Conference Proceedings, Intelligence Professionalism:

Ethical Basics, Codes of Ethics and the Way Ahead

February 16 & May 10, 2012
Executive Summary

This Summary of Conference Proceedings offers six alternative proposals to the Director of National Intelligence (DNI) on the issue of Intelligence Community (IC) ethos and the possible utility of a community-wide code(s) of ethics. This summary concludes that intelligence work is a “profession” in the traditional sense of the word and that, as such, the IC would benefit from an employee code(s) of ethics.

The National Intelligence University (NIU) hosted two Intelligence Ethics conferences over the past four months. The first conference discussed the importance of instituting ethical codes to assist intelligence professionals as they encounter morally ambiguous situations. Senior officials and experts shared their thoughts and experiences with 125 persons representing all major agencies in the IC. Later, on 10 May 2012, the NIU held a second conference for 40 persons in a workshop format. NIU students who had been enrolled over the past academic year in the Intelligence Ethics class presented six alternative intelligence ethos and code proposals to the workshop participants, with ample time for questions and answers about the merits of each proposal. The participants agreed that certain core principles captured a sense of commonality among intelligence professionals.

The Core Principles Highlighted in All Proposals:

- The Intelligence Profession: Expertise, Responsibility and Corporateness
- Guiding Right Behavior: A Code of Ethics
- A Unique Mission: Serving the American people

---

1 The statements of facts, opinion, or analysis expressed by conference participants are the personal ones of the participants and do not reflect the official policy or position of the Department of Defense or any U.S. Government agency. Review of the material does not imply Department of Defense or U.S. Government endorsement or verification of opinion or factual accuracy.
• A Call for Integrity: Speaking Truth to Power
• A Need for Accountability: Reporting “Malpractice”

The workshop participants concluded that there is enough evidence of an intelligence “profession” as to merit its own professional code of ethics. We consider ourselves to be professionals, as defined by our service mission, the unique legal, and ethical parameters within which we perform that mission, our specialized training, and our trust obligations to the American people. Broadly, the participants agreed that there is an intellectual necessity for thinking through ethical issues with wide participation in the community.

The participants broadly agreed that the current ODNI statement of IC Ethos (Service, Integrity, and Accountability), provided an appropriate ethos for the community. Moreover, the participants agreed that a more in-depth code of ethics would be beneficial, although it should probably be short (one to three pages). This code should embrace commonly shared principles and beliefs; new employees should be introduced to ethical issues during initial training with reinforcement throughout a person’s career to the point that shared principles and beliefs are embedded in community culture.

Overall, the participants believe that the DNI should put a central and senior-level emphasis on the issue of professional identity. In terms of the IC, the DNI should initiate a process of broadly socializing a code of ethics. This would further the practitioner’s sense of personal responsibility for his actions, as well as reinforce the trust relationship with the American people. The code of ethics should begin with senior-level circulation throughout the community, inviting comment and alternative views back to the DNI for working group review and/or a follow-on conference hosted by the NIU.
# TABLE OF CONTENTS

Introduction: Codes of Ethics and The Intelligence Community 5

Remarks by Keynote Speaker, Judge James Baker, 16 February 2012 15

Panel 1: The Intelligence Ethos 38
   Panelist 1: The Intelligence Community Ethos 38
   Panelist 2: IC Professionalism and The Ethos Issue 48
   Panelist 3: A Conspiracy Against the Laity? 50
   Panel 1: Question and Answer Period 59

Panel 2: The General Counsel/Inspector General Panels 61

Panel 3: The Collection and Analysis Panel 71

Remarks by LTG Ronald Burgess, Director Defense Intelligence Agency 82

Appendix 1: Proposed Codes 87
   - Version 1: IC Ethos Statement 87
   - Version 2: IC Core Values and Code of Conduct 88
   - Version 3: An IC Wide Ethos 92
   - Version 4: HUMINT Professional Ethos 96
   - Version 5: HUMINT Collector Ethos 98
   - Version 6: Analytic Community Ethos 101

Appendix 2: Recommended Reading List 105

Bibliography 111
Introduction: Codes of Ethics and The Intelligence Community

Overview

This summary offers six alternative proposals to the Director of National Intelligence (DNI) on the issue of Intelligence Community (IC) ethos and the possible utility of a community-wide code(s) of ethics. This summary concludes that intelligence work is a “profession” in the traditional sense of the word and that, as such, the IC would benefit from an employee code(s) of ethics.

On February 16, 2012, the National Intelligence University (NIU) hosted a first-of-its-kind conference, “Intelligence Professionalism: Ethical Basics, Codes of Ethics and the Way Ahead.” In part, this effort was spurred by the need to have a way to recognize the professionalization of the IC in the face of possible attempts to "politicize" IC analysis and products. The goal of this first conference was to discuss the importance of instituting ethical codes to assist intelligence professionals as they encounter morally ambiguous situations. Senior officials and experts shared their thoughts and experiences with 125 persons representing all major agencies in the IC.

This conference featured three panels. Panel 1 examined the subject “Intelligence Ethos and Professionalism.” What is the value of an ethos for intelligence professionals? What are the legal and moral sources for an intelligence ethos? What are the expectations of community clients? Panel 2 highlighted the IC General Counsel (GC) and Inspector General (IG) views on the possible value added from codes of ethics. The attorneys offered examples of difficult cases involving ethical dilemmas and discussed whether or not a code of ethics would have assisted in the handling of such delicate situations. Panel 3 explored the way ahead for an intelligence ethos.
and codes of ethics. The panelists represented the collector, analyst, and civil libertarian points of view. The outcome of the first conference was a consensus view on the utility of a code of ethics for the community, as well as a general understanding of what such a code might look like.

On 10 May 2012, the NIU held a second conference for 40 persons in a workshop format. NIU students who had been enrolled over the past academic year in the Intelligence Ethics class presented six alternative intelligence ethos and code proposals to the workshop participants, with ample time for questions and answers about the merits of each proposal. The participants agreed that incorporating ethical codes into community training and the workplace would enable employees to conduct the intelligence mission better by providing a strong moral compass for the conduct of their daily duties.

**NIU Methodology in Developing the Proposals**

The NIU taught three sections of the Intelligence Ethics course during the 2011-2012 academic year with roughly 50 military and civilian students participating from across the community. Each student was assigned to a small group, with an assignment to prepare a one- to two-page draft “ethos” statement or ethical code (for the entire IC, for a given agency, or for a given functional area, as decided by each group in consultation with the faculty member). Each group had available a range of resources, as outlined in the attached bibliography. Each group product was based upon the relevant missions, core values and skill competencies for the selected organization. Group submissions were then graded based upon originality, clarity of presentation, coverage of relevant issues, and use of key concepts. In total, the NIU students produced a total of six alternative proposals (attached).
Generally, the students defined ethics as the "moral principles that govern a person's [or organization’s] behavior or the conducting of an activity."\(^2\) Moreover, "intelligence ethics," was further defined as “a set of behavioral guidelines based on certain beliefs . . . regarding the role of intelligence in society." Moreover, students saw a reciprocal relationship between morality/ethics and the law. Often moral/ethical principles are more abstract and provide an underlying basis for laws (e.g., statutes and regulations); both also evolve over time. Born and Willis are helpful here: "Laws are necessarily general and abstract, leaving considerable leeway for interpretation by those individuals whose actions are regulated by them, as well as those who are responsible for enforcing laws.... [I]ntelligence officials must exercise discretion that 'defines that area of choice which is explicitly permitted by law or which exists by way of ambiguity inherent in law.' It is within this realm of legal ambiguity that ethics become a crucial guide to action...."\(^3\) In short, laws don't answer each and every dilemma facing intelligence professionals.

NIU Intelligence Ethics students participated in both conferences, and a representative from each group presented its draft code at the 10 May 2012 Intelligence Ethics conference.

The Student Proposals

All six student proposals highlighted one important point for the workshop participants: There is no agreement on what to call this ethical code. The submissions were variously labeled code of ethics, code of conduct, ethos, core values, and creed. In fact, the IC already has one Ethos statement (Service, Integrity and Accountability), derived from Objective 3.1 in the 2006 Strategic Human Capital Plan. While none of the student submissions critiqued that statement,


\(^3\) Ibid.
each expanded it to a considerable degree. The participants discussed this “labeling” issue, but
without reaching a consensus. However, the participants did agree that the DNI could retain the
current IC Ethos statement, and also add a code of ethics.

The participants agreed that certain core principles captured a sense of commonality
among intelligence professionals.

**The Core Principles Highlighted in All Proposals:**

- The Intelligence Profession: Expertise, Responsibility and Corporateness
- Guiding Right Behavior: A Code of Ethics
- A Unique Mission: Serving the American people
- A Call for Integrity: Speaking Truth to Power
- A Need for Accountability: Reporting “Malpractice”

The first set of proposals (1-3) revealed a complex theme that on the one hand
acknowledges the IC’s unique mission; but on the other hand also highlights a set of shared
common values and standards of conduct that are, in a sense, what defines us as “professionals.”
Implicit in all three is the belief that:

- The community has a trust (stewardship) relationship with the American people.
- Employees should focus on service to the nation while maintaining a sense of
  integrity and accountability.
- Intelligence practitioners are professionals with an ethical obligation to maintain
  high standards of care in terms of protecting sources and methods, an emphasis on
quality work (e.g., accuracy in reporting, eliminating bias, and collaboration), respecting the rights and dignity of others, and an obligation to report violations of law (e.g., a form of malpractice).

Proposal 3 is unique in that it begins with a creed written in the first-person singular form. This proposal has considerable merit in that it reinforces the personal, as well as the institutional, obligations faced by intelligence practitioners.  

The second set of proposals (4-6) included two focused on human intelligence (HUMINT) collector issues and one focused on analytic issues. Each of these documents starts with the same basic premise stated in the first three documents, but expanded those points within a functional perspective. The last document, Proposal 6, offers an expanded look at the “intelligence cycle.”

Areas of Consensus: A Way Forward?

The workshop participants concluded that there is enough evidence of an intelligence “profession” as to merit its own professional code of ethics. We consider ourselves to be professionals, as defined by our service mission, the unique legal and ethical parameters within which we perform that mission, our specialized training, and our trust obligations to the American people. Broadly, the participants agreed that there is an intellectual necessity for thinking through ethical issues with wide participation in the community.

---

The participants broadly agreed that the current ODNI statement of IC Ethos (Service, Integrity, and Accountability), provided an appropriate ethos for the community. Moreover, the participants agreed that a more in-depth code of ethics would be beneficial, although it should probably be short (one to three pages). This code should embrace commonly shared principles and beliefs; new employees should be introduced to ethical issues during initial training with reinforcement throughout a person’s career to the point that shared principles and beliefs are embedded in community culture.

The participants saw value in different approaches, such as an aspirational statement, a statement of core values or a code of ethics. Typically, professions use a code of ethics to help establish identity, as well as help regulate the unique activities of practitioners. In some professions, such as the practice of law, the code of ethics has a binding effect on attorneys and judges such that non-compliance may serve as the basis for a disciplinary action. Here, the participants noted the varying approaches within the IC. For example, the Federal Bureau of Investigation (FBI) has an “Ethics Pocketguide” that expands on the FBI Core Values with 50 pages of detailed information in various practice areas, while the National Security Agency/Central Security Service has a one-page statement of nine core values and the National Clandestine Service uses a handy pocket card that can be carried by each practitioner.

The participants agreed that the purpose of the DNI code of ethics should be to guide “right” behavior in morally ambiguous situations and help integrate the profession. The participants concluded that the DNI code should be aspirational, without the detailed rules, regulations or disciplinary standards that are usually implicit in a “code” (the participants were concerned that the term “code” has legal connotations). On one hand, a binding code that includes specific rules, including disciplinary standards, could help practitioners facing common
problems. But, on the other hand, the preparation of a binding code would be difficult, involving a lengthy and detailed process, and which might well result in another “regulation” that would sit on the proverbial shelf. Clearly, there would be considerable risk that such a detailed code would be overly restrictive, much as the Deutch Guidelines in the 1990s apparently inhibited needed collection activities. So, the participants thought that a non-binding code could be a better vehicle to build professional identity and develop consensus on important, shared values. Moreover, a successful, shorter code could lead—at a later date—to a more detailed code, if the community felt such a need.

The participants believed that the DNI should facilitate a code(s) for the community *writ large* (an umbrella code) with possible additional guidance by functional area (e.g., collection, analysis or special missions). An umbrella code for the community would help create that shared sense of professional identity. Here, there is a strong analogy to other professions, such as law, medicine or the military. In other words, a practitioner is a member of a broader profession, even though he or she may also belong to a narrower guild within that profession (e.g., the bankruptcy attorney or the fighter pilot). Clearly, such an umbrella code must emphasize the unique aspects of the intelligence practitioner.

Meanwhile, the community could also have more detailed codes that highlight the critical issues facing practitioners in different intelligence “guilds” or agencies. In this respect, HUMINT collectors in the Central Intelligence Agency (CIA) may have more ethical concerns in common with collectors in the Defense Intelligence Agency (DIA) than they do with analysts or other administrative personnel in their own agency. The participants noted that any such “functional” community code(s) would not necessarily replace any existing codes at the agency level; different agencies have varying mission requirements and cultures, and will likely need
different codes. In any case, while there may be strength in varying agency approaches to the central identity issues (who we “are” as professionals), any existing agency codes in the community should be clearly “nested” within the overarching community-wide concepts.

The participants concluded that appropriate ethical standards for professional conduct were essential in building and maintaining the trust of the American people in “who” we are and “what” we do.

Areas of Work Still Needed

What is the “jurisdiction” of the intelligence profession? The participants discussed – but did not agree on – the jurisdiction of the profession: Does the “profession” include collectors, analysts and others defined by our unique mission? Or, does the “profession” also include administrative and support personnel not necessarily unique to the intelligence community? What does it mean to be an intelligence professional?

Here, there are two general views on the professional jurisdiction. On one hand, intelligence practitioners could be analogized to lawyers: legal secretaries and paralegals lack the extended education, professional obligations, and ability to represent clients; such support staff are not considered members of the profession. However, on the other hand, intelligence practitioners could be analogized to military professionals. Intelligence practitioners, like military personnel, come from a wide range of educational backgrounds, and then go through training programs that integrate them into both the broader profession as well as a trade (e.g., an armor officer or a fighter pilot). Moreover, many people believe that the military profession includes both commissioned and non-commissioned officers. Indeed, non-commissioned officers are expected to take command on the battlefield if the officer becomes incapacitated. In
this analogy, all IC employees share some baseline characteristics, such as a security clearance and access to classified information. Some argue that such limited shared characteristics are an insufficient basis for an independent professional identity. Others argue that a broad, inclusive (a “big tent”) view would have the advantage of enhancing community cohesion. In short, the issue is how we approach our professional identity.

The participants also discussed two subsidiary issues. First, is there a possible role for a dissent channel in the IC, much as there is such a channel in the State Department that provides a relief valve on misguided policy decisions? The participants noted that such a channel could help professionals maintain a sense of personal integrity in the face of malfeasance, helping with the leaks issue. Second, does the IC require a professional disciplinary body, much as a state bar association oversees the work of attorneys, which would examine cases of ethical malfeasance? One conferee suggested that this could be an appropriate role for the Inspector General.

Recommendations

Overall, the participants believe that the DNI should put a central and senior-level emphasis on the issue of professional identity. In his classic formulation, scholar Samuel Huntington defined a profession as “a peculiar type of functional group with highly specialized characteristics.” He saw the distinguishing characteristics of a profession as expertise, responsibility, and corporateness. Here, neither our specialized expertise nor our responsibility (namely, the importance of our trust relationships) are in question; rather, the critical issue involves community “corporateness”: the claim that intelligence work is sufficiently distinct, with sufficient integration in the community, as to constitute a “profession.”

---

Ultimately, the issue centers on how professionals see themselves and how others see them, and this is often revealed through the way the profession self-organizes. Other professions, such as the lawyers or physicians, promote professional identity through multiple venues. There is a “top-down” approach in which a governmental agency (e.g., state supreme court or licensing agency) or a professional association promulgates codes of professional conduct, furthered in professional journals and training fora. There is also a “bottom-up” approach that involves socializing prospective and new members of the profession in educational settings. Both top-down and bottom-up approaches are mutually reinforcing.

In terms of the intelligence community, the DNI should initiate a process of broadly socializing a code of ethics. This would further the practitioner’s sense of personal responsibility for his actions, as well as reinforce the trust relationship with the American people. The code of ethics should begin with senior-level circulation throughout the community, inviting comment and alternative views back to the DNI for working group review and/or a follow-on conference hosted by the NIU.
REMARKS BY KEYNOTE SPEAKER, JUDGE JAMES E. BAKER

Chief Judge, U.S. Court of Appeals for the Armed Forces

Do’s, Don’ts and It Depends: Intelligence, Ethics, and the Law

February 16, 2012

National Intelligence University

Introduction

Thank you for inviting me today and thank you for having a conference on ethics. Ethics is at the core of the U.S. intelligence profession and mission whether you serve as an operator, an analyst, or a lawyer. Of course, at first glance, there is a temptation to smirk and say something about “intelligence ethics” being an oxymoron in a field dedicated to blackmail, bribery, and the theft of secrets. But as you well know, there is far more to the intelligence mission. Moreover, intelligence ethics -- personal, institutional, and cultural -- is critical to all aspects of the intelligence mission. It may be the essential intelligence value.

Ethics allows intelligence personnel to withstand the pervasive decisional pathologies that operate in the intelligence context including speed, secrecy, and the security imperative itself. Personal and institutional ethics are the firewalls that guard against the slippery slope of careerism, risk aversion, and politicization. Most importantly, ethics distinguishes intelligence service and services in democracies from those in authoritarian societies. All intelligence services operate under law; it is the ethical culture that defines and distinguishes the U.S.

---

6 For example, Russia’s intelligence apparatus was created by the Law on Foreign Intelligence of the Russian Federation, 1996, No. 5. China’s Ministry of State Security (MSS) was created in 1983 by combining previously existing espionage, counterintelligence, security components. Interagency OPSEC Support Staff
intelligence community and effectively subordinates that community to the rule of law and constitutional values.

Outline

In my time today I would like to do four things. First, I will provide a positive definition of intelligence ethics. Second, using that definition, I will describe a range of situational challenges intelligence officials typically face. These situational challenges reside between the obvious do’s and don’ts of intelligence conduct. As a result, I call this the middle grey, because the correct ethical answer will depend on context, not on a particular rule or code. Third, I will briefly describe a few of the don’ts of intelligence practice. Since I hope most of the don’ts are apparent, I will reference just a few, but they are important in preventing a skid down the slope of moral relativity in intelligence practice. Finally, I will identify a few principles for ethical conduct that should help intelligence professionals, including lawyers, address the ethical challenges of intelligence practice. In doing so, I will briefly consider the link between law, ethics, and morality.

I. A Positive Definition of Intelligence Ethics

Let me start with a definition of intelligence ethics. If you do not define the term then you cannot hope to know when and whether you have met its requirements. The tendency with ethics, especially for lawyers and the government, is to focus on the things one cannot do. The Model Rules of Professional Conduct are like that. So are the Principles of Ethical Conduct for

Federal Officers and Employees. The better course, however, is to focus on a positive definition of ethics.

Intelligence is the essential national security tool. It informs the use of all the other tools, and thus should be used in a positive as opposed to passive manner. That makes the duty to act, rather than to avoid, an essential intelligence ethic.

Moreover, a positive definition better guides us through the majority of situational dilemmas intelligence actors actually face. These are challenges that are not answered by a rule saying “do” or a rule saying “don’t,” but by the contextual application of the three positive principles that follow.

A positive definition of intelligence ethics should include at least three elements:

(1) **Truth-telling.** The essential ethic of intelligence is truth telling, a search for the truth to inform decision and prevent short and long-term surprise. This is the analyst’s mission and it is the case officer’s mission as he or she tries to identify, locate, and obtain information to supplement other sources of information. A lawyer might call this the substantive element of intelligence ethics.

(2) **Doing the Right Thing the Right Way.** Ethics is not only about doing the right substantive thing it is also about doing it the right way. The right way means it is consistent with U.S. legal, ethical, and moral values. These values include a commitment to operating within a constitutional system of shared and separate powers among branches. It also includes a commitment, as stated in the National Clandestine Service’s own informal code of ethics, not to use tradecraft internally.

---

The right way also means it is consistent with meaningful and timely process. Ethics allows intelligence personnel to address the pervasive pathologies of national security decision-making and, for that matter, intelligence activity: secrecy, speed, the culture of security, as well as the range of personalities that invariably find their way to this field. Because there are fewer external and structural opportunities to validate intelligence choices and assumptions, “the right way” is even more important in the intelligence context than in other contexts where validating mechanisms of internal and external appraisal and adjudication exist.

Consider for example rendition and targeted killing. Neither concept on its own presents a correct substantive answer; rendition and targeted killing are not inherently lawful or inherently unlawful. Whether their use is lawful and ethical will depend on the circumstances. That means that an ethical process of decision should not only seek the right security result; it should also necessarily strive to find the result the right way by identifying factual strengths and weaknesses of each proposal, policy merits and risks, and legal arguments for and against it. Moreover, because the process is not compelled by law and is subject to minimal external oversight, the particular process used will ultimately determine which views are heard, if at all. As a result, how this process is designed is a matter of ethical choice.

(3) Mission Context and Value: Third, intelligence ethics is informed by the intelligence mission, its importance, and its core components. The intelligence instrument serves four essential purposes: it informs decision; it prevents tactical and strategic surprise; it prevents attack; and it provides an affirmative national security tool. Intelligence ethics should take these mission elements into account. Thus, if one’s mission is to prevent terrorism by, or proliferation of, weapons of mass destruction, then one’s institutional and personal ethic should not only include truth-telling but also a positive ethic of risk-taking and ego subordination for the benefit
of the greater good. However, where the purpose served is only tangential to a core intelligence mission, one’s tolerance for ethical deviation or risk should diminish accordingly.

“Ethical conduct” is also a positive national security value in the intelligence context as it is elsewhere. First, an intelligence institution that does not stand by its commitments will soon find it has fewer agents and fewer liaison partners.

Second, adherence to ethical conduct can advance the intelligence mission. This is illustrated with reference to the story of case officer Milt Bearden, who worked with northern tribals during the Soviet occupation of Afghanistan. Upon his arrival, he was shown a picture of a Soviet pilot who having parachuted safely to the ground then shot himself in the head. Bearden stated: I was shown a photograph of a Soviet pilot in a silver flight suit, up to his waist in snow, skin burned by the relentless sun, with a bullet hole in the side of his head. His Tokarev semi-automatic pistol was still clutched in his hand. He had killed himself rather than be captured by insurgents. Back then, Soviet pilots had it particularly rough when captured.8

He did not want to be tortured to death. Bearden noted that such a practice violated Geneva principles requiring the humane treatment of prisoners. It also made no intelligence sense. Dead pilots do not provide intelligence. In time, he persuaded the tribals in his district to treat prisoners humanely, resulting in an increase in intelligence and even defection.9 In inverse fashion, we have also seen the negative impact on national security when America’s commitment to ethical conduct comes into question, regardless of the legal arguments that could be made for or against such conduct, as in the areas of detainee treatment and surveillance.

---


9 Ibid.
II. Ethical Issues – Navigating the Middle Grey

I have defined ethics not in relation to what one is not to do but rather in relation to the positive performance of duty. In the intelligence context, that means truth-telling, doing things the right way, and placing mission accomplishment first and in context. Reference to each of these positive elements in turn permits the actor to better address one’s conduct when the correct answer is not clear or falls into a grey area.

When I was in the executive branch, we used to have required ethical briefings. They were almost completely irrelevant to the practice of government. They told me things I already knew or should have known about conflicts of interest and self-dealing. The briefings did not address the hard issues an employee might face in that big middle area between the do’s and don’ts of the rules, like when and whether to speak up at a Principals meeting, what to do when a cabinet officer claims he told you something when he did not, or when it is appropriate to interrupt a briefer when he is not quite right, but the point is tangential.

I have chosen four rubrics as a means to identify some of the grey areas that intelligence actors face in the national security process. There is nothing scientific about these groupings. I have chosen examples that might get overlooked. They are “challenges,” because while we can all agree in the abstract that one should not lose essential nuance when briefing an issue, intelligence officials may be put in a position where they are acting on a continuum between ideal process and bad process. If you are only given two minutes at a meeting to brief a subject, how do you do it so that you will not unwittingly “shade” the truth or lose essential nuance?
My first category I call “Parkinson’s Law and Bureaucratic Games.” It is named for a little book written by Northcote Parkinson and published in 1957 titled *Parkinson’s Law*. The book is full of bureaucratic insight and knowledge. Parkinson, for example, is the person who coined the phrase “Work expands so as to fill the time available for its completion.” He also explains why an office manager will want to have two deputies: the deputies will tire themselves in rivalry as opposed to seeking the boss’s position. Because the book was written in 1957 from the vantage point of the University of Malaya, it also conveys the message that there are inherent and timeless pathologies in most bureaucracies. Knowing these pathologies, we are better prepared to mitigate them.

One of these timeless pathologies is the tension intelligence analysts and lawyers face to “get to yes.” In the intelligence context, getting to yes may mean providing an absolute answer, or a “correct answer,” to an unknowable question of fact or statement about intent. The challenge is compounded when the intelligence actor wants to be perceived as a team player. This is a natural and appropriate instinct when one is in fact on a team, and a vital team at that. A shared sense of mission is what allows the analyst or lawyer to work long hours, deploy to the field, and take risks in the judgments he or she reaches. However, there can be a thin line between esprit de corps and mission commitment on the one hand and a loss of objectivity that undermines truth-telling on the other.

One might call this latter risk “clientitis.” The risk may be heightened where the analyst or lawyer is collocated with the operator or for that matter the policymaker, like CIA lawyers assigned to Directorate of Operations (DO) divisions or judge advocates serving directly with
battalions. There is no correct answer. If one believes in the law or that intelligence should inform decision, then one should favor co-location. The analyst and the lawyer should be together in the room when decisions are formed and not just when they are made. The ethical response, therefore, is not to separate the intelligence specialist or lawyer from the policymaker but to spot the risk and then mitigate against it. This might be done by focusing on the positive definition of ethics presented above: truth-telling, the right thing the right way, and realizing that mission success requires effective role playing.

Role playing for a lawyer and an analyst means calling it as you see it as opposed to calling it as you or the policymaker might wish it to be. It also means focusing on one’s substantive legal or intelligence function rather than assuming the mantel of a policymaker or operator. This requires an understanding that factual and legal accuracy will better advance the mission than conformity and that operators will take greater risks in the field if they believe they are on firm legal footing; getting to “yes,” when “no” or “maybe” are better answers does not provide such a footing, even if it may please the recipient at the time. Finally, role playing for a person in a support function, like law or intelligence, involves subordinating one’s own ego to the interest of the mission. A quiet personality will have to stand up; an aggressive personality may have to sit down.

Additional safeguards may consist of a process of internal but external legal review, or in the case of analysis, red team review. Declarative codes of conduct are also useful in setting standards and shielding employees who are perceived to have too rigorously adhered to their norms. Like the law itself, such codes can be used as citations when the intelligence actor encounters bureaucratic obstacles blocking the performance of duty.
Another bureaucratic pathology might be called “two-timing.” This occurs when an actor says one thing to one audience and another thing to a different audience--each statement modulated to favor the expectations of that particular audience or elevate the comfort or status of the speaker. This is the classic dilemma we all face in our communications with others; no one wants to be the bearer of bad news. Let me give a couple of Washington examples.

Two-timing might describe the policymaker who says one thing in a Principals meeting (or perhaps nothing at all) and another to the reporter after the policy proves unworkable. It might also describe the intelligence actor who is asked by policymakers what further authority or resources his agency or program may need to accomplish the mission, to which he responds “Can do!” thus demonstrating his leadership up the chain of command. This same official might then return to his agency and report that he had asked for the moon and was rejected, demonstrating his loyalty to his bureaucratic constituency down the chain of command. The official has therefore appeared to please or accommodate both constituencies. He has also managed to shift the blame to the policymakers for any later shortcomings or perceived “failures.”

This scenario presents an obvious ethical inconsistency through delivery of different messages to different audiences. But it also defeats the truth-telling function. Why? Intuitively, where the parent agency or office is not aware of the need for additional authority or resources, it cannot make informed choices or address the problem. Alternatively, it cannot put a denied or modified request into the context of broader policy and thus mitigate the impact on morale and welfare at the effected agency.
Consider the hullaballoo about the CIA’s internal Deutch Guidelines for the recruitment of agents suspected of bad acts. The Guidelines followed the disclosure in the 1990s of the recruitment of a Colonel in Guatemala who was directly implicated in torture and murder. According to press reports, the Guidelines did not prohibit the future recruitment of bad actors, which is after all a necessity in certain areas of intelligence endeavors. But they did require headquarters approval in some cases, thus permitting greater accountability and contextual analysis of the risks associated with recruitment and the determination that it was worth the potential intelligence gain.

Following the 9/11 attacks, the Guidelines were condemned as an impediment to the recruitment of agents in the field. They likely were—a case officer is not well positioned to recruit an agent if at the moment of opportunity he or she is required to delay “the ask” in order to seek permission. However, if there was internal objection to the guidelines before 9/11, it was internal and muted, and certainly not conducted with the same rigorous disclosure to the press and external agencies as the objection after 9/11. Indeed, there is no indication the issue was raised with the NSC at all.

The problem of sending mixed messages up or down parallel bureaucracies is compounded in the intelligence context because secrecy and compartments prevent the correction by actual knowledge that might come with media disclosure and public debate. My point is not to pass judgment on a particular historic scenario. It is to point out how the practice of two-timing can undermine truth-telling, just as blow back from a covert action can do so by creating the perception of a ground truth that is in fact the product of one’s own creation. If there is an impediment to intelligence activities, the duty is to identify the impediment before rather than after the fact so that conscious choices can be debated and appropriate adjustments be made.
Finally, truth-telling also involves truth finding. In the context of secrecy and compartments, one cannot afford to wait to get asked. The analyst, operator, and lawyer must make themselves available and volunteer their input and service. Silence should be treated like an invitation to ask the operator or policymaker where the meeting is occurring.

(2) **Presentational Issues**

The next grey area I group under “presentational issues.” In this rubric comes a series of related matters like “shading.” This is when intelligence actors consciously or, more likely, subconsciously lean toward a preferred policy view or outcome. In the abstract, this may be the product of gross careerism, an effort to garner favor. However, for the most part, I believe shading occurs because people generally want to be helpful and when one is dealing with national security challenges, that tendency is especially strong.

This same tendency can also lead to a second presentational issue: the loss of essential nuance. Key words, phrases, or caveats can be dropped for a variety of reasons, including overt pressure on the presenter or time constraints on the speaker. There is nothing inherently unethical about summarizing intelligence; it is a necessity. That is what an intelligence brief is. One cannot very well present the full National Intelligence Estimate (NIE) every time a question is asked on a particular subject. Neither can one sort through all the raw data. The key to briefing is not to lose the essential nuance in the conveyance, including the identification of meaningful dissent. This is an ethical issue, of course, if it is the product of intentional pressure. It is also an ethical issue, whether done overtly or not, if the omission of essential information undermines the truth-telling process or the briefer does not have the wherewithal to insist on being heard out.
There are a number of situational methods to guard against shading and the loss of essential nuance. First, one might consider and focus on their ethical duty, which is the purpose of having an ethical code to begin with. Just as it is useful to define what the secret is that one is trying to protect, it is also helpful to identify the elements of the essential brief and determine that those points will be made no matter what the interruption or time constraints. It also helps to recognize that cross-examination of the analyst or the lawyer is appropriate. It is part of an effective process to test assumptions as well as statements of law and fact. The analyst and lawyer should not assume that such examination is the product of politicization or forum shopping rather than a genuine and shared desire to find fact and inform decision. They should embrace the opportunity to test their reasoning and truth-telling.

The analyst and lawyer can help themselves here by making careful distinctions between law and legal policy, or between fact and judgment. Sometimes consumers hear only what they want to hear. The quest for percentages may present special problems as well, just as a lawyer’s quest for evidence may do the same. Some intelligence judgments will simply not lend themselves to definitive statements of likelihood, just as much intelligence product would not qualify as evidence in court. Finally, if the analyst or lawyer needs more time, he or she should ask for it provided that the person knows and commits to meeting any real world operational deadlines.

(3) Informational/Decisional Issues

A third grey area has to do with the sharing of information in meetings, up the chain of decision, down the chain of decision, as well as with one’s peers. A number of informational issues recur in the intelligence-policy context.
First, when should one speak and what should one share at a policy meeting, be it a Principals Committee meeting, Deputies Committee meeting, interagency working group, or internal department or agency meeting. Should the answer change if you are a backbencher? Should you indicate where there is dissent? Ask questions about what is not known? Second, when should you share information up the chain of command? Third, when should you share information down the chain of command?

In the abstract, there are no “textbook” answers to these questions. On the one hand, a perceived lesson of 9/11 was the necessity of sharing more information among agencies in order to “connect the dots.” On the other hand, there are also legitimate reasons not to share information, such as the necessity of protecting sources and methods of intelligence gathering, as well as the need to minimize the distribution of information involving U.S. persons or that is privacy protected. In addition, while the answer may seem obvious in the abstract, that is, you should share information “when it is important,” it is also the case that given the volume of information that principal officers may receive from multiple sources, one of the essential functions of a staff person is to sift through that information and identify the truly important and actionable from the merely important.

How can one prepare for these issues in an ethical manner? First, it is helpful to think scenarios through in advance rather than resorting to dogmatic or instantaneous judgments. Likewise it is helpful to sit down with the principal or the client and ask these same questions in advance of any need. Second, when receiving information one should ask, who is on distribution and who is not, and if not, why not? One should also ask on what basis may, or must, I share the information and on what basis must I withhold it? One should also identify for decision-makers and recipients any process deviations and why they have occurred. Otherwise, the recipient may
conclude that the process has been observed and perhaps assume that the relevant actors concur in a judgment and all the facts known to the U.S. Government are in fact known and presented.

Are these ethical issues? Yes, if the answers undermine the essential intelligence ethic of truth telling and knowledge dissemination. They are also ethical issues if the answers to the questions derive from ego or a desire for bureaucratic power rather than mission necessity and efficacy. For although there are no correct answers, there are incorrect answers to these questions. Knowledge is power, as the saying goes and some bureaucrats like to conserve their power by controlling the dissemination of knowledge.

This manifests itself in different ways. “Hoarding” describes the bureaucrat who saves the most important or sensitive information for himself, allowing others to operate with an incomplete picture until he provides the missing piece. “Hiding” occurs when the official knows information cuts the other way, or that essential information is missing, but does not reveal that fact in the memorandum, report, or brief. “Camouflage” describes the process of hiding an important piece of intelligence inside the confines of a larger document so that one can assert that he has complied with his obligation to report, up the chain of command or to Congress, without drawing attention to the matter or being cross-examined on the facts.

Of course, one who is adept at these stratagems will also take care to discard “Old Maid” when the question is asked from above: “Who knew and why wasn’t I told?” Some are better at discarding Old Maid than others. This occurred to me once. The National Security Advisor (APNSA) wanted to know why he, and by extension the President, had not been told an important piece of information. The very senior agency official responsible assured the APNSA that the President’s own national security staff had been told. The fault therefore lay not with the
agency in question, but with the staff. When pressed on who had been briefed, the very senior
government official indicated “the Legal Adviser to the NSC.” To which, the APNSA
responded: “You mean Jamie?” “Yes,” the official confirmed, “I briefed her myself.” The
problem was that at the time, this particular “Jamie” was a male.

One is wise to test the motives when information is not being shared or shared
completely. If one cannot tie this approach to a positive ethical duty – truth-telling, the right
process, or the mission - one should be skeptical about and consider whether Parkinson’s law is
afoot. Of course, good process will mitigate many of these concerns, providing in a timely,
tested, and meaningful way for the standard sharing of information up and down the chain of
command. It would seem too that, in an ethical process dedicated to truth-telling and truth
finding, one should err on the side of disclosure to those with both a clearance and need to know.
Good process, in short, helps eliminate or mitigate the human factor in the manner in which
information is identified and disseminated.

(4) Risk-Taking and Risk Aversion

The final category is risk-taking and risk-aversion. These take many different forms both
in the field and at headquarters. Risk-taking, for example, certainly includes the taking of
physical risk in the field. It also includes the exercise of moral courage, perhaps in telling a
President that the intelligence does not support his assumptions, the lawyer calling the law
straight in the face of pressure, or the case officer who comes to realize and reports that his agent
is not what he claims to be.
Risk aversion takes on different forms as well. The term is perhaps most used with derision for those who are perceived to hold back in the field out of concern that their actions will get second-guessed in Washington. But policymakers also engage in risk aversion when they do not provide clear and/or accountable mission guidance. Intelligence actors engage in risk-aversion when they default to rote source and method protection without first determining whether more information can be shared in public in support of U.S. policy and actions. Analysts engage in risk aversion when they unduly hedge or refuse to offer a “best judgment” from uncertain facts. Lawyers do too when they refuse to put something in writing so as not to be bound to their views. This might be viewed as ethical if it is done to avoid tying the client’s hands when the facts are unknown or evolving; but it is less defensible if done to avoid accountability for one’s views or because the answer to the client’s question is always yes.

Here too, like so much else in the middle grey, there are few absolute or correct answers. Wisdom is another word for risk-aversion if the proposal at hand is a bad idea. Too much risk-aversion and an analytic judgment is meaningless; too much risk-taking and it is reckless. There are, however, some buoys that may guide one through these rocks and shoals.

First, intelligence actors should recall that an essential positive ethic of the intelligence community is to act rather than to avoid, to inform and prevent, not to sit and observe. This ethic favors risk.

Second, risk should relate to mission—the more important the mission, the greater the risks that should be taken. The more important the need for information or the source, the greater the leeway or tolerance should be permitted in the recruitment of agents. Likewise, the more important the mission, the more likely lawyers should get to no, and do so with honor.
That is because the more important the mission, the harder and further operators and policymakers should push to the limits of the law. This is the security imperative to which I referred earlier.

The greater the risk to national security, the harder the security specialist will and should push. Invariably, he will push too far, because the security specialist will and should always want to go one innocent suspect too far rather than fall one terrorist or spy too short. Understanding this imperative, a good process will provide for meaningful checks to validate and to confirm the use of national security tools. Such validation not only upholds the law and public support for the intelligence mission, it allows finite resources to be shifted to real threats. It also means that if the lawyer is not saying no, the security specialists are not trying hard enough or the lawyer has been captured by the mission or the client and is always getting to yes.

Third, risk-taking and risk-aversion depend in part on bureaucratic and institutional culture. Different cultures respond differently to similar circumstances and directions. Some agencies operate by the book. Others celebrate independent action. Compare for example, the different stereotypical manner in which an Army Ranger, SEAL, or Marine might respond to a mission to kill or capture someone with the manner in which a lawyer, diplomat, or perhaps an intelligence officer might do the same in terms of methods, means, and risks. Those who authorize the taking of risk should be aware of this variance.

Finally, where the law is clear and clearly invoked, operators will take greater risks in the field. It also follows that, where the President acts pursuant to Congress’s delegated authority as well as his own, he will act at the zenith of his authority. This is not just a constitutional truism
and a restatement of the Youngstown paradigm, it relates directly to risk-taking and risk aversion. Where operators know they are acting consistent with statutory and executive authorization, they will act with greater clarity and with less doubt of second guessing.

III. Just Plain Wrong

So far I have focused on situational ethics and the importance of risk-taking. However, a positive definition of ethics that accounts for risk as well as the nature of the mission can serve as an invitation to moral relativism. It also can lead to an ends-justifies-the-means outlook. However, there are safeguards against such a slippery slope.

One safeguard is the ethical obligation to do the right thing the right way. That puts a lot of emphasis on individual choice as well as the potential for equally well-meaning officials to reach inapposite results on process and substance. Hard breaks are necessary as well.

One such fire break is law. There is no blanket exception for intelligence activities in U.S. law. The law, including U.S. criminal law, applies to U.S. intelligence activities and conduct unless a specific exemption applies. This is reflected, among other places, in the National Security Act of 1947 as amended, which states that a finding may not authorize a covert action that would violate the Constitution or any statute of the United States. Likewise, recurring authorization language states that the authorization of appropriations shall not be deemed to allow conduct that is not authorized by the Constitution or laws of the United States. It is also

---

10 Youngstown Sheet & Tube Co. v. Sawyer (Steel Seizure), 343 U.S. 579, 635 (1952) (Jackson, J., concurring).
reflected in the informal National Clandestine Service code of ethics, which expresses loyalty to the Constitution as an essential ethic.  

Following the law is not only required and ethically sound, it also makes national security sense. Meaningful adherence to the law projects a critical national security value, distinguishing U.S. intelligence practice from those of authoritarian regimes, as well as encouraging risk-taking, as explained earlier. It also helps to sustain public and political support for an institution that some may view with skepticism in a democracy. Restated, the failure to observe the law may quickly result in the advent of additional restrictions and budget reductions. Moreover, once trust is lost, it can be particularly hard for the intelligence community to win it back given the asymmetry between the non-disclosure of successful actions and the repeated discussion of “failures.”

Where statutory law does not itself expressly reach or prohibit conduct, additional prohibitions may be found in executive directives of both an unclassified and, perhaps, classified

\[11\] This code reads in part:

**INTEGRITY**

We exhibit the highest standards of personal honesty. We do not employ the methods of our craft against ourselves.

**LOYALTY** to

The Constitution • Our Mission • Those who work with us • Our organization • Our Colleagues • Ourselves

**PROFESSIONALISM**

Discretion - Protecting How and Who

Risk Taking - Accepting Danger

Accountability - We Take Responsibility

Discipline - Physical and Mental toughness, Personal Sacrifice
nature. Executive Order 12333 as amended by Executive Order 13470, for example, expressly prohibits human experimentation. The directives also carefully regulate the collection, handling, and dissemination of information about U.S. persons.

Beyond law and directive, culture provides some absolute “no’s” as well. The politicization of intelligence or what a lawyer might call directed verdicts by intelligence analysts falls into this category.

IV. Conclusion: From Model Rules to Role Models

There is no greater source of ethical guidance than role models. Role models inspire. They define standards. They guide. And they are adaptable to need. Because ethical dilemmas do not always repeat themselves, the examples of role models are as important as any case-study or rules of conduct. Indeed, usually when one discusses “a principle” of intelligence or legal practice one is really thinking about a particular person and how that person dealt with a dilemma from which the principle is derived. The military might call such principles “lessons learned.” An academic might call them “history.” No matter the term, these principles move beyond exhortation because they are grounded in concrete example.

Role models remind us that if someone else can do it, we can too. Good role models minimize our excuses for not doing the right thing when presented with more than one path to follow. From role models also comes the strength and capacity to withstand the pressures of national security practice. When I was on the spot, I was not thinking about the Model Rules or even the law. I was thinking about my role models. I wanted to live up to their example and I did not want to let them down. But I am sure that I did let them down, and that I do, and then I
look to my role models for a sense shelter, knowing that trying your best is not the same as perfection and that grace is a form of honor.

My list of role models is as long as it is varied. As you can see from the pictures there are lawyers. Some you have heard of, like Nelson Mandela and Aung San Suu Kyi; some you have not, like Peter Murphy and Joseph Welch. There are government officials, like civil rights Judge Frank Johnson and General George Marshall. My role models also come from literature and history. Perhaps most of all they come from the private life, the private heroes of my life, like teachers, family, and friends. People you do not know and will never have heard of.

I have found it useful to have lots of role models. That may be a reflection of need. It certainly reflects respect. It may also reflect a sense that part of the trick is finding the right role model for the circumstance presented.

My list has also grown as I age. I do not think one is ever too old to try a little bit harder to get it right or at least try a little hard to do so by reaching a little higher for someone else’s example. That means, of course, that as you watch others, someone may also be watching you to see how you handle a particular circumstance and conduct yourself with others. I am thinking here of Jack Downey, who I knew of for many years but only met in the past few years. He is a Superior Court judge in Connecticut. But most of you know he did not start there. As a young CIA case officer, he was shot down over China and survived twenty-one years of confinement. He returned neither broken nor bitter. He went to law school, married, raised a family, and for over thirty years has served his community of New Haven. You will not find a better example of dignity and grace. And if you think you are having a bad day, think about him.
My goal, of course, is not to convince you to have my role models as your role models nor to have you validate my selections. It would be peculiar to say the least if you had my mother as your role model. Rather my goal is to prompt you to consider who your role models might be and what is it about them that inspires and guides.

I have thought about that a bit myself and think there are some common themes. Each of my role models I believe has or had a keen sense of mission, whether that mission was demonstrated on the beach at Normandy, in the courtroom, in a Pentagon hallway, or in a commitment to teaching others to read. In short, all of these individuals were motivated by a commitment to something greater than themselves and their own self-interest. They did not lose sight of this greater cause in moments of stress or occasions of personal opportunity or peril. It was ingrained. As a result, their first instinct was to do the right thing the right way or at least try to do so. In contrast the official who places career, promotion, or salary first, must first engage in a cost-benefit analysis to determine and balance personal cost and risk against doing the right thing.

Moral courage – a commitment to do the right thing - derives from an individual’s ethical identity and how the individual defines his or her personal mission. These people, I believe, have a strong sense of ethical identity from which they derive inner strength. This strength is not born of righteousness. It comes from a sense of modesty reflected in the value that one should always commit to doing one’s best, without the arrogance of assuming success. This is reflected in a quote from Abraham Lincoln that Frank Johnson kept on his desk: “I do the very best I know how; the very best I can, and mean to keep doing so until the end. If the end brings me out
all right, what is said against me won’t amount to anything. If the end brings me out wrong, ten angels swearing I was right would make no difference.”

Doing the right thing is not always easy, and for lawyers at least, it is rarely rewarded or recognized, except in the measure of our own self-respect. That is why I keep a quote in my office from the American educator, Whit Griswold. It serves like a locker-room talisman as a reminder to try to my best each time I enter or leave the office. “Self-respect cannot be hunted. It cannot be purchased. It is never for sale. It cannot be fabricated out of public relations. It comes to us when we are alone, in quiet moments, in quiet places, when we suddenly realize that knowing the good, we have done it; knowing the beautiful we have served it; knowing the truth we have spoken it.”

Codes of intelligence conduct help to define the identity of the intelligence profession. However, it is our role models that go the step further and help define who we are or hope to become as individuals and intelligence professionals. I hope that my remarks in some small way will remind you of your own role models and in doing so help you live up to the intelligence virtues, and self-respect, I know you already practice.

---


13 Alfred Whitney Griswold, President, Yale University, Address to Yale University (June 9, 1957).
PANEL 1: THE INTELLIGENCE ETHOS

The panelists are Panelist #1 (NIU), Panelist #2 (National Defense University), and Panelist #3 (NIU). The Panel 1 questions focused on: What is the value for an ethos for intelligence professionals? What are the legal and moral sources for an intelligence ethos? What is the meaning of the intelligence profession? What are the expectations of community clients/customers?

Panelist #1 (National Intelligence University)

The Intelligence Community Ethos: A Closely Regulated Profession

We do not act rightly because we have virtue and excellence, but we rather have those because we have acted rightly. -- Aristotle (384-322 BC)

The Director of National Intelligence (DNI) Human Capital Strategic Plan, 22 June 2006, outlines Objective 3.1: “Foster an Ethos of Service, Integrity, and Accountability.” Objective 3.1 then defines that Ethos as the “code” of shared values that guides the way an individual (and an organization) behaves, and defines an institution’s culture. In fact, the DNI Ethos is a critical document for intelligence practitioners involved in work with unique professional requirements; namely, that practitioners are involved in work that sometimes involves violation of foreign laws, as well as moral standards, that others share and consider important. Clearly, such practitioners must have a professional Ethos that guides duty performance in ambiguous, stressful conditions, with all work performed responsive to American law and values.


raises two important questions: Does the DNI Ethos of Service, Integrity and Accountability fully and accurately reflect who we “should” be as federal employees working in the intelligence community (IC)? Does the IC need further codes of ethics, either by mission practice area or by agency, which could more effectively guide our work? In any case, intelligence practitioners face complex ethical and legal problems in their daily work. Some problems raise critical conflicts in duty involving national security and democratic values. The resolution of such conflicts is neither straightforward nor easy.

This paper adopts a structural – as opposed to a philosophical – approach to the Ethos issue: The IC is established by federal statute, with specified missions and well-defined operating parameters, and often with close oversight from inside and outside government. In that respect, federal law delineates the core missions, functions, and primary tasks for the overall IC, as well as for the member organizations that constitute that community. In many cases, federal law further delineates restrictions on intelligence practices. Federal law, arising from constitutional, statutory, decisional, and executive sources, embodies values and norms that guide and constrain duty performance.

The DNI Ethos must be grounded in values and norms that are supported by the American people. Here, the legal and moral foundations for an intelligence practitioner’s work operate at both the institutional and individual levels. This paper offers a conceptual model (figure 1) for understanding an intelligence practitioner’s professional Ethos, as well as providing an appreciation for competing professional obligations.\footnote{This framework is adapted from a framework used to analyze the Army Professional Military Ethic. See Don M. Snider, et. al., “The Army’s Professional Military Ethic in an Era of Persistent Conflict,” Strategic Studies Institute, \textit{Professional Military Ethics Monograph Series}, vol. 1(Carlisle, PA: U.S. Army War College, 2009).} The first two (upper)
quadrants identify some of the legal and moral obligations operating at the institutional level, while the second two (lower) quadrants identify some of the legal and moral obligations operating at the personal level. Some documents (e.g., the U.S. Constitution or IC Mission documents) have both legal and moral foundations, providing some blurring between quadrants. In effect, the values and norms of behavior arising from these sources guide a practitioner’s performance, both on a conscious and an unconscious level. Moreover, this model should be useful in understanding conflicting obligations in a given context. What is the practitioner’s higher duty in a given situation?

Quadrant 1 raises issues involving primary duties under federal law. Here, intelligence practitioners have an overall mission to perform, whether it involves collection, analysis, counterintelligence, or special activities. As a practical matter, practitioners face three important issues when given a specific tasking: Does the tasking involve an authorized intelligence mission? Has the tasking (mission) received approval at the appropriate level of command/supervision? Does the tasking (mission) comply with appropriate rules and regulations issued by the Department of Justice?

Quadrant 2 focuses on the moral obligations of the government as an institution, both as it relates to values and norms derived from national source documents, as well as from Just War theory. For example, the U.S. Declaration of Independence calls for certain inalienable rights, to include “Life, Liberty, and the Pursuit of Happiness,” along with the “Right of the People to alter or abolish [their own government].” This implies that government should be based upon the rule of law, with a right of the people to abolish a government (or eliminate government activities) that undermine deeply held values and norms.
<table>
<thead>
<tr>
<th>INSTITUTIONAL VALUES &amp; NORMS</th>
<th>Legal Foundations (Quad 1)</th>
<th>Moral Foundations (Quad 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Constitution (oriented on Article II powers &amp; federal supremacy)</td>
<td>Declaration of Independence &amp; Constitution</td>
<td></td>
</tr>
<tr>
<td>Title 50 U.S. Code (advise &amp; support policymaker, &amp; protect sources and methods)</td>
<td>Agency Ethics Program &amp; Officials</td>
<td></td>
</tr>
<tr>
<td>Ratified treaty (e.g., UN Charter, the Geneva &amp; Genocide Conventions, &amp; the Convention against Torture)</td>
<td>Trust Relationships: President &amp; Congress</td>
<td></td>
</tr>
<tr>
<td>Federal regulations</td>
<td>IC/Agency Mission, Vision &amp; Values Docs</td>
<td></td>
</tr>
<tr>
<td>EO 12,674, 12,333 &amp; 13,526; NSDDs; POTUS orders; &amp; NSC directives</td>
<td>IC Organizational Culture, to include subcultures by agency, discipline &amp; practice area:</td>
<td></td>
</tr>
<tr>
<td>DoJ Memorandums, OLC Opinions</td>
<td>- Mission</td>
<td></td>
</tr>
<tr>
<td>IC Directives; DoD Directive 5240.1-R &amp; 2311.01E</td>
<td>- Ideology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Dissent Channel (State Dept)</td>
<td></td>
</tr>
<tr>
<td>PERSONAL VALUES &amp; NORMS</td>
<td>Legal Foundations (Quad 3)</td>
<td>Moral Foundations (Quad 4)</td>
</tr>
<tr>
<td>Legal Foundations (Quad 3)</td>
<td>Moral Foundations (Quad 4)</td>
<td></td>
</tr>
<tr>
<td>Title 18 U.S. Code (criminal statutes), Financial &amp; conflict of interest disclosures</td>
<td>HC Competency Maps &amp; Performance Reports</td>
<td></td>
</tr>
<tr>
<td>State professional licensing, with disciplinary standards and liability issues</td>
<td>Oath of Office, Creeds &amp; Mottos</td>
<td></td>
</tr>
<tr>
<td>Charge card use, <em>Hatch &amp; Privacy Acts</em></td>
<td>Trust Relationships:</td>
<td></td>
</tr>
<tr>
<td>Non Disclosure Agreements &amp; Prepublication Review</td>
<td>- Collectors: protect sources</td>
<td></td>
</tr>
<tr>
<td>Security Clearances (contacts &amp; travel)</td>
<td>- Analysts: support to customers</td>
<td></td>
</tr>
<tr>
<td>EO, IG, Whistleblower Statutes</td>
<td>Personal Moral/Religious Beliefs, including Equal Opportunity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aristotle, Virtue Ethics</td>
<td></td>
</tr>
</tbody>
</table>
Moreover, this vision was expanded in the Preamble to the Constitution: “to establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty ….” Indeed, Justice Potter Stewart, in commenting on First Amendment issues, remarked on the need for “an enlightened citizenry – in an informed and critical public opinion which alone can here protect the values of democratic government.” There is then an inherent tension between the need for secrecy to advance the “common defence” and democratic values. In short, both the Declaration of Independence and the Constitution envision a government that balances civil liberties and national security, neither sacrificing one for the other.

Generally, Quadrant 2 raises issues involving the moral (and public) justification for certain programs and activities. On one hand, the fact that a foreign nation or non-state actor poses an existential threat to the United States can provide justification for certain intelligence operations and activities to collect information, providing policy makers with a decisional advantage. Moreover, intelligence practitioners can undertake special activities to preempt a looming problem before it becomes worse. If, however, practitioners and policy makers propose an activity under a claim of justification, it is imperative that the activity be supported by a clear-headed analysis of national interests and values, especially if that activity is inconsistent with international law. In any case, Just War theory, using the basic principles involving just cause, right intentions, probability of success, last resort, and proportionality, provides a useful analytic model in assessing and acting against foreign adversaries.

On the other hand, the public disclosure that the United States sometimes acts contrary to its stated values and norms can also undermine public (international and domestic) support. Thus, the United States faces especially difficult problems when it undertakes actions, such as
the assassination of foreign leaders, inconsistent with international treaty obligations such as the Charter of the United Nations. This also highlights the tensions between secrecy and the need for public support, illustrating how excessive secrecy can have a catastrophic effect on the Administration’s credibility when it turns out that documents have been classified to cover-up illegal or embarrassing activities.

Quadrant 3 focuses on prohibitions imposed by federal and state law, creating criminal liability for acts contrary to U.S. law. Generally, Quadrant 3 involves limitations on intelligence activities either within the United States or involving U.S. citizens and property overseas. Here, federal law limits CIA operations within the United States, while the Federal Bureau of Investigation (FBI) is severely constrained in its domestic collection activities. However, the fact that certain intelligence operations may also violate foreign law is not a relevant consideration.

In effect, federal law creates “red lines” or limitations on what federal employees cannot do. For example, an intelligence practitioner has a fiduciary obligation to protect classified information from unauthorized disclosure and an employee who breaches that obligation can be prosecuted under federal law – without regard to how he or she personally assessed the national interest with regard to that disclosure. In 1983, President Ronald Reagan issued National Security Decision Directive 84 (NSDD 84) that required that all federal agencies handling classified information have employees sign nondisclosure agreements and, as appropriate, prepublication agreements. Such agreements create a contractual obligation, as a condition of employment and access, on the part of the employee to protect classified information from

\[17\] The UN Charter, Article 2 (4) prohibits “the threat or use of force against the territorial integrity or political independence of any state,” meaning that the United States is proscribed from conducting intelligence operations involving either large scale covert actions or political assassination.
unauthorized disclosure. Moreover, federal statute places limitations on military intelligence liaison relationships with foreign powers, especially where foreign officers are suspected of involvement in human rights abuses. Finally, federal law imposes criminal liability on persons who reveal the protected identities of certain intelligence officers.

Quadrant 4 raises aspirational issues (idealized values and norms). Here, individual practitioners draw inspiration from a wide range of sources, with some inspiration coming from the employee’s own background and other inspiration coming from institutional sources either while in training or through the work environment. On one hand, human intelligence (HUMINT) collectors often develop personal relationships with clandestine sources; in fact, many believe that the most effective source relationships are rooted in trust and loyalty. On the other hand, analysts often develop support relationships with collectors, inter-agency colleagues and customers. At more senior levels, managers must establish access and rapport with Executive branch and Congressional officials. Hence, an intelligence officer’s ability to establish trust relationships is a critical aspect of his overall effectiveness.

Some sources, such as Virtue Ethics, are deeply rooted in the western philosophical tradition and broadly address the character of a moral agent (here, the intelligence practitioner) as a driving force for ethical behavior. Other sources, drawing inspiration from personal moral/religious beliefs, are deeply held and sometimes quite specific in what an individual can and cannot do. Our oath as federal employees to support the Constitution helps us prioritize the allegiances we owe, to our fellow citizens, to our home agency, and to our co-workers. In any case, IC values and norms are reinforced at an individual level through IC core qualification standards and annual performance reporting. In short, the employee can be faced with a hortative blend of values and norms, some conflicting and some reinforcing.
The ethical conflicts faced by intelligence practitioners cover a range of issues, based upon frequency of occurrence and impact. Some issues involve low occurrence but high impact, such as the use of torture to support interrogations. As a practical matter, torture can be classified based upon the duration and severity of the technique, raising a scale of legal and ethical concerns. One writer describes a torture pyramid, with Psychologically Coercive Interrogative Practices at the first level; Cruel, Inhuman and Degrading Treatment at the second level; and Classic Torture at the third level.\(^\text{18}\) Clearly, some lesser practices might be unethical but not illegal under either international or domestic law, while more robust practices would be considered unethical and illegal from multiple perspectives. In truth, the U.S. government has sanctioned the torture of a very small class of persons, each with unique circumstances involving citizenship, location of capture, level of culpability in terrorist activities, and the anticipated intelligence that could be gleaned from that interrogation. Notably, these interrogations have been “high impact,” spawning a great deal of public interest.

The torture problem illustrates the legal and ethical issues faced by practitioners. In Quadrant 1, the practitioner may be under a legal obligation to execute a muscular program that has been the subject of a presidential finding, even though that program has suspect status under domestic and international law. In Quadrant 2, practitioners may justify the program under Just War theory (need to act in a timely, proportionate manner to forestall coming threats) or under a utilitarian analysis (the possible payoff for many innocents outweighs the temporary imposition on the guilty few). In Quadrant 3, a medical professional supporting the program may have conflicting legal/ethical obligations under state professional licensing law. In Quadrant 4, practitioners may have conflicting personal religious/moral beliefs. In some cases, the issues

surrounding the propriety of the program can be further complicated by conflicts within a single quadrant, and with conflicting interpretations of international and domestic law. How should an individual decide whether to participate in a program? What is the appropriate resolution of this underlying conflict? In any case, the fact that a program or activity raises so many issues should serve as an indicator of a looming moral/legal storm.

Many apparent conflicts can be resolved through an analysis of various factors such as the nature and specificity of the legal/moral obligation, the weight of the authority and the relevance of the source document. In some cases, a practitioner can also resolve a conflict through a clarification of the facts and issues, an alternatives analysis, or the time sensitivity of the problem. In other words, what is the source of the obligation? What other, less troubling but equally effective, methods of resolving the issue are there? Why is the problem so time-sensitive that the practitioner cannot obtain clarification from superiors, the IG, or agency General Counsel? In the end, each practitioner must make his own moral decisions about the nature and extent of his participation in a program or activity. One can rely on the counsel of others only to a certain extent when it comes to activities that may be viewed as illegal or immoral.

While it is important to discuss the high impact issues that stress our national values, I think it is much more important to discuss the high occurrence but low impact issues that confront intelligence practitioners on a daily basis – in other words, the issues that don’t reach the front pages of The Washington Post. Ethics must be integrated into the personal lives and actions of public employees, helping to prevent errors of commission, as well as errors of omission where there is a duty to act. A well-grounded professional Ethos, supported by relevant codes of ethics for practice areas, can sharpen professional judgment in time sensitive, ambiguous circumstances.
Conclusion

Intelligence practitioners face complex moral and ethical problems: not the garden variety questions about whether one may lie, cheat or steal, but rather sophisticated problems arising from conflicting legal and moral duties – and with a focus on important national security interests. Moreover, intelligence practitioners are often called upon to make decisions in a time-sensitive uncertain environment, with varying context depending upon mission (practice) areas. In that sense, there could be great utility in codes of ethics that assist practitioners in addressing unique problems. Does the DNI Ethos of Service, Integrity and Accountability reflect who we “should” be as intelligence professionals? I think the answer is “yes.” How does IC culture currently reflect the DNI Ethos? In other words, how are we living up to what we should be? Here, I think we have gaps, both in terms of how well the DNI Ethos is understood in the community, as well as in how well we live up to it on a daily basis.
Panelist #2: (National Defense University)

Intelligence Professionalism & The Ethos Issue

This presentation will make four points. First, intelligence is a profession. Second, an ethos is an integral part of a profession. Third, the military analogy may be helpful in looking at intelligence as a profession. Fourth, ethos development is an evolutionary process.

First, intelligence is a profession. What is a profession? Samuel Huntington writes that a profession has three features: (1) a specialized expertise and knowledge; (2) a service to society, or a “compact with society”; and (3) a sense of corporateness, which includes control over who become and stays a member of a profession, as well as a sense of consciousness of ourselves as professionals. Intelligence has all of these features.

Second, an ethos is an integral part of a profession. What is an ethos? It is as much about who you are as what you do. As Robert Coles wrote, “I learned a lot about what physicians do in four years of medical school and in internships and residencies. But I learned what it means to be (italics) a physician by going on house calls with a truly fine physician.” Who you are should inform and guide what you do. Conversely, if you do things other than those dictated by your ethos, you will start to become something else.

Third, the military is useful in examining intelligence as a profession. In the IC, there is no common identity, or at least there is no sense of one. Similarly, in the military, it was only the National Security Act of 1947 that created a “Department of Defense” out of the disparate parts of the Department of War and the Department of the Navy. In addition, General George C.

---

Marshall had S.L.A. Marshall write *The Armed Forces Officer* about the common responsibilities and duties of military officers.20 Education, such as NDU and NIU, can also be part of forming a common identity. However, all of this was not sufficient, leading lawmakers to pass the *Goldwater-Nichols Act of 1986* in order to further instill “jointness” in the officers of the armed services. Regardless of military specialty or branch, officers have a common ethos.

In the early 2000s, authors from around the Department of Defense gathered at the U.S. Naval Academy to revise *The Armed Forces Officer*. Because the terms “joint” and “jointness” are clumsy and unattractive, the revision’s authors chose the motto “*e pluribus unum*” to express the unified identity of the profession of arms.

Finally, who is a member of the profession of arms? Is it only officers? Some have argued that enlisted personnel too are members of the profession, not just officers. Nonetheless, despite vast differences in specific jobs military members do, they all share a common ethos—whether a fighter pilot, an infantryman, an adjutant general, or a submariner. The military ethos transcends all military occupational specialties.

It may be more fruitful to think in terms of guilds (apprentice, journeyman and master), which allows for degrees of membership, rather than in terms of “in or out” membership.

---

A Conspiracy Against the Laity: Is the Intelligence Community a Profession?

Introduction

More than a merely semantic distinction divides a “community of professionals” from a “profession.”21 This essay argues that the intelligence community (IC), while undoubtedly the former, is not, by most standard definitions, the latter. This in no way reflects on the high standards of training, character, and integrity necessary for every intelligence professional. Rather, it’s a recognition that the traditional professions—law, medicine, and a few others—are entitled to the name by a combination of both highly specialized training common to all within the profession, and a series of historical accidents. To try to stretch the mantle of “the professions” over the IC is to portray the IC as a thing it is not. But there is, fortunately, a far more tenable and respectable approach: acknowledging members of the IC as a community of professionals, in the wider sense of working people everywhere who take a modest pride in mutual solidarity, and in recognition of the importance of competence and integrity in their duties.

George Bernard Shaw famously wrote that “all professions are conspiracies against the laity.”22 If he was right, then the IC—formal profession or not—should do what it can to at least be a benevolent conspiracy, undertaken for the best of purposes: supporting the national security in accordance with law and, yes, high ethical standards.


22 George Bernard Shaw, The Doctor's Dilemma, Act 1 (1906).
Whether the IC—profession or not—needs a formal ethical code, and how that code might be conceived and implemented, is a question others address elsewhere. I focus here, rather, on the initial question of how best to define the IC as a coherent entity, and whether it passes basic tests for the traditional professions such as law and medicine.

**Who is Included in “the Intelligence Community?”**

Before discussing whether the IC is a true profession in the traditional sense, we should decide who we’re talking about. One of several problems with trying to define the IC, especially when the one aim is to formalize its members’ status, is what might be called “the 1st-grade birthday party problem”: the more people you include, the worse it is to be left out.

Collectors and analysts are obviously doing “core intelligence work,” so we could draw the line around them. But what about all the admin officers, interpreters, computer wizards, and legions of others who support and work alongside the analysts and interrogators? The tighter we draw the definitional circle to define full members of the “intelligence profession,” the more damage we do to the IC’s esprit de corps; the wider the circle, the more attenuated our claim to be a logically and practically unified community.

The obvious solution is to simply define the IC as “everyone employed by the sixteen designated intelligence agencies.” That might complicate the process of designing a single ethical code that’s relevant to everyone—a problem this author is happy to leave for others to resolve.
Why (if at all) Should We Attempt to Promote the IC to “Professional” Status?

What benefit accrues to the IC from a formal recognition, either among ourselves or the outside world, as a profession? There are at least two possible benefits:

Firstly, public service tends to carry with it a measure of pride of position, of one’s earned competence. Recognition of the IC as a formal profession validates that pride and image, in both our eyes and those of the outside world.

A second consideration has to do with our motive in approaching this whole question of whether the IC is a profession. Ethical codes are traditionally associated largely (though not exclusively) with the professions: doctors “Do No Harm,” and academics “Cite All Sources.” So perhaps publicly characterizing the IC as a profession would lend credibility to an IC-wide ethical code. And, perhaps cause and effect work both ways here: creating an IC ethical code might strengthen the IC’s case for eventual inclusion among the traditional professions.

What we should avoid is any kind of campaign to formally claim the IC as “one of the professions,” without taking concrete steps to bring the IC’s structure more into line with the traditional professions—otherwise it all tends to look like mere self-aggrandizement, undermining the real cultural dedication and pride in service that has characterized the IC—however we characterize it—for over half a century.
Is the IC, in its Current Form, a Profession by Traditional Standards?

There are countless variations on “checklists” for defining professions; I have chosen, for its clarity and applicability to the traditional professions, the six-item list propounded by Professor William Wickenden. Comparing his list to the intelligence community is useful for gauging to what extent the IC meets, in broad outline, the standard definition of a profession.

1. A profession renders services based upon specialized and theoretical knowledge and skill.

The IC seems to fit here, with a caveat: the community consists of dozens of tribes, each with a wholly different knowledge and skill set: case officers, SIGINT analysts, interpreters, lawyers, logistical and financial support personnel, administrative officers, and many others. That said, IC analysts generally meets the “theoretical knowledge and skill” test better than collectors. The former are more apt to live the “life of the mind” in building arguments, comparing evidence, and drafting detailed intelligence assessments; the latter, in general, rely more on hands-on training in and execution of debriefing, intercept transcribing, source handling, and other tasks which, while often intellectually and physically challenging, rely less on “theoretical knowledge.”

In addition, most traditionally recognized professions have a core of common theory and knowledge which (apart from a core of common security measures to protect information) is almost nonexistent in the current IC. The community is just too fragmented, with too many widely varying skill sets and Balkanized institutional knowledge bases depending on the agency and specific job or mission.

---

2. A profession maintains extensive education, competence testing, and association restrictions controlling entry into the profession.

This “high barriers to entry” test varies widely within the IC. A junior enlisted military analyst or collector goes through boot camp and a few months of training, often emphasizing hands-on skills and “buttonology” over theoretical frameworks and critical thinking. Civilian analysts, in contrast, are usually a bit more mature and have a college or graduate degree, but receive only a few months of intel-specific training. Clandestine case officers are usually commissioned officers or fairly mature civilians, with at least a college education; they undergo lengthy, intensive training (as opposed to “education”) to learn the business. Support personnel may come from almost any background and educational level. Apart from the need to qualify for a security clearance, almost no common set of entrance standards unifies these and other personnel throughout the intelligence community.

As for “association restrictions” controlling entry into the IC—yes, it can be hard to break into the intelligence business, but that may be said of carpentry or bartending as well. The total lack of uniform education and standards throughout the IC (beyond the universal requirement to qualify for a security clearance) weighs here against considering the IC a profession.

3. A profession involves a confidential relationship between a practitioner and a client or an employer.

This seems an obvious “yes,” for an entire industry based largely on secrecy—but note that most professionals such as doctors, lawyers and clergymen have direct, confidential relationships with their patients, clients, or parishioners. In contrast, only the most senior IC leaders usually deal directly with IC customers, though of course the duty to protect information
falls on all IC members. There is a confidential relationship generally between the whole IC and the whole government, but is this the same as individuals providing confidential services to a consumer, as with doctors, lawyers, and clerics?

Note that the IC is also unlike other professions, in that its sole customer is the government. Only in the most general, attenuated sense is an intelligence report meant for “society;” the IC’s product is directed and consumed by analysts who provide assessments for elected officials. On balance, however, I would argue that the IC does not meet this “confidential relationship” requirement on the level of the individual intelligence officer.

4. A profession enjoys a common heritage of knowledge, skill, and status to which professionals are bound to contribute through their individual and collective efforts.

This applies generally to subgroups within the IC, such as imagery analysts, interpreters, and interrogators, who may all support the same mission but whose actual jobs overlap very little or not at all. But the Balkanization of the IC prevents it from satisfying this “common heritage of knowledge and skill” test for a profession.

5. A profession has autonomy in how it provides services.

The IC is wholly a creature of the government and has nothing like the professional autonomy enjoyed by doctors, lawyers, and other members of traditional profession.

6. A profession has an ethical code.

Most IC members belong to the military or to one of the civilian agencies, each of which has an ethical code in place covering all personnel. These codes, however, vary widely in format, intended audience, and applicability to intelligence work specifically. As of now, the IC
does not meet this requirement for a *unified* ethos, although this issue is being actively addressed by National Intelligence University and other institutions.

So it seems that most qualities of the traditional professions apply only in part, or with significant caveats, to the IC. I therefore argue that trying to present the IC, either to its own members or the outside world, as a “profession” in the formally defined sense, would be counterproductive. It’s too much of a stretch, and the IC is too far-flung and varied, both functionally and organizationally, to apply the kind of unifying internal controls and discipline possible in, for example, medicine and academia. Most such controls are already exercised quite effectively by the 16 intelligence agencies over their respective workforces.

**So What Is the IC, if Not a Profession?**

If the IC does not qualify as a profession, what else might it be? In one sense, many individual functional tasks within the IC resemble the traditional *guilds*: formal associations of craftsmen with a common set of skills, protected by layers of self-imposed procedures, legal and training hurdles, and other measures intended to insulate their craft from casual usurpation by outsiders.

In a sense, the entire early period of modern intelligence work, from the Office of Strategic Services (OSS, during World War II) through the Cold War, followed this *guild* model fairly closely, but with guilds organized by agency rather than specific occupation or skill set—an inevitable consequence, perhaps, of security practices. It has had the effect, in any case, that

---

analysts throughout the 16 formal intelligence agencies receive a wide range of training and experiences.

Clandestine human intelligence, with its mystique and intensive training process, is one of the clearest modern-day examples of the traditional guild structure in the modern IC. At least in the DIA model, most clandestine officers start their careers as overt debriefers or interrogators, jobs that require far less training and lifestyle adjustments. Following a period of employment and observation by one’s superiors, overt collectors may be selected for increasingly intensive clandestine-oriented training and assignments, culminating in attendance at “The Farm,” and accreditation as a case officer. However, even then a newly minted case officer has much to learn from mentors in the field, from whom he or she will absorb not only (one hopes) high professional standards, but a healthy pride in their work and willingness to maintain a high barrier to entry into their career field, the better to protect it from the incompetent or unsuitable. All this seems to nicely fit the traditional model of the medieval guild.

Intelligence analysts and others in the IC also go through a period of formal and informal training and gradually increasing responsibility although analyst training probably varies more throughout the IC than (for example) HUMINT collection training generally.

Another way in which historical guild development parallels the modern IC is in the division of the overall mission into hundreds of discrete tasks, each assumed by a different group of workers. Just as the medieval metal-workers included not only armorer’s guilds, but also
specialty guilds such as crafting helmets, greaves, and polishers, so the modern IC is almost limitless in its division of jobs by both function and organization.\textsuperscript{25}

Of course, one major feature of the guild system decidedly unlike the modern IC, was that the guilds were expressly for the sole benefit and protection of their members—they were almost literally “conspiracies against the laity.” The few that survived the industrial age and evolved into the modern professions, did so largely by providing societal benefits: medicine, law, education, and a few others.

\textbf{Conclusion}

It seems that the IC refuses to fit neatly into any characterization more specific than “community.” And perhaps asking ourselves if we are truly a “profession” is not quite the right question. Maybe all we really need is a definition of our community that would facilitate the articulation of a common ethical viewpoint, reflecting our duty to the truth and to our customers and those who elect them.

If that’s the case, we already have the right term before us, one with which few would argue: a “community of professionals.” Any future measures, such as a unified ethical code for our community, would only strengthen this sense of teamwork and esprit de corps among the professionals of the intelligence community.

Panel #1: Roundtable Question and Answer Session

Q1 (Comment, Panelist #1): In law, one does not refer to either paralegals or legal secretaries part of the legal profession, but that does not stop law from being a profession.

A1: (Panelist #3): Excluding employees or jobs within the IC from the definition of the IC or intelligence profession would not help intelligence or the IC to become a profession.

Q2 (Comment, Panelist #2): Much of this refers to boundary issues. There is nothing set in stone, and it seems that it matters more who you are than what you do. What you do certainly matters when one needs particular skills, but this does not affect identity.

Q3: (Comment, Audience Member): There is no common training within the IC.

A3: (Panelist #2): Even among clergy, there is differing training in different schools. Similarly, the military has differing entrance training for its officers (Officer Candidate School/Officer Training School, the Reserve Officers Training Corps, and the service academies). Within the IC itself, there may be different training in a single agency.

A4: (Panelist #3, in reference to Q1): Declarative policy can insult personnel and hurt morale if the right people are not included.

A4: (Panelist #2): S.L.A. Marshall’s book did not decide matter of military professionalism, it made an argument for it.26

Q5: (Audience Member): Samuel Huntington’s book was intended to address the military.

---

A5: (Panelist #2): Huntington was writing in the aftermath of the Truman-MacArthur confrontation and the reaction at home to perceived politicization of the military. Huntington said that the military regulates itself from within, and that this is part of a profession.

Q6: I do think the IC polices itself

Q7: (Audience member with 30 years in IC): Analysts are somewhat afraid that if they are ever regularly asked to “show cause,” it could be used to silence them for not following a political party line.

Q8: If there is a code of ethics, will it apply in time of war? One often has to make quick decisions in such circumstances that are not always politically correct.

A8: (Panelist #1): Yes, a code of ethics has to be something that stands up in times of war. It must have real meaning.

A8: (Panelist #3): Ethics may get “bent” in wartime, but not, one hopes, to the point of breaking.

A8: (Panelist #2): You have ethics for the hard cases, not the easy ones. Absolutely, you must maintain the code of ethics in time of war.

Q9: (Comment): Until we have common training and education, like law, we will not have a profession.
PANEL 2: GENERAL COUNSEL/INSPECTOR GENERAL PANEL

The panelists are Panelist #1 (General Counsel’s Office, ODNI), Panelist #2 (General Counsel’s Office, intelligence agency), Panelist #3 (General Counsel, intelligence agency IG), and Panelist #4 (IG, intelligence agency). The moderator is an attorney and serving in a policy position in the intelligence community.

Moderator: Can you think of a scenario where you had to balance the law versus a policy decision? What was the hardest ethical dilemma you faced professionally?

Panelist #4: (Reply consolidated with response to subsequent question for clarity.)

Panelist #3: Scenario – two detainees died as a result of beatings. The incident was brought to light a year after it happened and the unit had redeployed. Neither the unit on the ground at the time nor the redeployed unit wanted to take ownership of the investigation. The Panelist eventually undertook the case and prosecuted several individuals involved in the beating.

Panelist #2: Passed on the scenario question. No attorney in the Office of General Counsel (OGC) is required to sign something they do not believe in; any legal issue can be raised to a higher level if an attorney is uncomfortable with the given situation.

When asked about the importance of having a statutory reporting chain, Panelist #2 stated that having a Presidential appointee is valuable because you know you ultimately answer back to the President. The formalized process would also lend credibility that may otherwise be in question. Important leaders have the ability to say no to support junior lawyers.

Panelist #1: Scenario was about whether the Foreign Intelligence Surveillance Court should publish the appeal on the challenge to the Foreign Intelligence Surveillance Act (FISA) Amendment Act. His opinion was to redact the appeal to protect sources and methods but to
publish it to get public opinion back in the government’s favor. He also spoke of being clear when you are giving legal advice versus policy advice. Attorneys should be viewed as counsel, not just legal advisors. It’s vital to characterize what the advice is that’s being given; it may be an opinion, not necessarily legal statute.

**Moderator**: What gives you the right to feel uncomfortable, your moral compass or your ethics?

**Panelist #4**: Both.

**Moderator**: What value added would be provided by codes of ethics, either by agency or by functional area? What are some examples of “hard cases” involving ethical dilemmas? What is the most difficult decision you’ve had to face in your career?

**Panelist #1**: We have unique responsibilities because IC elements apply law and the *U.S. Constitution*. We perform statutory oversight of collection, and have community responsibilities: foster legal consensus, to keep the same degree of consistency--to keep the same IC legal viewpoint, and oversee general legal issues facing the community (the FISA is one example). The IC is at the intersection of law and policy addressing ethical legal questions that are complex and straddle the gray area of law and policy.

**Panelist #2**: If we’re successful, no one knows we’ve been there -- we steal secrets foreign intelligence secrets without them knowing we were there.

**Panelist #3**: We deal with fraud, waste, and abuse, and the U.S. Army Staff Judge Advocate General officers force disciplinary system. Once we have a code, what do we do with it?

**Panelist #4**: IG has oversight role of fraud, waste, and abuse. The IC is a unique environment because we operate in secrecy outside of public debate. The oversight function provided by the
IG is critical to public trust. The hardest ethical dilemma I faced as an attorney dealt with a legal vs. policy dilemma. I was asked to approve a collection operation which was legal but violated a U.S. policy prohibition. The operation carried a huge risk–even if it was legal I didn’t sign off on it because I felt the risk was not properly justified. It was putting the agency at an unnecessary risk. I was told to make my case. This is the question of ethics–what to do when you are in a position to protect the public and the organization. Ethically, my job as an attorney was not just to determine if the operation was legal, but to assess risk to the organization, as well. This comment prompted a question from the audience, “When have you overstepped your bounds as an attorney by distinguishing what you believe to be bad policy though you know it is legal?”

Panelist #2: To sign or not to sign … if you are uncomfortable as a professional with signing such a document, kick it up the chain. Do it out of respect for the profession and your legal skills. This is one reason why diversity of opinion is needed in the office. My organization deliberately tries to hire people with different backgrounds to encourage diverse discussion on one issue and attack it from multiple angles. The strength of a vibrant law office is in part the diversity of its staff and their opinions.

Panelist #2: You can get through a tough ethical situation with good lawyers and a strong ethical code. A strong code instills an ethos of openness, such as standing by the junior attorney when she said I’m not comfortable signing this document; there are tough ethical issues that involve real human lives.

Moderator: How useful would a code of ethics be in your organization?
Panelist #1: His organization tries to provide consensus between the IC and is the lead for oversight, which includes ethical issues. The intersection of law and policy is typically at the “50,000 foot level,” which usually involves the DNI.

Panelist #2: Due to the nature of the sensitive operations at the agency ethics are extremely useful in guiding the attorneys in the office, who are given increasing amounts of personal discretion in their practice. Since the office now over 100 attorneys, and has expanded rapidly in the past decade, ethics training is essential to ensuring a sound and responsible law practice.

Panelist #1: Attorneys are legal counsel – but what happens when the boss asks for “other advice” between policy and legal?

Panelist #1: You separate legal versus policy advice but give both. After the passage of the FISA act of the IC, it was challenged and the court approached DNI to publish an opinion. Characterize when making a policy decision.

Audience Member: How do you advise people on disclosure of Section 7 IG act that provides identity of the employee?

Panelist #2: Employee identity will not be disclosed unless avoidable. Intelligence personnel are not dispensable. We do care, and conduct used with asset can be publicized at times, but we will fight tooth and nail to protect the person’s identity.

Question from audience related to ethical issues and sources.

Panelist #3: By statute (Section 78 of IG Act) we cannot disclose sources of information unless it becomes necessary. The investigations standing operations procedures dictate that. Sometimes
it’s necessary to disclose sources of information because of other situations (personnel/Equal Opportunity litigation).

**Panelist #2:** Panelist emphasizes the need to protect assets at all costs. Confidential informants/assets are the “lifeblood of the agency.” We do care about them. They understand the risks up front, the nature of the covert relationship, and that we’ll make every effort to protect their identity, our communication with them, and the relationship we have with them.

**Panelist #4:** For internal investigations (whistleblowers), our biggest concern is with retaliation. We might not be able to protect their identity in every case, but we should be able to protect them from retaliation.

**Audience Member:** How do you feel about anonymous complaints?

**Panelist #4:** Depending on the allegation, you have to look into it. Some anonymous complaints raise significant issues. However, you’re not going to be able to get back to that person and tell them their case has been solved. There’s no opportunity to close the loop because of their lack of trust in the system. The IG must show that the system works and that an employee that comes forward with a complaint will not be retaliated against.

**Audience Member:** How do you manage your biases in the IC – we are a risk averse organization, no one gets fired for reporting the attack tomorrow and it doesn’t happen, but will get fired if we don’t report an impending attack and it happens. Do you believe this to be true, that we are a risk adverse organization, and how can we fight worst case mantra? How do you counter it?
Panelist #2: Lawyers are trained for worst case scenarios. The practice of law requires us to lay out all worst case scenarios and ensure we distinguish legal and policy matters for the clients. Lawyers advise on likelihood of an action; and make it clear if there is no case law. The lawyers shouldn’t make the final call on matters of policy. Also, the role of the National security lawyer is different. We must look at the big picture as it involves our agency and the IC. Ultimately it’s the policymaker that makes the final call.

Audience Member: We talked about “gray areas” earlier. Have any of you signed something against your gut? Are there times that you have had to look at the gray areas when providing legal advice?

Panelist #4: With oversight committees, there’s a lot of looking back. The examination should show all sides. Lawyers should not be taking the risks to skirt the law; laws can be changed, so lawyers should lay out what they are.

Panelist #2: There are going to be gray areas. But every case deserves a fair review outside the ‘pressurized’ area.

Moderator: What is the legal standard? Are there times that you feel like you’re standing on the code? Have there been moments where you’re glad there’s a code to rely on?

Panelist #1: Lawyer may point out the legal “dark areas” of the law, but it’s generally just their job to point out the law (legal or not) and provide options; client ultimately makes the decisions. “You never want to be the only lawyer read into something.” Basically, you always want to talk to another lawyer, collaborate and bounce ideas off of each other. If the client will let you be the only lawyer, you can push it up through your management chain or you can caveat it in your response; you hope you can convince your customer he needs more lawyers.
Panelist #3: We need a prescriptive ethos of discrete rules, not just encouraging teamwork. Lawyers already follow a specific code/ethical standard.

Panelist #3: Not sure if there is a code. Instead, we need to use best judgment by talking to another attorney, find someone “read-in” on the case because in a gray area, there really is no code. An ethical “prescriptive” code may be helpful. Lawyers follow rules of conduct with codes that are helpful. There is currently no set standard of what to look at; you can argue from all sides – but – you still have to ask yourself, did you look at everything? Also, the attorney-client relationship is essential.

Panelist #2: There is merit in encouraging behaviors we would like to have in the IC. Training and education should be part of our curriculum. We didn’t go to “right and wrong” school, we went to law school. Culture is not so much a code; it’s a set of values that you make decisions on. Where is that line?

Panelist #3: Once you have a code of ethics, what do you do with it? How do you enforce it? This is a primary challenge to developing a code of ethics.

Panelist #2: The office has a practice that it will not require attorneys to sign off on operations if they are personally uncomfortable with the legal basis for the operations.

Panelist #2: Having an independent general counsel is a huge benefit to the organization, and encourages ethical behavior. It is most important for the General Counsel to establish an ethical ethos in the office, and stand by subordinates who refuse to sign off on operations due to ethical considerations.
Panelist #1: Policy and legal intersection is tricky. We must separate legal and policy advice. Give both, but characterize properly. (The panelist then gave an example of a FISA case with source methods; he noted a need to separate the case and methods to ensure integrity.)

Audience Member: How do you fight “worst case” bias in one agency or another?

Panelist #2: Lawyers are trained to lay out worst case as well as all sides, so worst case scenario will always be a factor. They are also responsible for making it clear whether it is a legal problem or a policy problem.

Panelist #4: The role of the lawyer in the national security area is to navigate grey areas and assess risk. There is not much precedence. Lawyer risk should be clearer than analyst risk.

Moderator: We’re talking about this here, but what are you personally doing in your organization to share this ethos?

- Answer: You must often ask, who is your client? Review bar rules, communications with outside clients, you can look into the code, but in this office we practice this way. Training case studies is critical to get at “code.” It is critical to have an offsite or a time out to talk about biggest issues; one of the concepts is exploring the culture of the DNI.
- Answer: One of the biggest is treating customers as clients. The IC should call their customers clients, and stop using the world customer.
- Answer: Training programs should exist that are similar to the military. And, why not a code of ethics? Locksmiths have one … why doesn’t the IC?

Moderator: In the case of malpractice for one of you, how would that work?

Panelist #1: You have an obligation to note if you’re not able to practice in an area of law that is unfamiliar to you. You need to caveat your opinion and you also need to explain to your client that you need another opinion.
Panelist #3: The principal may be driving you towards practicing in different areas. It’s malpractice for you to practice in an area you’re not familiar with.

Panelist #4: Cases involving a government attorney would be removed to federal court. IGs do look at the role attorneys played in issues they are investigating.

Panelist #2: What we should be doing is lessons learned, not punishment or malpractice. It should be a learning environment. As for resigning in the face of controversy, it may be more effective to stay with the organization so that you can change it from within. Resigning may temporarily heighten awareness, but it does not always bring about change in a controversial policy. These are tough jobs that don’t allow you to simply admire the problem set. You’ve got to decide on a course of action and act.

Moderator: In the IC we asked how many in the audience considered themselves professionals. Only 50 percent raised their hands.

Moderator: Could there be an ethical code for lawyers?

Consolidated answer from all panelists:

- There is no proscriptive code for lawyers in the IC
- Lawyers are reluctant to see more codes (as they only create more things for lawyers to debate), but need a way to encourage good behavior. Codes encourage a “race to the bottom,” not something to strive for. We need a way to get toward the “inspirational.”
- Lawyers should avoid making policy
- Purpose of a code should be to encourage right behavior, rather than encourage enforcement. Purpose of codes is to arrive at good decision making; turning to a myriad of regulations does not necessarily lead to good decision making
- Codes tend to make organizations fall back on relying on penalties, not striving for best performance
Three out of the four seemed to be against a codified code of ethics but were in favor of building a culture of behaviors that are desirable versus a black and white code that people may try to skirt around.

**Moderator:** Asked Panelist #3 to expand on the two chains in command for the military Judge Advocate General (JAG) Corps.

**Panelist #3:** Spoke of the benefit of having both chains of command and his responsibility was to both. The JAG chain of command was designed to be independent and follow the requirements prescribed by statute. The other chain of command was responsible for the unit and the mission.

**Panelist #4:** Spoke of the value in protecting sources of IG complaints against retaliation.
PANEL 3: THE COLLECTION AND ANALYSIS PANEL

The panelists are Panelist #1 (a former CIA Station Chief), Panelist #2 (a retired DI Officer/National Intelligence Officer), Panelist #3 (an ODNI employee), and Panelist #4 (an ODNI employee in a training position).

Panelist #1 (Collection Issues): My background of 27 years gave me a unique perspective on the topics discussed today. I’d like to put this in the context of a story. My involvement with ethics and professionalization of the IC started in the mid-1990s when I took over training in my service. When the Department of Defense (DoD) visited and asked what we were doing for ethics training my response was “nothing.” My predecessor always said that if you didn’t have an inherent set of ethics, there was nothing we could do for you, meaning we couldn’t train someone to have a good ethical code.

That was the wrong answer. We needed to work to develop ethics training as a part of a particular code. Professions each have a code of ethics and we needed one. It was important because in the clandestine service we do a lot of unethical things but for a good reason. We needed a code pertaining to the people we served and to show that professionally we what we were doing was in the name of our service. The things we do must be secret from the people we are serving and that comes with responsibilities. Certain elements such as loyalty are owed as well as a code and contract with those we served. I felt that it was important to establish a more formal code of ethics to empower our people – and maybe one for the entire community.

How do we form this code? It is impossible to address all moral dilemmas in this profession. We needed to identify values in our line of work and elaborate on those values based on what we do. We were mostly concerned with the right versus right dilemma. In the world of intelligence, we need to protect secrets and inform policy but where is the line? We are supposed
to protect agents, yet we ask them to do dangerous things. At the end of the day, we don’t get to choose our mission.

How do we reconcile our mission, protect our colleagues, and not get in the way of the ultimate mission? We developed a hierarchy of loyalties that we can turn to when in conflict and have to make hard choices. The Chief of Staff at the time put together a group to scrub everything; to get real organizational buy-in, which was needed.

But was a Board of Ethics needed? I’m skeptical of new layers of bureaucracy, but we do need a frame of reference where we can discuss right and wrong. This is not intended to remove power from our agents but to make them accountable. In the clandestine service, we have accountability boards. It wouldn’t necessarily serve us well to have a separate board of ethics.

Can we do this across 16 agencies in the IC? A set of common values might be more useful but in order to live these values, they must reside in the work people actually do. If people are focused on the right priorities, this should be no problem.

**Panelist #2 (Analysis Issues):** My background and experience has been the opposite of the previous panelist where I spent most of my time in Washington, DC and one tour overseas. One third of my time was spent in analysis, another third was spent in a policy role, and after I retired in 2009 I’ve been teaching at the War College. I’m surprised to hear that analysts and lawyers have anything in common.

The first question of ethos and profession: why does it matter? We care about the performance of our community. Embedded in that is collaboration. With a common identity, we will work better together. Now we have 16 agencies with unique identities and multiple personalities within them. As a result we behave differently.
When in a classroom of analysts and you ask how many consider yourselves a profession of analysts, only about half will raise hands. When the same question is asked of doctors and lawyers, all hands go up. This isn’t because we lack ethos or ethics, but we lack a common identity. The problem is: how do we interpret these standards and put them into practice?

1. How do we address quality control vs. politicization? How does analysis determine what is politically correct? Many feel that managers look to see how their work is perceived in the oval office and not evaluate the quality of the analysis itself. It is a judgment call.

2. How do you protect a dissenter or the alternate view? Some great analytic breakthroughs start as a minority opinion. When first drafting a national estimate in 1990, the original drafter said the breakup of Yugoslavia was not likely; only when a few analysts spoke up was the community able to re-examine the view that somehow Yugoslavia would muddle through. A junior expert had just returned from Belgrade and contradicted the senior expert reporting. His draft report predicted that Yugoslavia would not exist within 12-24 months. How do we protect analytical integrity and ensure we don’t get locked into a mindset? Managers need to be on guard and not suppress outliers for their alternate views.

3. How do you protect accountability? We have accountability reports but how do we assign accountability fairly? The Iraqi Weapons of Mass Destruction (WMD) National Intelligence Estimate (NIE) was created by 200 analysts cutting and pasting from other reports. Reports are rarely formed by one single analyst. Also, we are told to take risks but to be right! Managers need to be prepared to defend their analysts.

4. How do we become the best intelligence analysts in a culture of secrecy? We need to find information regardless of where it resides. Our culture of secrecy makes it very difficult for analysts to do outreach, especially when they are subject to polygraphs and numerous
other bureaucratic hurdles to meet with outside experts, particularly foreigners. How do they get smart on issues and at the same time not get cut off from policy and transnational issues where expertise lies beyond the U.S. government? This is a dilemma for us because we tend to be highly security conscious and risk averse.

5. What are the analytic challenges of dealing with policy makers and collectors? Speak the truth and don’t nuance. There is a greater danger to self-censoring than anything we may disclose. In the case of Iraqi WMD, we hadn’t considered the second hypothesis. We hadn’t thought through the possibility that it wasn’t there. We needed to be all-source questioners, not wedded to one scenario or forecast.

6. How can we be better collection managers? There is a danger that the closer one gets to collectors, the less objective we become. A “targeting analyst,” for example, gets very close to targeting units or operators. Where do you cross the line from being objective to having bought into an operator’s agenda and view of an issue? Does this start to impact the way you weight evidence or draw conclusions, in such ways as to support the views of the operators without question. As an example, one can point to a dispute within different elements of the IC over Iraq and al Qaeda. There was a distinctly different assessment to be found between the Counterterrorism Center (CTC) analysts and Near East analysts, partly based on their focusing on different aspects of the problem and having different outlooks. Those in the regional office saw less of a connection between the two than those whose job it was to find terrorists and help eliminate them. But this presents an analytical dilemma, for whose view do you put in front of the policymaker.

I’d like to make two points for improving the community:
1. Increase and improve training. This will improve the selection and promotion of senior officers. For military officers, education continues throughout their careers yet analysts get only four to five months. The IC needs professional, standardized, required education similar to the military services, formal education that occurs routinely throughout their careers.

2. Select senior managers through a DNI-wide service board. It would be based on the community perspective of qualified candidates, not solely based on their service to their home agency.

Panelist 3 (Civil Liberties Issues): My duties, IC wide, are to advise how to protect civil liberties in the context of the intelligence mission. You have a code of ethics on a card or analytic standards that align with civil liberties. My code is the Constitution of the United States.

The primary issue is that we operate under a veil of secrecy and most of the time mission statements are organic to each agency. This is critical to each intelligence agency and to operate in a secret environment. I operate outside those environments. People outside our agencies suspect a lot about what we are doing. I think they would love to hear how we wrestle with these issues such as ethos and intelligence as a profession.

I’ve been at ODNI since its stand up and the CIA before that. I believe there is already a common ethos and common respect and understanding of the tradecraft. I served on the McLaughlin panel at Fort Hood and we looked at ourselves critical in order to achieve any lessons learned or benefit from this. Accountability is important. A code should reflect things you are accountable for. If there is no accountability then there is a problem with the code.
Panelist 4 (IC Training): I have served in a variety of positions to include Deputy Chief of Staff at the ODNI, at the Department of Homeland Security (DHS), at the Department of Defense (DoD), and as a foreign service officer. This has been a tremendous day, yet we are still challenged. It’s partially about what you put on a card (referring to the lanyard/pocket cards sometimes used to remind employees about key issues) and the people involved in the mission. At the CIA, it’s all about the mission.

There are tens of thousands who apply for nominal hundreds of positions with the National Clandestine Service (NCS). It is an extensive process to find qualified NCS officers and then operators. We put our code of ethics – integrity, loyalty and professionalism -- on this shiny card so when you look at it you see a reflection of yourself. Integrity means that we exhibit the highest standards of personal honesty, and that we do not employ methods of tradecraft against ourselves. Personal integrity may override loyalty to the organization as long as dissent is given openly and honestly. We are loyal to the U.S. Constitution, our mission, our colleagues, our organization, and ourselves. Our sense of professionalism includes a sense of discretion (e.g., protecting how and who), appropriate risk taking, accountability and discipline (e.g., physical and mental toughness, and personal sacrifice).

Education is working with the community to discuss training standards. What is a collector and what does it mean to serve in that position? Are there different kinds of collectors or do we have a common vernacular. We know right versus wrong, but how do we deal with right versus right cases? We are you looking internally to make decisions?

The Tradecraft Training Division is one year old and is building a lessons learned facility. These are the lessons to get back out to our officers. We have nothing in between our
initial training and retiring. We’ve developed mid-career program called “reframing” to learn how to be a manager. We also have a scholarship program for 25 officers per year to go to graduate schools. The National Security Education program defined and set specific criteria to meet requirements of training.
Panel #3: Roundtable Question and Answer Session

Q1: What types of training tools are being used?

Panelist #1: I want to stress that when building a program from scratch, it takes time. While these people had a strong sense of ethics, we also wanted to formalize the process. A big part of the training was looking at case studies. It helped to build a body of scenarios to engage discussion.

Panelist #4: In our leadership training, we use case studies as a means to discuss ethical issues and problems.

Q2: Intelligence officers need to be very self-critical. Having no sense of ethics is to risk mission failure and personal difficulties. These are people who are authorized by society to do things that most are prohibited to do. How do we build on our own sense of ethics and work through these difficulties?

Panelist #3: We are hard on ourselves. From the outside we look like a profession. We’re secretive and we exercise powerful authorities and we can’t be sure. We have access to unbelievable amounts of data and assets compared to Law Enforcement agencies. Should they be part of the IC? What about the New York City Police Department? I think we look a lot different from the outside looking in and don’t need to kill ourselves with a super detailed code.

Q3: How would an IC-wide ethical code be perceived?

Panelist #4: Intelligence Community Directive (ICD) 401 gives the FBI a different authority. FBI ethics and CIA ethics are very different and the discrepancy is wide. The two agencies have
a completely different outlook on assets and human intelligence. There is still a need for an IC-wide code of ethics and we are all doing this to protect the security of the nation but we do this differently in each agency.

**Moderator:** Clearly, the CIA has a robust internal ethical code. I doubt each agency will want a new code.

**Panelist #1:** It is a complicated issue. For codes to be useful, they must be mission oriented. They must be able to be used to define right practice. Intel elements in the FBI are different because it is law enforcement. The types of interrogation used by the CIA would not be admissible in court but go to the heart of the mission.

**Panelist #2:** I believe there is an ambivalent response from intelligence analysts because to varying degrees, some are not sure what the profession of analysis is about. Until we have a rigorous certification process, it may not be seen as a true profession. The CIA efforts are laudable, but do not help with the community-wide ethos. There is ignorance in each agency about other agencies. I spoke to a senior Directorate of Intelligence (DI) official who joined in 1965. Back then you had the same training whether you went to the division of operations or division of analysis. I think this is a better approach. We need to integrate communities, not to degrade the agency, but for the specialized training of our personnel.

**Panelist #4:** We have a school with cross-community programs. This does bring people across different agencies to discuss what we do but we need more.

**Panelist #1:** We could learn more from our armed services. I’d like to learn more from the DoD and see how they square these issues.
Q4: How do we deal with a culture of bureaucracy?

**Panelist #1:** It is something we have to work on every day. As a senior officer, I would run evening sessions to talk to junior officers about ethical issues. It is difficult to detect self-censorship within the organization but like gardening, it requires constant cultivation in order to get any growth.

**Panelist #4:** When junior officers come to me, I tell them to find a senior officer who listens. And, we have a blog spot to ask questions anonymously.

**Panelist #3:** We should stress the importance of the Inspector General to the intelligence professional and emphasize that speaking truth is the most important without fear of reprisal. Keeping information secure must be a principle driven throughout the organization.

Q5: Is ethics and courage harder at higher levels?

**Panelist #1:** As a junior officer I saw how conservative senior folks were. I didn’t want to be concerned when I was at that level. I saw that my elders were very concerned about how they were seen. I tried to keep that in mind later. There were lots of issues with the Iraqi WMD report. I saw, day after day, IC briefers in the oval office and the president didn’t want to hear about how bad things were in Iraq. In my perspective, the IC did a good job with policy makers.

**Panelist #2:** At the War College, we tell the colonels to openly challenge each other. But when a brigadier general enters the room, the student body language changes. There is a culture in the military where it is negative to be seen as not being part of the team. It’s hard to face a policy maker with that perspective.
Panelist #3: Some of this is human behavior and will be present no matter what the rank. How do you raise an uncomfortable issue publically? It can be embarrassing. Sometimes senior people will let mistakes go and then scramble to correct the record later. It takes courage to point it out at the time.

Moderator: Thank you all for your participation today.
REMARKS BY LTG BURGESS, DIRECTOR DIA

Good afternoon and welcome to the Defense Intelligence Agency. On behalf of the agency and the National Intelligence University, we are grateful for your participation in this very importance discussion today.

Few of you may realize this, but right now I am serving in the most dangerous position in Washington because I am the guy standing between a day-long seminar and the end of the day for each of you.

So, I will try to adhere to the four hours allotted to me and get you out of here by 8:30 or so.

Actually, I will try to be mercifully brief and I believe I can because this is an issue that should not be difficult, at all.

Having reviewed the line-up of distinguished speakers and much of what was presented here today, my challenge is to distill what has been a complex discussion with many views and perspectives into a single concept that – hopefully – will inform the efforts by NIU students to build a moral code of ethics for intelligence professionals. Their first draft, I believe, is due March 30th and then subsequently, will be circulated throughout the community for discussion.

What I will propose is something that has rung increasingly true with every year that I have spent in this uniform and in the intelligence business at more senior positions.

And it is this:

While much of what we do is secret, our work is a public trust.
To some, there would appear to be a natural conflict between secret work and a public responsibility.

And others may see tension between trust and elements of HUMINT often require deception and manipulation.

But I know I speak for everyone in this room when I say there should be no conflict between “secret work” and our “public trust.”

As someone who has watched and been involved with the legislative process that created the Office of the Director of National Intelligence, reauthorized FISA and debates over publication of the intelligence budget, I keenly appreciate the tension inherent in what we call “process” – or what passes for process when the gears in the government machinery grind together on contentious issues.

There is tension, as there should be. There are enormous equities at stake, the most important of which are rooted explicitly in our nation’s foundational documents – the constitution, bill of rights, and the framework of statutes and executive orders that govern our work.

But I would venture to say that, notwithstanding that natural and even desired tension, there is no conflict between “secret work” and our “public trust.”

In fact, in our tradition of self-government, the former cannot work without the latter.

They cannot be separated.

Earlier in our history, we have seen what happens when secrecy violates the public trust and of course I am referring to the Church Committee hearings which, while painful for the
Intelligence Community, constituted a point of departure and led to a new framework upon which so much of our work today depends.

In the United States, secret work is a public trust. It must be viewed that way internally and externally to succeed.

But a statutory framework is one thing. Culture, tradition, training and discipline are quite another. As many of you have learned first hand throughout your careers, having a rule, regulation or policy on the books does not stop people, including at the senior levels, from making bad decisions.

Happens every day, whether personal or professional or some mixture of both.

And so that is why I strongly support the development of a moral code of ethics for the Intelligence Community. We owe it to our employees and to the American people to make explicit the high standards we must hold ourselves to every day, no matter how trying the circumstances we find ourselves in, no matter how far we are operating from “the station” or headquarters or no matter the pressure we receive from on high.

Which brings me to the topic of integrity, both personal and professional.

And I believe that often, integrity is needed most when it is hardest to maintain.

And in our line of business, our people – whether they are analysts or collectors -- get tested daily in ways that few outside the Intelligence Community can understand or appreciate.

I am talking about integrity in our analysis.

Integrity in our collection tradecraft.
Integrity to our sources, those who risk everything including their lives to work with us, and integrity to our customers, whether it is a Special Mission Unit, a combatant commander, the Chairman of the Joint Chiefs of Staff or the President.

Integrity sometimes requires the delivery of news that policymakers or commanders don’t want to hear.

Other times it requires us to say “no” when following a request or an order would cross an ethical redline.

Or sometimes we have to say “yes, but I want something signed by the agency’s general counsel or the Attorney General or a Presidential Finding, first.”

That is all part of speaking truth to power.

I also include how we conduct ourselves personally, at all ranks and pay-grades. It must be part of the equation.

Because at the end of the day, our colleagues, partners, allies and customers will consider our character and integrity when they weigh they truth, the value and the meaning of the information we provide to them.

I have seen it. Over my years in the Army and in the intelligence business, I have found there is a high correlation between personal and professional integrity. And that informed my thinking in hiring, firing and promoting.

In our personal and professional lives, we are defined by the actions and positions we take, less so how for we explain or rationalize them.
The right words left off a page can be as damaging as the wrong words included.

Character and integrity are not “nice-to-haves.” They are not “window dressing” to decorate a “rough and tumble” business. They are foundational elements in all of our efforts to safeguard the public trust – that trust given to us as individuals and to the Intelligence Community more broadly.

Earning that trust anew every day is part of our mission. And as we go forward as a community and as a nation into an increasingly complex and evolving strategic environment, we need to tools to instill that into every generation that comes into the Intelligence Community.

Recognizing that would be violating your trust if I go any longer, I am happy to take any questions.
Appendix 1: Intelligence Community Codes of Ethics, Alternative Views.

During the 2011-2012 academic year, NIU students prepared six alternative ethos statements/codes of versions for consideration by the wider intelligence community.

Version 1: IC Ethos Statement

1. **Service.** Our shared commitment to our national security mission must have priority, taking precedence over parochial interests, organizational as well as personal. We have an uncommon mission, and it requires selfless dedication to our Nation and its citizens.

2. **Integrity.** We must have the courage to seek and speak the truth…to our leaders and policymakers, our superiors and subordinates, our colleagues and co-workers, accepting the consequences of doing so, even in the face of personal or professional adversity.

3. **Accountability.** We must hold ourselves personally accountable for achieving results, as well as for adherence to all the laws and rules that govern how our most sensitive missions are to be accomplished. In this regard, we are ultimately accountable to the American people, for protecting them from harm, but also for protecting their privacy and civil liberties.

4. **Professionalism.** We must always foster a competitive, highly trained, and proficient workforce. The value of intelligence starts with our people. Professionals in the intelligence field protect their sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order.

5. **Duty.** We must stand ready to engage, deploy, and destroy the enemies of the United States of America, both foreign and domestic. Duty to our country comes before individual desires.

6. **Agility.** We must be adaptive to our rapidly changing world using mission-driven professionals who embrace innovation and initiative.

7. **Tradition.** "You can't move forward if you don't understand your past." The IC is the result of much more than the National Security Act of 1949, it has undergone hundreds of minor tweaks, adjustments, evolutions, and restructures due to the "4 P's" of many administrations working in vastly different geopolitical environments. We cannot afford to make the same mistakes again…the legacy we leave behind is directly related to the work we do today.
Version 2: IC Core Values and Code of Conduct

Introduction

The U.S. intelligence community (IC) is committed to the highest ethical standards of conduct in pursuit of its goal to provide policy makers with needed intelligence. Accomplishing this mission demands integrity, good judgment and dedication to public service from all members of the community. While the IC affirms each person’s accountability for their individual actions, it also recognizes that the shared mission and the shared enterprise of the IC require a shared set of core values and ethical conduct to which each member of the IC must be held accountable. Furthermore, the IC acknowledges that an organizational culture grounded in trust and faithfulness to the Constitution is essential to supporting these core values and ethical conduct. The following Statement of Core Values and Code of Conduct are intended to build, maintain and protect that trust, recognizing that each member of the IC is responsible for doing his or her part by upholding the highest standards of competence and character. The nature of IC operations is such that the IC Code of Ethics is focused on expounding the IC’s core values in lieu of a detailed list of ethical requirements. Understanding of and adherence to the IC’s core values provides a framework for ethical action in defense of the nation.

Applicability

The IC Ethics policy applies to all members of the IC community. The IC community includes:

- Oversight bodies charged with the governance or monitoring of the IC;
- All individuals employed by the IC to include vendors and contractors; and,
- Agents of the IC insofar as those agents are acting on behalf of an agency.
Members of oversight bodies and IC employees shall participate in periodic ethics policy training and shall certify compliance with the IC Ethics Policy as determined by the Director of National Intelligence (DNI) or the DNI’s designee. Vendor and contractor compliance with the IC Ethics Policy shall be incorporated into written agreements to which an IC agency is party. IC agents shall be briefed on relevant IC Ethics Policy requirements. The IC Ethics Policy governs only official conduct performed by or on behalf of an IC agency. Violations of the IC Ethics Policy may result in disciplinary, civil, and/or criminal action.

Statement of Core Values

Every member of the IC is required to adhere to the IC’s Statement of Core Values – Integrity, Excellence, Accountability, Respect for Others, Loyalty, Diversity, Collegiality, Courage, and Trustworthiness. These values form and guide the daily work of both the organizations and personnel that comprise the IC.

1. **Integrity** – We will be honest, fair, impartial, and unbiased as we collect, report, analyze, and disseminate information. We will be true to the law and report wrongdoing if it is encountered. Professionals protect their sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order.

2. **Excellence** – We will perform our duties in a manner that fosters a culture of excellence and high quality in everything we do. Our work ethic must reflect this goal.

3. **Accountability** – We firmly believe that our mission is a public trust. We will live up to this trust through safeguarding our resources and being good stewards of the American tax dollar.

4. **Respect for Others** – We recognize the inherent dignity and rights of every person, and we will do our utmost to fulfill our responsibility to treat each person with fairness, compassion and decency. We will employ the least intrusive methods to accomplish the mission at hand. We recognize that the nature of our profession inherently conflicts with human dignity but we strive to minimize that conflict while serving as guardians of our nation and its way of life.

5. **Loyalty** – We will serve the American people, be true to the U.S. Constitution and, consistent with the law, and obey the leaders of the U.S. government. We hold the protection of the American way of life a sacred duty.
6. **Diversity** – We are committed to diversity because a wider range of backgrounds and experiences makes us a stronger learning organization and more effective in meeting our mission. We are committed to maintaining a culture of inclusion that treats all employees fairly and provides equal opportunities based on merit. Our employment policies prohibit discrimination.

7. **Collegiality** – We strive to share and disseminate our work to the widest possible audience. Members of the IC will cooperate with each other for the betterment of the country.

8. **Courage** – The defense of the nation requires both moral and physical valor. We aim to exhibit both.

9. **Trustworthiness** – We recognize that the work we do is inconsistent with openness and transparent government. We will mitigate this by sharing as much as possible and declassifying records. The inherent secrecy of the IC requires extra vigilance to adhere to this code of ethics.

**Purpose of the Code of Conduct**

The IC recognizes that each employee attempts to live by his or her own values, beliefs and ethical decision-making processes. The purpose of the Code of Conduct is to guide employees in applying the underlying IC Statement of Core Values to the decisions and choices that are made in the course of everyday endeavors. Each IC Agency should ensure that its ethical policies are consistent with this IC policy.

**Code of Conduct**

As members of the intelligence community we will:

1. Seek the truth and report it accurately.

2. Continually strive to increase the quality of our work while complying with the professional standards that govern our work.

3. Put loyalty to the highest moral principles and to country above all else.

4. To the maximum extent possible, promote the sharing of information. Avoid over classifying.

5. Be fully accountable to management, the executive and legislative branches as well as the American people.
6. Support an environment of respect for the rights and viewpoints of all people.

7. Avoid improper political activity.

8. Professionals in the intelligence field protect their sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order.

9. Disclose and manage potential conflicts of interest.

**Interpretation and Sources**

The Statement of Core Values and the Code of Conduct are intended to address significant ethical challenges that an IC employee may face in the course and scope of employment. However, situations may arise resulting in actual or perceived conflicts between the various core values and conduct statements. IC employees are charged with executing a potentially dangerous and always challenging mission with minimal oversight by the public other than through the Constitutionally-established mechanisms in place through the U.S. Congress. Self-governance and mutual forbearance are required to ensure effective implementation of the IC Ethics Policy. IC employees are encouraged to discuss potential ethical challenges with objective parties, in a manner consistent with security protocols, such as the agency general counsel, inspector general, or ethics ombudsman.

There are additional sources of authority that address specific questions or situations. Examples include: the U.S. Constitution, acts of Congress, treaties and conventions to which the United States is party, Executive Orders, DNI Directives, agency policies and procedures, and the international Law of Armed Conflict.
Version 3: An IC Wide Ethos

I am an Intelligence Professional.
I serve the People of the United States.
I will defend the Constitution and exemplify our nation’s values.
I will embrace the fairness of fact and fight to mitigate bias.
I will integrate my work with that of my peers from all agencies.
I shall not endanger others or my country with incomplete information.
I will protect my sources and methods.
I will master my craft.
I am proud to be an Intelligence Professional.

A holistic approach was used to design this ethos, beginning with a thorough review of existing ethical codes. This IC-wide ethos implements the best frameworks and themes from a broad range of reviewed material. Among the most effective codes reviewed and implemented in the IC-wide code include those from the medical community, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the U.S. Coast Guard (USCG). In addition to using frameworks presented by the above existing codes, an examination of core concepts in classroom discussions helped develop an understandable, relatable, and above all, applicable ethos for the entire intelligence community (IC).

The initial target audience for this project was the members of IC agencies; however, as research progressed, the target audience gradually expanded to include the American people as an integral portion of the audience. We came to realize that an ethical code is meant to serve the general public involved with the agency, however tangential, just as much as the intended recipient of the code (the IC). One reason for this is to gain back credibility and trust from the American public that may have been lost during recent events that undermined public confidence in the community, such as the fiasco involving Weapons of Mass Destruction (WMD) in Iraq. While the focus of this code is not to specifically address culpability for perceived intelligence failures, this ethos is a reminder that the IC is aware that the ultimate goal of the organization is
to proudly serve the American people while upholding the defense of national security. Ultimately, the goal of this ethos serves two purposes: to guide every member of the IC in daily activities while also rebuilding the relationship between the American people and the IC that is vital to national security and prosperity.

The IC-wide ethos is divided into three critical elements to specifically address each of these goals: Distinguishing Character, Guiding Beliefs, and Fundamental Beliefs.

**Distinguishing Character**: The first section of the ethos serves as a reminder that intelligence analysts, collectors, and managers are not only experts in each intelligence field, but above all, are *professionals*. Further, this section outlines the ultimate goal of the intelligence community: to serve the people of the United States. The nature of this work requires navigation through a challenging environment that demands high moral and ethical standards. Through this challenging environment, this code serves as a moral compass to guide IC members by reminding them of the ideals and values they defend and that their actions must always be above reproach.

**Guiding Beliefs**: The second section outlines intelligence-specific challenges that IC members should endeavor to always follow through the course of public service. Embracing and weighing all facts equally will ensure that inherent bias is effectively mitigated in collection and analytical efforts. Integration is identified by the Director of National Intelligence as one of the three core characteristics essential for effective intelligence work. Articulating this in the IC-wide ethos demonstrates a never-ending commitment to share information and collaborate on collection. Incomplete information or analysis can improperly influence policymaker’s decisions affecting credibility of the United States at home and abroad. These policy decisions carry not only the security and future prosperity of the United States, but also directly impact U.S. service
members and allies serving on the front lines. The IC always strive to provide the most complete information possible for the war fighter; and where needed, articulate remaining gaps to policymakers without exception or fear of reprisal.

**Fundamental Beliefs:** This final section summarizes what each intelligence professional must embrace to be successful in the intelligence community. Protection of sources and mastery of all skill-sets and management levels will enable every member of the IC to be successful as a team, an agency, and a community. Professionals in the intelligence field protect their sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order. The final line, though at first glance appears repetitive, contains one important addition: pride. Though many of our greatest accomplishments may never be known; we must always take pride in our quiet service to the nation and the professional manner in which we serve.

**Distribution of Message Ideas**

The most successful messages that “stick” tend to have innovative approaches. Anchoring new approaches in the IC through a simple message: “I am an Intelligence Professional,” has the capacity to positively change the current culture and create better performance through customer and productivity-oriented behavior.27 Some key ideas to spread this message include displaying a banner or plaque through each entry and exit of IC buildings with this simple statement: *I am an Intelligence Professional.* Additionally, badges issued by each agency should include the statement on the front: *I am an Intelligence Professional.* Accompanying each badge will include a similar sized card to carry that has the extended version of the IC-wide ethos. Chief Executive Officer (CEO) Alan Mulally of Ford Motor

---

Company turned around the company by embracing the concept of distributing a similar message relative to his company. The corporate motto, “We are One Ford,” is now printed on the back of every employee’s ID badge.\textsuperscript{28} Some other ideas to help IC members embody the IC-wide code include adding the statement, \textit{I am an Intelligence Professional} to office letterhead, adding quarterly awards that are given to individuals embracing the code, challenge coins with living the code, and something as memorable as including the statement in fortune cookies distributed in the building. If the IC is serious about its members internally embracing an IC-wide ethos, the desired message must be readily visible in the simplest of ways.

HUMINT Professional Ethos

I am a HUMINT professional interrogator. I have been entrusted by the U.S. government and the agency I serve with the unique mission of acquiring information from human sources. I must abide by the laws and regulations of the Constitution, my government, and my home agency in the performance of my duties. I am self-reliant, investigative, alert, and well trained in the art and skill of active and passive information collection as a HUMINT professional. I have been entrusted to foster positive relationships and communicate effectively. I will strive for constant improvements in myself and my profession while maintaining appropriate bearing and resiliency. I am a professional, will take pride in my calling, display the highest levels or moral and ethical conduct, be an example to others, and understand that I must always reflect integrity as I serve. I will protect my sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order. I will uphold the value of human life and will not deprive others of their rights and privileges. I willingly commit to this creed and to the profession of Human Intelligence.

HUMINT Core Values:

- Duty: Devotion to duty comes first
- Integrity: Adheres to legal, ethical, and moral principles and standards
- Objectivity: Maintains an unbiased attitude towards sources and information
- Credibility: Provides clear and accurate assessments to superiors
- Respect: Treats sources fairly to encourage cooperation
- Initiative: Remains cognizant of the environment and exploits new opportunities
- Self-Control: Maintains both personal patience & psychological well-being while working with sources
HUMINT Professional Creed:

- I am a proud American HUMINT professional.
- I will fatefuly adhere to all regulations
- Never discouraged by opposition or noncooperation,
- Always assessing the veracity of new information;
- I am emotionally detached, but empathetic to my sources.
- While I am persuasive with my sources, I am completely honest with my comrades, for in courageous truth lies intelligence victory.
Version 5: HUMINT Collector Ethos

As a human intelligence (HUMINT) collector, I will pursue our intelligence needs with vigilance, persistence, initiative, and tenacity, knowing our Nation depends on my efforts. Predictive knowledge of our adversaries’ capabilities, plans, and intentions affords the United States a strategic advantage against its adversaries. The manner in which I execute my operations reflects equally upon my level of professionalism and my credibility. Tradecraft provides a powerful toolkit designed for exclusive use only during operations. American law frames our opportunities and serves as guidance, although not as counterproductive lists of prohibitions and limitations. During HUMINT operations, context and content are equally important. The value in secrecy lies inherently within operational security, not within the compartmentalization of intelligence to prevent disclosure to our customers. I will capitalize on the opportunities presented by operational ambiguity, and embrace the principal of favorability. Thorough operational planning is critical and enables me to react to the realities I am presented with, as operations unfold.

HUMINT Collector Core Values

**Autonomy:** I recognize that HUMINT collection methods are often ambiguous and ill defined. This subjective paradigm allows me operational freedom to execute my mission without restrictive management from superiors.

**Imagination:** Creativity is the cornerstone for problem solving. History and tradition are not substitutes for innovative thought processes. I recognize the value in the indirect approach and the pitfalls of linear thought.
**Risk Taking:** HUMINT collection holds an inherent amount of risk. I will not shy away from operations simply because the risk involved. I will strive to develop courses of action designed to mitigate the degree of risk while accomplishing the mission.

**Resourcefulness:** Working alone and far from headquarters, I realize that resources and organizational support can be scarce. My ability to leverage all available tools at my disposal and improvise to overcome unexpected challenges will result in mission success.

**Professionalism:** I represent my organization, the intelligence community, and the U.S. Government during the course of my professional duties. I will remember that when I interact with foreigners outside the borders of America and far from home, I am the United States. Professionals in the intelligence field protect their sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order.

**Statement of Purpose**

After the passage of *Intelligence Reform and Prevention of Terrorism Act* (IRPTA) in 2004, the human intelligence (HUMINT) community has been broadened and expanded to reach across several intelligence community (IC) agencies, as well as maintain a role in the Department of Defense (DoD). With more entities now conducting HUMINT operations, a code of ethics is necessary to guide the behavior of all HUMINT operators. The Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), as well as the DoD, all have a role in HUMINT collection, but each has vastly different cultural practices. The necessity for this ethical code is rooted in the recent statutory changes which dramatically impacted the organizational structure of the HUMINT community.
First, the focus of this ethical code is for overt and clandestine HUMINT collectors, not analysts. The code should serve as a tool designed for the specific challenges of HUMINT operations. The audience for this code is the HUMINT collectors themselves; however, the code is unclassified and accessible for both internal and external consumers. This transparency helps mitigate the distrust often created by the secret nature of the profession. The code serves to fulfill the social contract between the IC and the public it serves.

The mission focus for all HUMINT intelligence collectors should be in support of a common IC goal. Historically, the objective of each agency was to focus on specific mission requirements and accomplishment. Additionally, some agencies have not been organizationally focused on HUMINT operations. For example, the FBI has traditionally been focused on law enforcement procedures. However, information sharing now has to be conducted across agencies for one unified goal. A common ethical code can align the disparate organizational cultures and facilitate a sense of community.

Second, this ethical code focuses on virtue ethics, placing value on the positive attitude toward a moral duty. Highlighting the ideal representation of a HUMINT collector will help to shape the IC in the future. Developing this ethical code aids in combating past practices of consequentialism. Historically, some IC collectors have defaulted to a utilitarian approach to justify their actions. Utilitarianism states that the proper course of action maximizes overall happiness and effectiveness. The contemporary environment demands that the actions of HUMINT collectors be driven by an ethically guided process. Increasing public scrutiny combined with significant economic cutbacks emphasizes the importance of virtue ethics within the secret society of HUMINT collectors. The HUMINT collector ethical code will guide the conduct of good intelligence with a focus on proper ethical consequences.
Version 6: Analytic Community Ethos

The intelligence cycle captures the complex process of producing valuable intelligence for the policymaker by packaging it into five discrete stages: planning and direction, collection, analysis, production and dissemination. Throughout each stage, significant ethical issues arise that analysts, collectors, and policymakers must consider as they contribute to the intelligence community’s mission to evaluate security interests to inform policy decisions. Intelligence analysts play a unique role in each stage of the intelligence cycle, making it a particularly useful framework from which to construct an ethical code specific to the analytic community. Professionals protect their sources, and disclose both corruption and questionable activities pursuant to law, rule, regulation and executive order.

The intended audience for our ethical code is analysts in the U.S. intelligence community (USIC), rather than for public release. This is for several reasons. First, since analysts regularly face a specific set of issues throughout each stage of the intelligence cycle, they will realize greater benefit from a code that is specifically tailored to their analytic work. Second, concepts and terminology that may be unfamiliar to the general public, such as the relationship between the National Intelligence Priorities Framework and collection or the problem of stovepipes within agencies, speak specifically to the analytic community. Our belief is that a narrowly focused code of ethics will provide more direct applicability to an analyst’s daily work.

In addition to a specific audience, we also crafted the code of ethics with a very specific purpose. The code does not simply outline general inspiration principles—rather, it articulates specific directives of ethical behavior for the most important issues at each stage of the intelligence cycle that analysts must adhere to in order for the mission to succeed. Driven

---

primarily by the imperative voice, the code’s language and tone reflect the seriousness and attention to detail with which analysts daily approach their vocation. The determined and focused effort that analysts dedicate to the substantive issues at each stage of the intelligence cycle must also be applied to the ethical issues that ultimately affect the success of the mission. In essence, adherence to the code enables the ultimate purpose of intelligence analysis: to turn raw information into useful assessments for the policymaker.30

The code also addresses the analytic community’s various relationships with other participants of the intelligence cycle. For instance, in the planning and direction process, analysts must prioritize their efforts based on requirements provided by the policymaker. In collection, the analyst must respect the complex relationship with the collector. During the analysis phase, the code stresses the importance of objectivity, honesty, and self-examination to avoid politicization. The production stage speaks to the analytic community’s responsibility to the American people, recognizing a product’s concrete influence over policy, public resources, deployment of military force, and legislation.31 Finally, the dissemination phase calls analysts to uphold the integrity of their analysis by speaking truth to power in their relationship with the policymaker and collaborate ethically with other levels of government and foreign partners.32

Despite its direct tone, the code cannot be strictly enforced due to the inherent subjectivity of analytic work. Still, we believe it can raise the standard of analysis in the community. The imperative language warns analysts individually and collectively that ethical decisions made at each stage of the intelligence cycle contribute to the USIC’s ability to protect

30 Born and Will, 48.
31 Ibid., 47.
32 Ibid., 48.
national security interests. By the nature of the intelligence cycle, this ethical code is detailed in its attention to the diversity of concerns within the intelligence community but general in its flexibility to address analysts from each agency. Some may criticize the intelligence cycle’s inability to comprehensively explain a highly complex process. Ultimately, however, we believe it provides the most valuable framework to inform and guide the analytic community’s ethical behavior.33

The Ethical Intelligence Cycle

1. Planning and Direction:
   - Ensure targeting and collection priorities are proportional to the national interests at stake.
   - Use the National Intelligence Priorities Framework when considering potential outliers and anomalies.
   - Consider the least intrusive methods first. Open source should be your first resource.
   - Recommend that resources be used wisely and anticipate potential consequences in allocating collection requirements.
   - Be objective and avoid political influence in developing collection requirements.

2. Collection:
   - Provide honest and timely feedback to the collector.
   - Act responsibly as your own collector. Do not collect just to collect; collect within the scope of your mission.
   - Take care to describe the source properly – be diligent and objective in the source description.
   - Protect sources and methods.
   - As an analyst, your job is not to direct or instruct collectors to take action. You recommend.
   - Appropriately scale collection to the immediacy and severity of the threat.

33 Born and Wills, 42-43.
3. Analysis:

- Avoid abuse of access to information.
- Recommend but do not direct.
- Trust but verify – seek the truth, evaluate information and do your best to corroborate information with other sources; however, do not immediately distrust single source information.
- Maintain objectivity and avoid politicization.
- Always use alternative analysis and consider the widest possible range of hypotheses.
- Do not lie or overinflate in your analysis.
- Let the policymaker be the policymaker – do not make policy decisions. Remember the difference between providing political context and taking a partisan position.

4. Production:

- Be cognizant of the weight that analytical products carry; understand that assessments have influence over policy, allocations of public resources, deployment of military force, and legislation.
- Coordinate with the widest possible range of IC experts before disseminating analytical products.
- Strive to find a balance between quality and timeliness in production – an on-time C- product is worth far more than an A+ product that is too late.

5. Dissemination:

- Speak truth to power – give the policymaker accurate information rather than what he or she wants to hear.
- Don’t be a stovepiper – disseminate to the widest possible audience; when in doubt about sharing or disseminating information, seek guidance.
- Always follow your agencies guidelines for appropriate dissemination and release of information to domestic and foreign intelligence partners.
Appendix 2: Recommended Reading List

This reading list provides a wide range of books and journal articles on diverse ethical issues for intelligence professionals.


Blanc, Maria F. “Moral Permissibility and Legitimacy of the Use of Coercive Interrogations: Implications for the Intelligence Professional, Participating Health-Care Professionals, and Society.” *International Journal of Intelligence Ethics*, vol.1, n.1, (Spring 2010).


Erskine, Toni. "'As Rays of Light to the Human Soul?' Moral Agents and Intelligence Gathering." *Intelligence and National Security* 19, no. 2 (Summer 2004): 359-381.


Langan, John, S.J. "Moral Damage and the Justification of Intelligence Collection from Human Sources." *Studies in Intelligence* 25, no. 2 (Summer 1981): 57-64.


Treverton, Gregory F. "Covert Action and Open Society." *Foreign Affairs* 65, no. 5 (Summer 1987): 995-1014.


American Bar Association. “About the ABA.”

American Dental Association. “Mission and History.”


Cable, Josh. “Management Lessons You can Learn from Alan Mulally: Kotter’s 8 steps,”

Central Intelligence Agency. “Clandestine Service.”

Defense Intelligence Agency, Office of the Research Director. DI Analyst Career Development Portal, available on JWICS.

———. “Competency Development Guide,” available on JWICS.


Goldman, Jan. ed.* Ethics of Spying: A Reader for the Intelligence Professional*. Lanham, MD: Scarecrow Press, 2006. Appendix A provides a useful range of exemplar documents illustrating the range of material regarding intelligence community principles, creeds, codes, and values.


IC Core Values Statement, 7 August 2007, available on DNI Homepage (JWICS).

Institute of Internal Auditors (IIA). “Code of Ethics.” URL: [https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx](https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx). The IIA sets the professional standards for internal auditors internationally. Many elements of internal audit work coincide with intelligence analysts. In particular, both operate as key supports in providing information and “intelligence” to decision-makers but generally are not involved in setting policy and must remain objective in their efforts.


Pierce, Dr. Albert C. “The Value of an Ethos for Intelligence Professionals,” paper delivered at the Annual Meeting of the International Studies Association, 2 March 2007, Chicago, IL.


Shaw, George Bernard. The Doctor's Dilemma, Act 1 (1906).


The UN Charter, Article 2 (4).


