category of "between the two." What's the problem, and what do you do about it?

On the ground, the problems are fairly obvious when you think about them. When we've got CIA and FBI both in Bogota, trying to pick up information about drugs, they're both likely to deal with the same informant (the FBI would call him an informant, and the CIA would call him a source), and he will think we're crazy. The CIA may know A and C, and the FBI may know B and D, and what you're really interested in is the relationships among A, B, C, and D, but they're not likely to tell each other. The CIA won't do it because it's worried that its sources and methods will be compromised at a trial or somewhere else. The FBI won't do it because they're equally protective of their informants and don't trust the CIA at all. They're sure the CIA will leak it. So neither of them trusts the other.

One problem is, if you've got them both doing the same thing abroad, and neither one is prepared to be open with the other, how do you coordinate their activities? Each of them is fighting a good bit for jurisdiction, too. I think the only answer to that is that the ambassador's got to be the one who manages that coordination. You have to find a way to make sure that the information that each is gathering and what each is doing gets to the ambassador. I think that's the way they're moving. Otherwise, we've got some kind of great embarrassment.

Oettinger: Unfortunately, it's complicated by the fact that, for reasons we'll go into a bit more during the rest of this semester,

ambassadors, in caliber and in practicality, have diminished in stature and in their ability to do this task. So I agree with you that it would be desirable, because nominally the ambassador is the guy in charge for the United States. But through the miracles of modern telecommunications and computing and one thing and another, there's been a 40-year trend turning ambassadors increasingly into our former mayor[11] and the like, as opposed to genuine managers. So that opens up a whole other set of issues. It's a complicated set of intermeshing wheels.

Heymann: The prestige of the agency has a lot to do with it. The FBI has immense prestige with the Congress. The State Department is in very hard times. If the FBI were to complain that it wasn't getting cooperation on drug matters from the ambassador in Bogota, it would be a very serious matter for the State Department. So, it's not so easy.

Then there's a separate question about what you do with the expensive technology—the satellites and the computers that can make something of photographs or signals intelligence. Here the question is one of sources and methods. What you'd like to do is to use those capacities to gather information that would be useful for law enforcement as well as for intelligence. The intelligence agencies would like to cooperate, because they'd like to justify their budget in part by the help they give to law enforcement agencies, let's say with drug dealing in Latin America. (I don't have any idea where we use such satellites and photography; we probably do, but I'm not revealing any secrets.)

If, however, the relationship becomes close between the FBI and the NSA, which, let's assume, is managing the satellites, then the NSA will become subject to the rules that are binding on the FBI at trial, including rules that require them to reveal any exculpatory (that means tending to show innocence) material that the agency has. The notion is called "alignment." If the FBI asks for help from the NSA in investigating somebody they think is the largest drug dealer in Peru, and the NSA gives them help, the defense attorney will stand up at trial and say, "The NSA helped the FBI. It was part of the prosecution team, and therefore they should be required to turn over to us any information they have that may tend to show that the defendant was not guilty"—any exculpatory information. Basically, they should be treated like a police department, or like the FBI. That fills the NSA with horror, because its sources and methods would be revealed, and with that much of the value of extraordinarily expensive technology would be lost. The case could always be dismissed, but the Justice Department would undoubtedly fight that.

So, the trick is, the satellite technology is there from the Cold War days. It probably ought to be updated and kept fresh because it's a very valuable way of protecting the United States. While at the moment there's not a lot of national security use for it, the Justice Department will demand access to information from it. The intelligence agencies would like to give the information, so that they could justify the expense of it, but it has to be done in a way that protects them from a judge ordering some public revelation that would cause them a problem. There are two things they object to: a search of all their files, which turns out to be an incredible job, a very mammoth job, and, if they find anything that could possibly be helpful to the defense, its revelation, which will quite possibly reveal how the NSA gathers information.

The answer to that is to work out very complicated and careful arrangements that determine when you ask for help from an intelligence agency, how you ask for help, and a variety of things like that. In fact, I think that's what they're doing. With that let me stop.

Oettinger: Again, with an eye to coming attractions and reading in the record of the seminar from the past, I agree with every word that Phil has said on this last point, but it's even worse. One glib way of addressing the problem that he raises is to

[11] Raymond Flynn, former mayor of Boston, currently U.S. ambassador to the Vatican.

say, "Well, these conflicts should be resolved by the President." Of course, if all of them were resolved by the President, he wouldn't have time to do anything else, so it has to be done at a lesser level. Devising ways of doing this when the protagonists are already essentially cabinet-level officers is difficult. There isn't much room for maneuvering politically between the President and his cabinet officers, so it's a hard problem in any structure. That's number one.

Second, he understated the magnitude of the problem, especially with regard to the technology, because he gave you a very accurate picture of the law enforcement versus the intelligence thing, but those are not the only parties. You now have the same technology, assets, and so on involved in an entirely different struggle within the intelligence family, so to speak, between strategic intelligence, tactical intelligence, and the national-level people in the military, over whether at any given moment the damn thing should be over Peru looking at drugs, or over Bosnia doing something for the guys on the ground there, or over Iraq looking to see if there are any more nuclear or chemical weapons, or over a number of other places. So the questions of these jurisdictional issues and resource allocations then take place in several venues. You'll hear a lot more from some of our later guests about the intra-intelligence aspects. When you hear that, which sounds relatively complicated, remember that's overlaid on everything that you've heard Phil describe here today, for which, I must say, we are enormously grateful to you.

Heymann: Thank you.

Oettinger: That was splendid. If you're willing and we have any more questions, we have a few more minutes.

Student: Is there a link now between your CIPA (Classified Information Procedures Act) and some of the computer hacking that has been done, for instance into the Pentagon and whatnot, from overseas?

Heymann: What CIPA does is it allows you to avoid making U.S. secrets public at trial. I don't think there's any link to the computer hacking from abroad. The computer hacking from abroad is very interesting. It's a big deal with the Justice Department. My son, who's a senior prosecutor in the U.S. Attorney's Office here, did the biggest case, which was catching the teenage hacker who went from Argentina into Harvard's computers, and then into the Defense Department's computers. When he tells me how the investigators caught the hacker, it seems to me they were very lucky. The next case they're not going to be able to solve that way. This guy signed his own name on a bulletin board. The same name he was using on a Harvard computer was on an Argentine bulletin board, and as soon as they were smart enough to find out that he was coming in from Argentina, they were able to identify him that way. That won't happen again.

It's a very interesting process: the whole field of computer crime and the investigation of computer crime, and, as Professor Oettinger said, "the absolute internationalization of it." It doesn't make the slightest bit of difference where you are, you can get into computers anywhere in the world if you're a good hacker.

The trick from the law enforcement point of view, the thing my son gets credit for, is figuring out how to search Harvard's computers to find the hacker's messages without reading all of your messages. With a warrant, with Harvard's knowledge, he had to find a way (which you can do technologically, using familiar computer technology) to tap into Harvard's computers, which were handling tens of thousands of messages, and only pick up the two or three that were coming from the hacker, so that the government didn't even see the others. But that's going to be the Brave New World of law enforcement.

Student: As I recall, the campus newspaper reported on that last year, and they said the University did not want to cooperate with the investigators at the time because they felt that it was an invasion of privacy for the students. They said basically, "If

you want to do it, you'll need a warrant," and so the government went out and got a warrant. My understanding was that it was some kind of filtration algorithm that scanned for key words. They only picked out the ones that had certain key words that were relevant, and only then, when you had a very small fraction of the total volume, did they actually have humans going in and reading the messages.

Heymann: Exactly right. The only thing that maybe isn't right, if my son is telling me the truth (which happens most of the time), is that very often if you're an organization like Harvard and the government comes to you and says, "We'd like to go into your computers to find out how the hacker is using them to get into the Defense Department computers; will you consent?" you don't really object, but you don't want to be responsible for the decision. So you say, "Why don't you go get a warrant?" because you don't want everybody at Harvard to be saying, "Why did you consent to let the government go into our mail?" You want a judge to take the rap for that.

Student: May I ask another question? It seems pretty disturbing to me that a teenager in Argentina, who obviously doesn't have a lot of financial resources or a lot of training, doesn't have a college degree, or any amount of time working with these computer systems, can hack into the DOD system. I would wonder how much of a threat is an actual concerted, organized effort, and how much of a threat is coming from terrorist organizations? My impression of the terrorist organizations around is that they are really not that technically sophisticated, certainly not as much as a foreign intelligence service. I was wondering if you had any opinions on that.

Heymann: I'm going to turn this quickly to Professor Oettinger, but let me just say that he didn't get into classified Defense Department computers. The Defense Department classifies some of its computers and protects them more than others. These were not classified computers. He wasn't in a place where he could launch a missile. He was in unclassified material, but it's still surprising that he could get in.

Oettinger: That's one answer. A lot of the hacker incidents have been minor. I mean, what is the big deal if somebody steals a computer from a Harvard office? Most Harvard offices are unlocked, in buildings that are not secured, and anybody could walk in off the street and steal a woman's handbag, or a computer lying loose on a desk, or a coat hanging on a rack. There was a guy for years working the Faculty Club, well-dressed and so on, stealing coats and bags off the rack until they finally caught him. So the point of my message is that things that are not defended are easy to penetrate. Many of these attacks are of that type, but your question still remains a very, very good one. In fact, one of the things that we ought to do, if he does it in time, is explore this idea with Greg Rattray, who is doing a Ph.D. thesis at Fletcher on this whole question of gradations.[12]

I'll give you another analogy. If anybody in this room wants to go assassinate the President of the United States, it's quite easy, so to speak, if you want to commit suicide. The history of presidential assassinations and assassination attempts is such that it can be done. Now, will that bring down the United States? Is that a strategic threat to the United States? No. Our Presidents happen to be eminently expendable, so that, awful as it would be, in the last analysis, if you've seen one President, you've seen them all, and the system is more robust than any one individual.

So the question then becomes: When is a hacking attack in the category of a nutty act or a crime, which, however awful it may be for the victim and family, is not catastrophic, versus when is it a strategic attack? I'm not trying to laugh out of court the death of any one individual, or a property loss, but if you lose your wallet and your credit card, it's annoying, but it doesn't necessarily ruin you. The loss of one political official doesn't bring down a country. Now, at what point does that

[12] See Major Rattray's presentation in this volume.

change, and what does it take to mount a strategic hacking attack that would indeed be the sort of soft war equivalent of a nuke? The answer to that, I think, is unknown. I hope that Greg Rattray's thesis will begin to frame that question and shed some further light on it. At one end of the spectrum you have undefended stuff, which most of it is, by the way, and your point is well taken. Those Defense Department computers were undefended. Okay, there's a lot of stuff. So, big deal. But, at the other end, where the boundary line is between the trivial and the serious, we don't really know.

Student: Over the summer, there was a lot of attention to the fact that we revoked Colombian President Samper's visa because we thought we had evidence that his campaign was funded by drug traffickers. Nominally, the State Department is responsible for foreign activities of the U.S. government and relations with other governments. In the case where there may be a conflict between the aims of the State Department working with the Colombian government, either to eradicate drugs or on other issues, and the desire of U.S. law enforcement agencies operating in Bogota to arrest somebody who may have political ties, which should take precedence—the law enforcement aspect or the diplomatic concerns?

Heymann: I'm pretty clear that it ought to be treated first of all as a diplomatic matter, but it wouldn't necessarily play out that way. If you were Warren Christopher or Madeleine Albright, you would worry very much about what would happen if you told the DEA special agent in charge, only 82 layers below you in the great federal bureaucracy, that you didn't want somebody arrested. Obviously the DEA cannot arrest people in Colombia, but it can go to the Colombian police and say, "We've got lots of evidence on this guy. Why don't you arrest him?" If you told the DEA officer not to do that, you'd be very frightened of the repercussions.

Oettinger: What a headline in the *Washington Post*!

Heymann: It's just that drugs are such a big issue. So many people are hostile to the State Department. So many people are friendly to law enforcement, but it ought to be a foreign policy decision, just on the theory that that's more important than *any* single arrest.

The case where a lot of the law was made on what are the rules abroad resulted from the activities of the DEA around the death of their agent Camarena in Mexico. He was tortured and murdered, and the Mexican authorities were corrupt and were making no effort to solve the case. The DEA paid the Mexican police (more than the people paid them not to investigate the case) to kidnap the doctor who they believed had given Camarena drugs to keep him alive so that he could be tortured longer. He was not the most attractive figure in the world. They kidnapped him and brought him to the United States, and the DEA went out with the Mexican police and searched homes on the grounds to gather evidence for those cases. I have no particular reason to believe that the ambassador liked any of this. All of that was sustained as not illegal, but Mexico has demanded that it stop, and it's stopped.

Oettinger: Sir, we thank you again, and we've got to get out of here because there's a four-o'clock class.

INCSEMINARS1997

ISBN-1-879716-47-X