

Intelligence Ethics:
Laying a Foundation for the Second Oldest Profession
Draft 7 final to editor Loch Johnson mailed Feb. 24, 2006 Draft 7

Michael Andregg, University of St. Thomas in St. Paul, Minnesota, USA.

Introduction

The first reaction to the idea of ethics for spies is often a big laugh or comments with “oxymoron” in them. Spies lie, cheat, steal, deceive, manipulate and sometimes much worse in the course of their work, so this reaction is understandable. That masks a more important point. The world needs a professional code of ethics for spies and other “intelligence professionals.” So some are working hard to create one now. A former operator asked, why have intelligence agencies at all if you want to encumber them with rules? Because the nation is in danger, and our world is at war with “terrorists” who don’t obey any rules at all. To win, spies must be better than mere terrorists.

Before discussing that developing code of ethics, a brief review of the varieties of spy is in order, since different types of intelligence professional often have different ideas of virtue and vice. For example, those who monitor phone calls or read other people’s mail every day often take great offense when lumped into the same category as the “spies” who betray their countries for us, or betray us to serve some other country. I will reduce the many different kinds of intelligence professionals into 5 broad types.

Collectors, gather information, data or both, usually by technical means like satellites or from human agents, and feed it up a chain of command. Protecting “methods,” “sources” and especially their own anonymity are cardinal virtues to them.

Analysts process that information, and combine it with “open sources” information to generate higher order papers or other “products” that provide their policy masters with more useful information. Usefulness means timely, relevant and “actionable” as well as accurate information. Avoiding “politicization” of their information products is an important virtue to analysts. Politicization means altering one’s formal opinion to suit the prejudices of policy makers, and this is a special but common sin among analysts.

Operators go places and do things, sometimes very dramatic things like starting wars and such, but more often they are doing quiet things they would prefer we not observe or talk about. Of all the types of intelligence professional, operators are the most likely to kill, blackmail, extort or torture in their work, and they often “handle” spies who are at risk from their own governments. So guarding “operational security” is a core value to operators to protect their operations, the people they employ, and themselves.

Managers organize the work of all of these people and the budgets that support them. Managers must contend with many bureaucratic forces, so their morality or lack thereof is more familiar to us all. And finally,

Policy makers, in theory, make the decisions that have the greatest impact. In theory, all the others are working to support good decisions by policy makers in governments. The most obvious policy makers are politicians, who also must contend with odd forces in their work. Most have security clearances, but some do not. All lie; it is required by the job. So in contrast to analysts, “truth” is far less important to most policy people than expedience, or practical utility in their political struggles, 80% of which are domestic.

These types of real intelligence professional are all different from the James Bond-like image of a spy who sails into town in a cool car, steals secrets from rich bad men, grabs a beautiful woman or two and leaves just in time to avoid the building blowing up. They are also different from the Mata-Hari image of a beautiful woman who trades sex for secrets and then kills the foolish king or bureaucrat. The real spies also need a real professional ethic more sophisticated than that found in James Bond movies.

Ethics is the study of moral logic and paradigms, but it is not just lists of rules or laws. If ethics were that simple, attorneys would have a different reputation than they do. In ordinary life we can more easily observe the ancient moral virtues: be honest, don’t steal, kill or assault, respect your neighbors, honor your debts and so forth. But the world of official intelligence involves activities in many grey areas of moral thought, and generates perplexing dilemmas where agents must balance the national interest in security which they are bound to protect, against some other virtue like the ancient rules against lying, stealing, killing and so forth.

Classical Western philosophy as written by Plato, Aristotle and others concentrated on identifying moral “virtues” and asked how these could be cultivated in civilized men. Later Europeans generated doctrines that are now called “deontological” (or rule-based) as in Kant, or “consequentialist” (based on the consequences of an act) of which a good representative is the philosopher John Stuart Mill. To put these broad theories of moral reasoning into a small frame, any serious decision involves three things: an actor, an act and consequences of the act. Virtue theory concentrates on the actor, deontological theories concentrate on the morality of acts, and consequentialist theories focus on what happens after.

These Western theories of ethics often ignore parallel but not identical thinking from Asia, Africa and indigenous peoples world-wide. Buddha had many things to say about this, for example, and Confucius and Lao Tzu. There are also more elaborate theories from Western tradition that are especially appropriate models for the spy world, like “Just War Theory” developed by Catholic priests and theologians searching for their own guides to moral clarity in difficult circumstances. There are many connections and similarities between “national intelligence” and war, so Just War Theory is sometimes used in training spies too. At least, it is referred to occasionally! Such complex ideas are what philosophy courses are for. With this sparse introduction, we will now turn to the major ways that spies or intelligence professionals of any kind must struggle with the moral dilemmas most peculiar to their unusual, but ancient profession.

Covert Action

The most serious ethical dilemmas occur in the realm of covert, or secret, action. A career covert operator once told a colleague that “we use less than 10 per cent of the budget, but we generate over 90 per cent of the bad publicity.” This is true because covert operations may employ all of the dark arts, and are responsible directly or indirectly for millions of deaths during the 20th century. On the other hand, covert operations can also prevent wars from starting and there is no accurate way to number the lives saved by such methods. This captures the core dilemma of spies and spying quite sharply. Spies are extremely important to the question of whether wars start or do not start, as well as to who wins and who loses. Consequences for life and death can be vast. But measuring those effects is almost impossible even after the events in question.

This is a problem for consequentialist theories of what constitutes moral behavior. If you cannot really know consequences, how can you judge if an act is moral? If you could save a city from a nuclear terrorist, for example, a consequentialist would usually conclude that it is perfectly OK to torture that terrorist if one might obtain information enabling you to recover and neutralize the bomb before it goes off. But who can know for sure, especially during crisis moments? These situations, called “ticking time bomb” scenarios, are discussed in law schools when they are considering the laws that (most say) strictly forbid torture under any circumstances. The deontological group would generally conclude that if the law forbids torture under any circumstances, well that is the rule and it should be obeyed regardless of consequences. Others conclude that it would be cruel to let a silly rule keep one from saving thousands of innocent children. I leave the reader to determine what course of action the virtuous person would pursue.

Let us consider a more complex case based on real events. During the early and mid-1980’s the U.S. President Ronald Reagan decided that a political party in Nicaragua called the Sandinistas who had deposed a previous dictator was too closely aligned with the Soviet Union and should be removed. Simpler measures failed, but energized some in the U.S. Congress, who wrote amendments to national legislation prohibiting any U.S. intelligence agency from trying to overthrow the Sandinista government. Frustrated by these “Boland Amendments,” the then-Director of Central Intelligence, William Casey, authorized an “off the books” project in 1983 run out of the National Security Council which raised tens of millions of dollars by various clever and illegal means like selling American weapons to a country that was an official enemy at that time, Iran. This affair became known as the “Iran-Contra” scandal.

That operation broke a great many national and international laws, but it is important to recognize that it also accomplished its political goals. A “secret” army was created, armed, and funded which came to be known as the “Contras.” They created such chaos in Nicaragua that, combined with clandestine economic warfare and psychological operations from abroad, they managed to push the Sandinistas from power.

Regardless of whether one approves or disapproves of that political goal, this case vividly illustrates the dilemmas and the powers of secret operations. They won, by cheating. One document that was written by a CIA contract officer (on loan from the U.S. Army) and published

in tens of thousands of copies distributed to Contra troops, for example, called for selected assassinations of mayors and attacks on humanitarian groups, schools and medical clinics to demoralize Sandinista supporters. It was titled “Psychological Operations in Guerrilla Warfare” and it is well worth study by professionals interested in insurgencies or in developing an ethic for spies that is higher than the gutter. To win the secret war, America was disgraced, with powerful long-term consequences that continue to this day. No longer would the USA be seen as a genuine moral leader in the international effort to establish and strengthen human rights.

It has been a canon of diplomacy for centuries that morality has no place in international affairs, and putting ethical boundaries on projects like the Iran-Contra operation seems near impossible. This is the reasoning of cynical men. In a world with weapons of mass destruction (WMDs) and millions of people angry enough to use them, we must do better than that. So I want to share the simple guidance of an operator I know well. His rules, based on experience rather than books are:

First, do no harm, especially to innocents. (Innocents have a very high place in his moral framework – this is not true for all operators or all “intelligence professionals.”) When colleagues laugh, he tells them ‘Be an artist, not an oaf, and if you absolutely must; be a sniper, not a bomb. Most missions can be accomplished without undue harm, and even wetwork can be quite precise – stop excusing incompetence.’

Second, and only if techniques under rule 1 cannot protect the people, chose the lesser evil when moral dilemmas cannot be avoided. Thus if you must lie, cheat and steal to protect the people, this is permissible with reservations. Torture, murder, extortion and so forth should not be used except under the most extreme, compelling circumstances.

Third, remember that the law of unintended consequences is real, and that perfection is not possible. So, he urges us to remember that the means chosen to do a thing usually determine the actual results achieved. Intentions matter little, consequences much, and millions of people have tried to do good by doing a little evil first. This almost never works in the long run. Rather, one wins tactical battles while losing the strategic war.

Thus he urges spies to go back to the gold standard rule of solving one's problems without doing harm, especially to innocents. Avoid harsher measures unless absolutely compelled by extreme circumstances. The argument that good ends justify any practical means to achieve them is a treacherous, slippery ethical slope. Down that slope lie the rationalizations that excuse murdering doctors in clinics or teachers in schools or children in a village as a method of war to accomplish political objectives.

Handling Agents

America's CIA has a category of career employee called a case officer whose primary job is to recruit and to manage (or "handle") spies from foreign countries (called assets or agents). Avoiding more jargon, the core point of this section is to point out that these agents often have families at risk, and a spy always risks his freedom or her life when s/he agrees to betray their country to benefit ours. This risk may be assumed for money, or it may be assumed for ideological reasons or for other reasons, although money and politics are by far the most common. Sometimes agents are blackmailed or extorted into serving their handlers, so coercion may be involved. But always the agent has put his or her life in the hands of the officer who handles them. This puts enormous responsibility on the case officer, and presents some extraordinary moral dilemmas.

For example, what do you do if your superiors order you to send your agent into a trap to serve the larger interests of the nation? There is a reason some agents are called "expendable" but that will not help you sleep better at night if you betray someone you have spent years building trust with. On the other side of moral dilemmas, what do you do if your trusted agent begins blackmailing you, by threatening to reveal your entire espionage operation to their counterintelligence people, for example? This could endanger many other agents in the field, maybe even you if you are in the country in question right now.

It is for reasons like this that "protecting sources and methods" is such a core value to so many intelligence professionals. First, the effectiveness of the operation is usually destroyed if it is discovered. But also they recruit each other to take mortal risks sharing secrets when the penalty for detection can include at best prison and disgrace, and at worst, torture and death. They tend to recruit each other after long periods of earning trust slowly. But spying is a business of deception

and betrayal, so sometimes these arrangements go awry. This is painful enough if it involves only individuals. If it involves war plans or national secrets, thousands of people may die because of bad decisions made in the darkness of false, incomplete or compromised information.

Analysis

Analysts are more like college professors who don't talk openly about their work than like the action commandos and sneaky divas called covert operators. Thus one might think their moral dilemmas are small, and they certainly would prefer to think so too.

But this is not true. Rather, this is an illusion encouraged by the "compartmentation of information" within official intelligence agencies. Analysts send their papers into a kind of black hole from which they seldom receive feedback whether anyone cared or took action on their recommendations. But the opinions of intelligence analysts can have profound consequences far from the desks where they were written. For example, one colleague spent three years of his life researching ways to destroy the economy of a small and already poor country. Economic warfare can have very profound effects. While many papers are ignored in official intelligence as in life, it is escapism to pretend that such analyses are never used, especially when covert wars are involved.

One cardinal sin among analysts has already been mentioned, politicization. Analysts are never, ever supposed to color their analyses to suit the prejudices of policy makers, even though policy people are often making very clear what they want to hear. Analysts are supposed to "speak truth to power" "without fear or favor," telling things like they are, no matter what. Of course, reality differs from theory here, since the easiest thing a policy maker can do (rather than changing their own mind) is to stop listening to one analyst and start listening to another who says what the politician wants to hear.

A reciprocal issue of especial importance to analysts is to avoid making policy oneself by what one writes. This is easy to say, but hard to do. Analysts are supposed to remain as objective as possible and to let the policy people do the policy. But being human beings, analysts inevitably develop opinions and even political values of their own.

This can become a significant moral dilemma when analysts warn about grave dangers, but are ignored by policy makers intent on other objectives. Those who warn loudest may be dismissed or just ignored by politicians who don't want to hear contrary views or who have simply already made up their minds on a course of action. Losing the ear of leaders is a serious issue to analysts; it is a grave issue to others when life and death is involved. Whether Iraq had active weapons of mass destruction (WMD) programs before the Gulf war of 2002, or not for example, generated great controversy when such weapons were not found. A closely related question was whether this was a failure of intelligence or of policy, since the policy makers had made their preferences very well known before hand. Thus many analysts in the CIA and elsewhere had to ponder what they should do when the leaders were clearly determined to pursue a course of action with great peril, and on false evidence, no matter what analysts wrote or said.

Whistle Blowers vs. Leakers; Treason vs. Saving the Nation from Mad Leaders

To "leak" secret information to the press is considered a cardinal sin among those for whom protecting sources and methods, and operational security are prime values. Yet to reveal criminal activity among governments is considered a virtue among the media and many citizens of democracies. When is a person bravely "blowing the whistle" on wrong doing, and when are they merely "leaking" secret information for bad purposes? These two interpretations involve exactly the same act, telling a reporter something that he or she wants to write about, but that someone else wants to keep secret. Finally, leaking information is as common as dirt among politicians. Who prosecutes them?

This dilemma is of the same kind, but much less severe than another which many intelligence professionals have had to face. What should one do if the Supreme Commander becomes insane, and orders things that put the nation itself at risk? Closely related to this is the issue of hubris. Derived from a Greek word, hubris means "overweening pride" or "dangerous arrogance" and it is an occupational hazard for kings, spies and professors. Any of these may come to believe that they are so special or so smart that rules which apply to lesser people need not be obeyed by them. Such overweening pride can lead to serious disasters if combined with power. Hubris is also extremely corrosive to wisdom which is quite a different thing from intelligence.

Most intelligence professionals work for governments, or if not for governments for Kings and other Supreme Commanders. They are pledged, and paid, to serve those institutions and individuals with great loyalty on some of their most difficult tasks. What does one do if the Commander threatens the lives of all the innocents in his domain? Issues of nuclear war and other WMDs make this not a theoretical question.

Here there may be (should be) a significant difference between dictatorships, police-states, and constitutional democracies. In constitutional democracies all power is ultimately derived from and vested in the people, and states are empowered in order to protect the people primarily. In Kingdoms and police-states power is held by a single man, or by one political party or government, not by the people *per se*. To legalists this is a very significant difference, because the relevant laws are certainly different. But intelligence professionals are distinguished by a degree of indifference to laws. At a deeper level, even democracies are ruled by men and women with mixed motives, and even tyrannies require a substantial degree of active support by the people they organize and oppress. What does one do if the Sovereign goes nuts, and threatens the very life of the state, and the lives of its people?

Do not expect an answer here, because this is the most delicate question intelligence professionals must face, and its answer depends on many nuances one cannot truly address in an academic exercise. But have no doubt there are reasons why sovereigns both value, respect, and fear their intelligence communities.

Just be advised that people who deal in the life or death of millions actually have to ask questions like that, and answer them. Like a commander in the field who must decide whether to blow up a building full of armed men who are killing his troops (plus a few dozen utterly innocent children held as hostages) these are questions that tear hearts apart. What to do when one must choose between evil alternatives? What to do when sacred values conflict? It appears that the hardest questions are often those where two “good” values come into conflict. These are the same kind of questions whistle-blowers ask. They have been taught from the beginning that revealing secrets can harm many people far away. But they also see something criminal, or dangerously wrong, which cries out to be revealed to the public that, in theory, the state is created to protect. What should spies or junior commanders do if their leaders become insane or grossly corrupt?

What is the responsibility of democratic citizens under the same circumstances? What about the ordinary soldier, pledged to support his leaders and his team? What about ordinary people, who also have great stakes in the life or death of their communities? These are difficult questions for anyone, but they are questions life presents from time to time. Citizens may choose to answer or ignore them, but sometimes intelligence professionals must decide concretely because the lives at risk are in their eyes.

Propaganda and Psychological Operations

The previous section may have left an impression that intelligence agencies rarely leak information to the press. On the contrary, this is a primary operational method for influencing political opinions. Amateurs call this propaganda, which is common as dirt in political discourse. Professionals use a near-science called psychological operations, which is more devastating precisely because such “PsyOps” are professionally designed, managed and deployed with the resources only governments possess. The evolution from propaganda as practiced by the Germans and many others during World War II to modern psychological operations is one of the darker chapters of spy history.

Space does not allow even an outline of techniques involved, except to note that they employ all the methods of advertising and public relations that are taught in business schools, as well as darker arts employed to destroy individual people’s minds or to hoodwink whole populations. Some of those darker arts were discovered during a period of great fear in America, when apparently “brainwashed” prisoners of war prompted a massive effort to find drugs or other methods by which individual beliefs and behaviors could be manipulated. That program, called MKULTRA among other names, remains one of the least discussed chapters of the hidden history of American intelligence. Of course, the Russians had their version too, and the British, the Israelis, the Chinese and the Koreans who started this ball rolling. It appears that most large intelligence agencies have some psychological operations capability in their inventory.

The primary ethical problem with psychological operations is that its foundation is calculated lying. In theory, the ultimate goal of intelligence agencies is pursuit of “truth” uncontaminated by the prejudices of top leaders, biases of the analysts, or by the propaganda of other nations that are ever intent to conceal their dark secrets. In theory, bumblebees can’t fly. In reality, even

simple propaganda often works, so it is routinely employed in statecraft. The problem is that lies sent to alter behavior in other nations, often “blow back” to contaminate thinking among domestic populations too.

This violates a bedrock principal of democracies, which is that the people need to know what is going on so that they can wisely select leaders based on realistic consideration of the policies they propose. For this reason the CIA was expressly forbidden from conducting propaganda operations within America when it was created. Unfortunately, even when the letter of this law is followed, modern technology makes a story planted in an obscure paper half way around the world instantly accessible to anyone who seeks it. Thus lies sown to bamboozle others far away may quickly blow back to contaminate domestic thinking. There is a reason many spies snort at public news.

Despite these grave complications of propaganda and psychological operations, it is important to recognize that there are some very good uses to which they may be put. For example, if one is about to destroy an enemy army, what is wrong with bombarding them with surrender leaflets first? This is now a standard practice, and when thousands do surrender, their lives are spared along with allied troops who would also die if compelled to destroy their enemy in close combat. And is it not better for professional interrogators to use sophisticated and less brutal means of persuasion to get tactical information from their prisoners of war, than to try torture which is ever a temptation?

Technology and the Surveillance Society

Not long ago, to bug a telephone required a human being to put a physical device on the phone or physical phone line, and to do that legally required an actual warrant signed by a live judge attesting to probable cause to believe that the owner was a danger to someone. Now the NSA (National Security Agency) can tap almost any ordinary telephone just by pushing a button thousands of miles away, and they do so every day. Controversy over the laws involved is being overrun by technical developments which make it ever easier to monitor anyone, and as importantly, everyone.

In fact, it is much easier to monitor anyone if you are routinely but secretly recording everyone, which is the darkest secret of modern eavesdroppers. When the “Echelon” system was adopted by the signals intelligence agencies of the United States, Great Britain, Canada, Australia and New Zealand, they relied on trapdoors built into almost every communications satellite deployed in space, or major relay station on the earth’s surface. These trapdoors split the signals sending a copy to massive arrays of supercomputers whose job was to scan everything looking for keywords or codewords or simply picking off all communications to any designated number for review by human analysts. That was 20 years ago; we have come a terribly long way since then.

Today, the more electronically connected you are, the more accessible you are to automated systems looking for “terrorists” or whatever they are told to look for. And it is not just phone or computer data. The average person in London, for example, is photographed or videotaped at least 50 times per day, by cameras installed to watch the streets and deter crime. Such systems are incredibly useful for looking back when a serious crime has been committed, because real culprits may then be observed, their faces analyzed by specialty software and coded like a fingerprint. Your cell phone can be used to track you, and a phone in a home can be turned into a microphone for others to listen with, even when the phone is not being used for its normal purpose. Technical enthusiasts drool at what modern digital devices can do, especially when employed by the secret services of major nation states. Civil libertarians despair, and they don’t know half of what is out there.

For just one more obvious example, your computer keeps the most detailed records on what you look for, write or do, and the same kind of trapdoors that were built into satellites were built into many mass market computer systems by agreement with the governments that could say yes or no to many aspects of business important to large corporations. So if they want to, they can peek from very far away and you will never know unless they knock on your door. The surveillance society is here. The question for professionals and for ordinary citizens is what to do about that?

One concept offered by some signals intelligence people is that of “minimum trespass” which roughly corresponds to the police ethic of “minimal force.” In other words, they urge their colleagues to pry as little as possible into the private lives of their citizens while doing the business of looking for “terrorists” or other criminals out to do harm. This standard is notoriously

weak because “minimal” is a very subjective concept and there is no real guarantee that the powers of surveillance won’t be used for private gain, or for those currently in power to cripple those who aspire to power. The latter is fundamentally undemocratic, but ever a temptation to governments anywhere. In police states, this is actually the main job of the security services rather than protecting the people *per se*. That presents ethical dilemmas to some, who quickly become not employed by the secret political police ... or suffer much worse fates.

A different conundrum presents itself. When one can look at what nearly everyone is saying or writing, one is immediately paralyzed by the vast volume involved. So most of the snooping is done by automated software instead of by human beings, and even those humans who must read the sifted gleanings are routinely overwhelmed by the volume of “potentially interesting” but ultimately irrelevant stuff that hits their screens. Second, to the consternation of professional intelligence agencies, the best media and the best academics are now getting more accurate answers to many questions faster than the professional spies. This is very disconcerting to intelligence professionals.

The reason why provides a clue to resolving the inevitable ethical tensions that come when people spy on everyone. The best media and academics must **collaborate** with others every day. So accuracy, honesty, and open information sharing are core values to them. When reporters or professors make mistakes, these are quickly exposed by others in the business, which is embarrassing. So when working on collaborative projects, these “open source” professionals routinely ask each other to expose their mistakes while material is in draft form, so that errors will be corrected before public release. This concept of open information sharing instead of secret keeping, and of collaborative searching for truth rather than solitary, aggressive attempts to penetrate information barriers, is absolutely central to the ethics and to the performance of top-quality media and academic people and institutions. Betraying people you share with ends the sharing; this is the misery of many spies today.

Restoring a more healthy relationship between spy agencies more sharply focused on consensus endeavors (like protecting the people) with the academic and media communities is the key to a revolution in intelligence affairs more fundamental than mere computer power. As I write, Google is trying to create a global brain accessible to all. Wish them well, because you can be

sure that dark forces will also try to build the brain, but they would like to keep its power entirely to themselves. This is the fundamental ethical dilemma for those in the electronic intelligence domain today.

Codes of Ethics for Government Agencies and Commercial Spies

There is a Society of Competitive Intelligence Professionals (SCIP) that concentrates on those who work for businesses, full-time or often as contractors. Their code of ethics is among the simplest and has been reproduced in hundreds of places, so we shall begin this section there. The University of Illinois has a collection of ethical codes from many sources at its Institute of Technology Code of Ethics website, <http://ethics.iit.edu/codes>. This site was gleaned from Jan Goldman's excellent book on the "Ethics of Spying," which has the unclassified versions of ethical codes from most of the main American intelligence agencies, and of a few international groups like SCIP, in its Appendix A. He also provides cases in Appendix B, which are especially useful for realistic training.

The SCIP Code of Ethics is:

- To continually strive to increase the recognition and respect of the profession.
- To comply with all applicable laws, domestic and international.
- To accurately disclose all relevant information, including one's identity and organization, prior to all interviews.
- To fully respect all requests for confidentiality of information.
- To avoid conflicts of interest in fulfilling one's duties.
- To provide honest and realistic recommendations and conclusions in the execution of one's duties.
- To promote this code of ethics within one's company, with third-party contractors, and within the entire profession.
- To faithfully adhere to and abide by one's company policies, objectives and guidelines.

As you can see, there is nothing here about industrial espionage much less blackmail, theft, assassination or the many other dark arts, except the injunction to “obey all laws.” If theory and reality were more closely related, we would have little to write about!

Government ethics codes face a more difficult problem, because many governments have special laws for their spies that grant them immunity from laws that apply to ordinary citizens. Some of those special laws can be found in the public domain, but many are secret. In America, the annual Intelligence Appropriations Acts often contain classified codicils related to current operations of political importance. Another source of special laws are “Executive Orders” by the President, most of which are published, and a range of other orders that are more or less secret. During Reagan’s time, these were called National Security Decision Directives or NSDDs. The First President Bush called his NSDs, Clinton called them PDDs, and George W. Bush issues NSPDs and HSDDs (the latter are Homeland Security Decision Directives). The acronyms chosen do not matter, the fact that special and often secret rules are created for spies does.

Furthermore, every national governmental spy agency expects its agents to obey most domestic laws, but specifically empowers many to go break the laws of other countries. And finally, agencies of police-states may or may not have any legal boundaries at all on their activities, but if any exist, these are widely seen as window-dressing only. So the gap between written codes and actual practice is, as one might expect, quite wide!

A brief look at assassination is in order here. In 1976 U.S. President Gerald Ford issued Executive Order 11905 to specifically forbid assassinating foreign leaders partly because CIA plots to assassinate Fidel Castro had become publicly embarrassing, and partly due to the historic memory of the murders of President John F. Kennedy and of Martin Luther King by dark forces. To this day the CIA denies any involvement in the murders of Patrice Lumumba of the Congo, Rafael Trujillo of the Dominican Republic, Salvador Allende of Chile and a long, long list of other political leaders and ordinary people despite vast international skepticism. And who doubts that America wants to kill Osama bin Laden today (2006) whatever domestic or international law says about that?

But let us be fair. “Targeted killing” is employed by many, many nations. The Russians certainly killed Bulgarian dissident Georgi Markov by inserting a platinum pellet loaded with ricin (a

specialty poison) into his thigh, and when they killed Chechen Rebel General Dzhokhar Dudayev, we actually helped them home in on his cell phone which provided the target data for the missile they used. The Israelis certainly killed most of the Palestinians who had been involved in the murders of athletes at the Munich Olympics (along with some utterly innocent people in Lillehammer Norway); and even the gentle French killed an innocent man who was sleeping on a Greenpeace boat they decided to bomb in New Zealand. When innocents die, it is always an “accident” in spooky-lucky land. Back to American sins, we wanted to kill an Al Qaeda leader in Yemen, so we blew up his car with a high-tech missile fired from a pilotless airplane. Four other people were in the car including an American citizen, but guilt by association is often assumed when intelligence agencies wage war. Death squads empowered by intelligence entities murdered six priests, their cook and her daughter at the University of Central America in El Salvador in 1989, and another assassin killed the Archbishop Romero while preaching at his church in 1980. The list of people murdered in Latin America, Africa and Asia alone by agencies of various governments would be too long for this book if it could be written accurately. And when politicians desire a fig leaf, some hire mercenary killers from the contract world. So do not be deceived when governments say they have “outlawed” assassinations. This is what propagandists call a “partial truth,” that is, technically true but quite misleading.

Most of these assassins thought that they were obeying the laws of their governments and whatever ethical codes their agencies employed for training. But deception and betrayal are the business of spies, and the principle tools called tradecraft have always been extortion, blackmail and murder or threats of murder whatever they say on paper or in public. So the presence of secret laws and special codes for secret agents is a central problem for those who would attempt to create a professional ethic for spies.

The official codes of the CIA, the FBI, the NSA, the DIA and the U.S. government in general are full of excellent words like “integrity” and “honesty” and avoiding conflicts of interest and such. This is not to denigrate excellent words and noble goals, but rather to highlight the difference between legalistic codes and the core of moral thought.

In the nature of their work spies must deal with issues that challenge the best moral thinking, and while most people who enter this strange business are not moral morons, they are also not Snow

White Bambi-kissers either. Many were military officers first, so many are accustomed to accomplishing missions as a primary value, some of which risk death of someone. So while codes, and rules of engagement, or lists of do's and don't can help, they cannot ever deal well with wrenching dilemmas like what do you do if terrorists threaten an entire city, but shield themselves with babies? Or what do you do if the leadership is insane, or just so blinded by lust for power or hubris that they would destroy society in their quest for some objective? What does one do, when the ancient laws of God and the modern codes of men are inadequate to the challenges before you? This is a question for you, dear citizen reader, as much as it is for spies.

Conclusion

Every era has pivotal forces or events that define that generation. The pivotal forces of today are Peak Oil, Globalization and the technical information revolution that has so empowered police-states and the wealthy everywhere. As we come down from the peak of global oil production, energy will become more expensive faster because the easiest, cheapest and best has already been used. Globalization and the information revolution make problems anywhere metastasize much faster than before, from emerging diseases to the latest device for spying on your neighbor.

Rather than engage in the global struggle between those who have and those who don't, it is the sacred duty of intelligence professionals during this generation to rise above the habits of the past. Your policy masters will give you many missions, some wise, others not. It is imperative for you to distinguish between the two, and to help your leaders to comprehend that the only way to beat this crisis is to save almost everyone. The nation is in danger and the children are in peril ... from ignorance and hubris, as much as from any other forces at work on this earth. Be professional, and protect them.

References:

1. Ethics of Spying: A Reader for the Intelligence Professional. Edited by Jan Goldman, 26 contributors, published by Scarecrow Press of Lanham, Maryland, 2006.
2. "Psychological Operations in Guerrilla Warfare." By "Tayacan," a pseudonym for a U.S. Army psychological operations professional who wrote this for the CIA for use during the Contra war in Nicaragua. Original text can be accessed at a Federation of American Scientists website, <http://www.fas.org/irp/cia/guerilla.htm>. A paper edition was published in 1985 by Random House, under the title Psychological Operations in Guerilla Warfare: The CIA's Nicaragua Manual, with essays by Joanne Omang and Aryeh Neier (human rights advocates who put the text in contextual perspective). Like the CIA's earlier torture manual (called "KUBARK" and still used during the 1980's) they would prefer you not read it at all, but especially not with "context" unauthorized by their publications review board.