Syllabus Section 1 — Human Intelligence: From Sleepers to Walk-ins

1. Week 1 (5 September 2006)
    a. Intelligence vs espionage
        i. *Intelligence* covers all the different ways of deliberately collecting information for national advantage — satellites, wiretaps, reading the open press, etc
        ii. *Espionage* refers specifically to the use of human spies to collect information
    b. Overt vs Covert vs Clandestine
        i. Overt: Open and above board. Not secret or hidden.
        ii. Covert: The event itself is publicly observable, but the sponsorship is hidden. For example, an intelligence service can covertly supply weapons to one side in a war. The fact that the weapons are there and being used is publicly observable, but their source is hidden.
        iii. Clandestine: Hidden or secret. The work of a spy is clandestine -- completely hidden, hopefully for all time.
    c. Legal vs Illegal
    d. Definition of intelligence (from Lowenthal)
        i. *Intelligence* is information that meets the needs of policymakers and has been collected, refined, and narrowed to meet those needs.
    e. Where is the intel? Is it available overtly? Is it a secret, but a secret not worth stealing? Is it a secret that is worth stealing?
        i. Overt information is cheap and easy to collect
        ii. Some secrets are valuable, but not crucial. These are left alone. Too much risk compared to likely payoff.
        iii. A small slice of secrets are valuable enough to steal. That is why (some) countries have secret intelligence services.
    f. Intelligence failure: WMD in Iraq (Topic came up. Not part of original

lesson plan.)

i. National Intelligence Estimate (NIE) of October 2002
    1. Unambiguously stated Saddam had WMD
ii. NIE had little recent HUMINT to drawn on
    1. Not surprising, since Saddam spent most of the previous decade killing everyone suspected of having anything to do with the USG
iii. NIE compensated by relying on three other sources of information
    1. Historical information
        a. Nuclear program we discovered after Gulf War was far more extensive than we had thought
        b. Chemical program revealed in mid-1990s
        c. Repeated use of CW against civilians
        d. Consensus of world's intelligence services
    2. Negative inference
        a. E.g., if Saddam won't explain what happened to the 6,000 CW bombs missing from Iraq/Iran war, we assume he still has them
    3. COMINT, SIGINT, satellite photos
        a. E.g., buildings we knew manufactured WMD in the past were being physically expanded
    4. NIE deliberately erred on the side of caution

2. Week 2 (12 September 2006)

a. Intelligence Cycle
    i. Requirements
        1. Things we need to know, questions to which policy makers need answers
        2. Levied by policy makers (mostly in the Executive branch) and by people in the Intelligence Community
        3. In practice, intel collectors in the field usually know

what the requirements are without much guidance

ii. Tasking
    1. Assignment of assets (technical or human) to collect intelligence to satisfy the requirements
        a. Collecting of the intelligence, e.g., steal the secrets — this is sometimes included as a separate step in the Intelligence Cycle
        b. Processing of the intelligence, e.g., put it in a written form to send to the intelligence analysts — this is sometimes included as a separate step in the Intelligence Cycle
    2. Done by operational entities, e.g., CIA's National Clandestine Service, National Security Agency
    3. The product is *raw intelligence*, e.g.
        a. Written report from a human source
        b. Transcript from a cell phone intercept
        c. Satellite photo of a training camp

iii. Analysis
    1. Evaluation and interpretation of raw intelligence
        a. CIA's Directorate of Intelligence
        b. National Geospatial Intelligence Agency (photo interpretation)
        c. State Dept's Bureau of Intelligence and Research
        d. Others
    2. Draws mostly on open source material
    3. Product is *finished intelligence*, e.g.
        a. *President's Daily Brief*
        b. *Senior Executive Intelligence Brief*
        c. Ad hoc studies and papers
        d. Production is sometimes included as a

separate step in the Intelligence Cycle

iv. •Dissemination
    1. Finished intelligence is sent to consumers, e.g., policy makers, members of the intelligence community
    2. Raw intelligence is also disseminated, e.g., terrorist threat reports. Policy makers need to treat raw intelligence far more cautiously than finished intelligence.
    3. Disseminated intelligence generates more questions, which lead to another round of requirements

b. Broad categories of intelligence collection — the INTs
    i. Open Source (OSINT) — Ninety-five percent of everything we know
    ii. Technical intelligence
        1. Signals Intelligence (SIGINT) and Communications Intelligence (COMINT)
            a. Intercepting and decoding communications
            b. Purview of National Security Agency (NSA), which is also responsible for America's own codes
        2. Electronic Intelligence (ELINT), e.g., radar signals
        3. Telemetry Intelligence (TELINT), e.g., missile test data
        4. Measurement and Signatures Intelligence (MASINT), e.g., lasers, particle beams, various categories of WMD
        5. Overhead Photography
            a. Satellites and planes
            b. National Reconnaissance Office (NRO) operates America's satellites, National Geospatial Intelligence Agency (NGA)

interprets the images

c. Cold War was heyday for manned recon (SR-71, U-2), but most of today's are Unmanned Aerial Vehicles (UAVs)

6. Technical systems were build for Cold War
    a. Designed for use against big, slow-moving, relatively visible targets; e.g., armies, military bases, government ministries
    b. Not designed for use against small units, terrorist cells

iii. Human Intelligence (HUMINT)
1. HUMINT collection is classic espionage — spies, cloak-and-dagger
2. HUMINT is about people betraying their side (e.g., government, NGO) by passing secrets to our side
3. CIA's National Clandestine Service (NCS) is America's premier HUMINT collector
4. Other USG agencies also contribute, e.g., DIA's Defense HUMINT Service

c. What is an "agent?"
i. An agent is a member of a target organization (e.g., foreign government, terrorist cell) who clandestinely passes secrets to the USG
1. Think of the 'agent' relationship in commercial law
ii. In the eyes of the target organization, the agent is a traitor
iii. The agent is recruited and handled by a case officer
iv. Protection of the agent's identity is crucial

d. Clandestine Service Officers
i. People in the Clandestine Service who go aboard to conduct espionage are *officers*, not agents
1. Operations Officer (aka Case Officer)

2. Collection Management Officer (aka Reports Officer, Intelligence Officer)
3. Operational Targeting Officer
4. Language Officer
5. Special Skills Officer
    a. Looms larger since 9/11

e. Cover in the Clandestine Service
    i. False story about who you are and what your job is
    ii. Provides general access to targets of interest
f. Two broad types of cover — official and nonofficial
    i. Official cover
        1. Government employee, typically a diplomat
        2. Broad entrée to classic targets (e.g., Ministry of Foreign Affairs), but less access to people associated with al-Qa'ida and company
        3. Diplomatic immunity
    ii. Nonofficial cover
        1. Any cover besides that of a government employee
        2. Officers under nonofficial cover are called NOCs
        3. Traditionally low-profile handlers of sensitive penetrations, not recruiters
        4. Possibly better able to gain access to terrorist circles
        5. No official protection
g. Types of Agents
    i. Classic recruitment
        1. Case officer convinces person to commit espionage
    ii. Walk-in
        1. Shows up and offers his services
        2. Historically some of the best agents
            a. Oleg Penkovsky (British/US agent)
            b. John Walker (Sov agent)

c. Aldrich Ames (Sov agent)
d. Jonathan Pollard (Israeli agent)

iii. Access agent
    1. Does not have access to intel, but knows others who do
    2. Important against terrorist target

iv. Double agent
    1. Side A thinks the agent is a penetration of side B, but agent is really a penetration of side A working for side B (or even side C)
    2. Often a channel for disinformation

v. Support agent
    1. E.g., safehouse keeper

vi. Covert Action agent
    1. E.g., foreign journalist who can do press placements

vii. Agent of Influence
    1. Someone who can affect policy of a foreign entity

h. Impromptu discussion of James Jesus Angleton, CIA Chief of Counterintelligence, 1954-1974
    i. Came to believe CIA was penetrated by KGB
    ii. Believed KGB exerted such control that any Soviet official who allowed himself to be recruited by the West had to have been a double agent — i.e., pretending to cooperate with Western intelligence, but really controlled by the KGB
    iii. See “Of Moles and Molehunters” in **Optional Readings**. This article is a review of various books written on Angleton and counterintelligence, and gives a decent flavor of the controversies surrounding him.

i. Impromptu discussion of Morris Childs, American communist who reported to the FBI on his intimate contacts with the Soviet and PRC leaderships over several decades.

3. Week 3 (19 September 2006)
    a. Ethics and intelligence
        i. The distinction between Justice and Utility offers a useful model for evaluating the ethics of intelligence operations
            1. *Justice* (defn): Treatment in accordance with dessert — i.e., treating people as they deserve to be treated.
                a. Past-looking
                    i. What a person has done in the past determines how he or she should be treated in the present — e.g., if you robbed a bank, you should go to jail; if you worked hard all day at an agreed-upon $10 per hour, you should be given $80.
                b. Oriented toward the individual
                    i. Looks at the past actions of the individual
                    ii. Immanuel Kant and the Categorical Imperative — Treat each individual as an end in himself, not as a means to an end.
                c. We tend to side with considerations of justice in most situations in everyday life.
            2. *Utility* (defn): Act to promote the greatest good for the greatest number — See the 19th British Utilitarians, e.g., John Stewart Mill, Jeremy Bentham. For a 20th century proponent, see J.J.C. Smart.
                a. Forward-looking
                    i. Do what will have the best results for the future, regardless of what has happened in the past.

   b. Oriented toward the group, the collective
      i. Promote the best results for the most people, with each person counting as one
   c. When our moral intuitions lead us to make decisions based on utility, it is usually in cases where the consequences are extraordinarily significant.
      i. For example, if there are five people in the lifeboat and the lifeboat can only hold four, we would probably say the right thing to do is to toss one individual overboard and save the other four, rather than keeping all five in and letting the boat sink. Even though the act of tossing the person overboard would be unjust — i.e., that person would not deserve to be thrown overboard — still we tend to feel it would be the right thing to do, because the consequences are so significant.
3. In the world of intelligence operations, the consequences are often very significant — e.g., the safety of a nation may hang in the balance. Thus, when we try to morally justify intelligence operations, we tend to do so on the basis of utility. If we look at these matters from the standpoint of justice (i.e., from the viewpoint of how people deserve to be treated), we tend to see intelligence operations as immoral and difficult to justify.
   a. The best way to look at this is as a hypothetical

— i.e., if we believe an intelligence operation is morally correct (or even obligatory), we are probably basing our belief on utility ("This is the best thing for my country") rather than on justice.

b. Agent Recruitment
    i. Classic steps one goes through to recruit a spy
    ii. Used by intelligence services around the world
    iii. Has limitations when used against Islamist terrorist organizations like al Qa'ida
    iv. For details on the steps outlined here, see *Running a Ring of Spies* by Jefferson Mack. For a good real-world view of the application of these principals, see the texts assigned for the HUMINT section in our syllabus.
        1. Step 1: Spot
            a. Looking for people with access to information of interest
            b. Techniques
                i. Mixing in target-rich environments, classically the diplomatic circuit
                ii. Attending conferences, meetings, professional functions
                iii. Surveillance
                iv. Public and semi-public documents, e.g., internal phone directories
                v. Problem: Where do you go to spot al Qa'ida affiliates?
        2. Step 2: Assess
            a. Once a potential spy is identified, his exploitable vulnerabilities and motivations are scrutinized

i. Lonely? Looking for a friend?
ii. Low salary? Greedy? Needs money to send children to school?
iii. Ideological motivation? Hates his system, admires ours?
iv. Passed over for a promotion? Not appreciated by peers and superiors? Seeking praise and recognition?
v. Adventurous? Looking for personal challenge? Wants to be James Bond?
vi. Egomaniac? Wants prove he can get away with it?
vii. Problem: What can you exploit with an al Qa'ida terrorist?

3. Step 3: Recruit
    a. Case officer builds relationship with potential agent, who at this stage is called a *developmental*
    b. Drawing on his knowledge of the developmental's vulnerabilities, the case officer builds trust and solves problems for the developmental
    c. Case officer moves the developmental toward treason
    d. Starts by asking for innocent information, gradually moving into more sensitive and confidential areas
    e. May request documents — open source at first, then classified
    f. Case officer moves the meetings into more private settings, getting the developmental

used to a clandestine relationship

g. All the while, case officer is building psychological control, helping the developmental justify to himself his increasingly treasonous behavior
h. When the time is right, the case officer ‘pitches’ the developmental, offering cash in return for an unambiguous espionage relationship
i. Problem: Social environment of an al Qa'ida developmental makes this phase difficult

4. Step 4: Test
    a. Compare agent’s information to known facts, both secret and overt
    b. Watch for red flags, e.g.:
        i. Does agent’s reporting contradict other intelligence accepted as true?
        ii. Do the verifiable portions seem to have appeared in the open press?
        iii. Does much of the agent’s reporting focus on past events, with his “behind the scenes” commentary thrown in?
    c. Check information for internal coherence — it’s much harder to lie than to tell the truth
    d. Pay special attention to predictions
    e. Polygraph
    f. Problem: With little internal knowledge of terrorist organizations, testing is problematic
5. Step 5: Train
    a. Ideally done in a safehouse somewhere outside the agent’s home country
    b. Spy gear, e.g.:

        i. Subminiature cameras
        ii. Concealment devices
        iii. Secret writing
        iv. Radio and computer devices
    c. Tradecraft, e.g.:
        i. Impersonal communication
        ii. Dead drop
        iii. Car toss
        iv. Signaling for clandestine meeting
    d. Surveillance detection
    e. Escape and evasion
    f. Problem: How does a member of a small terrorist cell find an excuse to go abroad for training without arousing suspicion?
6. Step 6: Handle
    a. Good agent can can run for years, even decades
    b. Even with the most sensitive agents, occasional personal meetings are important in maintaining psychological control
    c. Regular salary
    d. Psychological rewards are also important
        i. KGB made John Walker an admiral in the Soviet navy
        ii. CIA made Oleg Penkovsky a colonel in the U.S. army
    e. ‘Guarantee’ safety of the agent and family
    f. Psychology of control — agent must respond to direction
    g. Pass the agent to new case officer
    h. Problem: Risk of detection makes personal

meetings with terrorist agents difficult

7. Terminate
    a. All good things must come to an end
    b. Prime goal is to ensure the agent's espionage never becomes public
    c. Spies often have psychological or emotional problems, and this can complicate termination
    d. Termination bonuses, sometimes even retirement programs

c. New ways of doing espionage?
    i. Nature of Islamist terror networks (e.g., al Qa'ida) creates problems for classic, Cold War-style recruitment strategies
        1. But don't go overboard — classic recruitment still has its role against conventional, government targets
    ii. New ideas and fresh approaches are needed to deal with these new, difuse transnational threats, like al Qa'ida.
        1. More NOCs?
    iii. One possibility recently discussed is *natural capacity*
        1. The point of this natural capacity example is not to give a concrete example of what is going on, because in fact I do not believe this particular approach is actually being used. Rather, this example is intended to illustrate the type of thinking that goes into inventing new approaches to HUMINT collection.
        2. For a fuller treatment of natural capacity, see my "What's Wrong with American Spies?" on the Optional Readings section of the class website
    iv. Natural Capacity
        1. Example requirement: What's going on at specific airport in the Middle East?
            a. Who's coming and going, on and off the

record? What's in the hangers and warehouses? What are the finances? Political connections and loyalties? Access to planes on the ground? Flight plans?

2. Create a genuine, private sector venture at airport
3. Not traditional 'front' company
4. Enterprise would grow, morph, adopt, and generally ensconce itself within the airport
5. Over time, the company's business would become *co-extensive* (more or less) with what policy makers want to know about the airport
6. Historical parallel might be Armand Hammer's business dealings with USSR, including his personal relationship with Lenin in 1920s

v. Possible real-world applications for Natural Capacity
   1. Mining company looking for mineral deposits in Afghanistan
      a. Could get close to al Qa'ida training camps
      b. Operational climate, personalities, and physical infrastructure
   2. NGO providing mobile hospital services in Philippines
      a. Access to terrorist camps on remote islands
   3. World of Islamic charities provides endless possibilities
   4. Advantages over traditional espionage operations
      a. No penetration or recruitment
      b. Because company's employees (aside from a few senior managers) are not involved in anything covert, old notion of cover does not apply
      c. Other than normal issues of proprietary

information common in any company, the only secret would be the CIA connection at the very top, so counterintelligence problem is simplified

5. Natural capacity has disadvantages, too, but the point is to think about radically new approaches

d. The Iron Law of Espionage

i. The more secure an operation is, the less efficient it is. Because espionage operations need rigorous security, they are always inefficient — they take a lot of time, energy, and money.

4. Week 4 (26 September 2006)

a. Discussion of a specific recruitment case from *A Spy for All Seasons* by Duane Clarridge, chapter 8 “The Long Pursuit”

b. The Problem of Source Protection

i. If the opposition learns about an intelligence source, the source will be neutralized

1. Technical intelligence

a. Cell phone use discontinued, codes switched, activity camouflaged, disinformation spread

2. HUMINT

a. Arrest or murder

b. Doubled

c. Other sources become more difficult to recruit

3. Intelligence from foreign liaison

a. Liaison service more reluctant to share in the future

ii. Source description: A statement at the beginning of an intelligence report to let the reader know something about the source of the intelligence

1. Gives the consumer a general idea of the source, without revealing source’s identity

a. Statement of access
b. Statement of reliability

2. Can be a “notional” description if the source is especially sensitive, though this is rare

iii. After t he source description comes the body (or main content) of the intelligence report

1. Intelligence information from the source, with no slant or editorializing
2. Clarification, background, and even opinion may be added, but it must be clearly marked as not coming from the source

iv. Source protection is more than simply a good source description

1. Content of an intelligence report can also be revealing, especially if only a few people have access to the information
    a. Difficult to tell whether content is source-revealing just by reading the report
    b. E.g., “The Prime Minister had a headache on 24 February” does not seem like a sensitive state secret — but what if the only people he told were his wife and his doctor?

c. Sharing intelligence with law enforcement

i. Trust and a good relationship is part of it, but not the main part

ii. From an intelligence perspective, the problem with sharing intel with the police is not that law enforcement officers will tell someone about it, but that they will ***do*** something with it, something visible to the enemy

1. The concern of the intelligence officer is ***not*** that law enforcement is irresponsible or cannot be trusted

iii. The concern is about the action-oriented nature of law enforcement itself
iv. Action with visible consequences is key

d. Source protection done badly: Example
   i. Aldrich Ames passed intelligence to KGB on American agents in the USSR
   ii. Acting in police capacity, Soviet government arrested the agents and executed them
   iii. This *action* was one of the clues that tipped us off about Ames

e. Source protection done well: JFK and Penkovsky
   i. Oleg Penkovsky
      1. Soviet GRU officer
      2. British/U.S. spy
      3. Between Apr 61 and Aug 62, he passed more than 5,000 photographs of classified Soviet military, political, and economic documents
   ii. John F. Kennedy
      1. In Cuban missile crisis of Oct 62, Kennedy knew (from Penkovsky intel) Soviets were weaker than advertised
      2. Kennedy *did* nothing with the intel, but the knowledge it gave him was crucial in his confrontation with Soviet Premier Nikita S. Khrushchev
   iii. From perspective of intelligence professionals, Kennedy's subtle use of intel is a paradigm case
   iv. Fate of Penkovsky
      1. Arrested by Soviets on 22 Oct 62, shot for treason on 16 May 63
      2. Reasons unclear — may have been betrayed, or possibly sloppy tradecraft

f. Source protection and unintended consequences: VENONA case study
    i. Successful source protection has its own problems — it's not free and sometimes the price paid for effective source protection is quite high
    ii. VENONA was a highly classified COMINT program against Soviet cable traffic between Moscow, Washington, and New York
        1. Active from 1939 thru late 1940s
    iii. Revealed massive Soviet espionage network inside the United States
    iv. Existence of VENONA was disclosed in 1995, when VENONA archives were opened to scholars
    v. A tiny number of U.S. policy makers had access to the VENONA intercepts
    vi. What did VENONA reveal or confirm?
        1. Soviets had at least 349 spies in the U.S., many in sensitive government positions
        2. Almost 200 remain unidentified to this day, know only by their Soviet code names
        3. Penetration of the Manhattan Project, which developed the atomic bomb
        4. Lauchlin Currie
            a. Administrative assistant to President Franklin Roosevelt
            b. Soviet sympathizer
            c. KGB source
        5. Harry Dexter White
            a. Ass't Treasury Secretary in Roosevelt administration
            b. Passed information to KGB, plus advice on

how to frustrate US foreign policy

c. Used his position to promote more than a dozen KGB sources in federal gov't

6. Alger Hiss
    a. Senior American diplomat, State Department official
    b. Attend Yalta Conference (1945), advisor to Roosevelt
    c. Temporary UN Sec Gen
    d. KGB agent
7. Laurence Duggan
    a. American diplomat
    b. Respected member of Washington establishment
    c. Chief of State Dept's Division of American Republics (1935-44)
    d. Friend and foreign policy advisor to Vice President Henry Wallace
    e. KGB agent
8. Communist Party USA under complete control of USSR
9. Although tightly held, VENONA affected USG's domestic anti-communist policies in late 1940s, 1950s, and beyond
    a. Supposed anti-communist 'paranoia' looks different in light of VENONA
    b. "What if the American government had disclosed the Communist conspiracy when it first learned of it? [That might have] informed the legitimately patriotic American left that there was, indeed, a problem that the Federal

Bureau of Investigation, for example, was legitimately trying to address. But this did not happen. Ignorant armies clashed by night." — Senator Daniel Patrick Moynihan (D-NY)

c. "…the success of government secrecy in this case [i.e., VENONA] has seriously distorted our understanding of post-World War II history. Hundreds of books and thousands of essays on McCarthyism, the federal loyalty security program, Soviet espionage, American communism, and the early Cold War have perpetuated many myths that have given Americans a warped view of the nation's history in the 1930s, 1940s, and 1950s. The information these messages reveal substantially revises the basis for understanding the early history of the Cold War and of America's concern with Soviet espionage and Communist subversion." — Haynes and Klehr, *VENONA*, p. 18

10. For a defense of keeping VENONA a secret, see my article "The Case Against Intelligence Openness" in the Optional Readings section

Syllabus Section 2 — Counterintelligence

5. Week 5 (3 October 2006)
    a. What is Counterintelligence?
        i. Internal counterintelligence (also called "defensive" counterintelligence)
            1. Catching spies inside one's own organization or, more broadly, in one's own government
            2. Often responsibility of the Security department

3. Strong law enforcement overlap

ii. External counterintelligence (also called “offensive” counterintelligence, or clandestine warfare)
    1. Direct attacks on opposition intelligence services
    2. Purview of a professional intelligence service, e.g., CIA
    3. Penetration, double-agent operations, deception
    4. Also know as *counterespionage*

iii. A strong external CI program greatly enhances internal CI
    1. If you can penetrate the opposition intelligence service (external CI) and find out who its spies are, you can arrest them (internal CI)

iv. Counterterrorism’s connection to CI
    1. Counterterrorism is very close to counterintelligence
    2. Methods are almost identical
    3. Difference is mainly in goals — CI aims at protecting your secrets from theft, and CT aims at protecting your people and assets from death and destruction

b. Detail on Internal CI: Security
    i. Detect and deter penetrations by outsiders
        1. Espionage, simple theft, vandalism, violence, sabotage
    ii. Most organizations, whether gov’t or private sector, have their own security departments
        1. Physical security (locks, fences, cameras)
        2. Personnel security (background checks, badging)
        3. Information Technology security (network security, proper operating system installations, logon password regimes, audit trails)
    iii. Like law enforcement, internal CI deters, prevents, detects and solves “crimes” — i.e., infractions of rules, attacks on

the system, violations of espionage statutes

iv. Law enforcement and intelligence services
    1. Intelligence officers operating abroad spend much of their time avoiding the local police
    2. Even when working on the same side, relationship between law enforcement and intelligence officers is complicated by their two very different cultures
        a. This is one reason for the suggestion that U.S. should create its own separate domestic intelligence organization (the British MI-5 model), rather than giving domestic intelligence to the FBI
    3. Some general differences between law enforcement and intelligence
        a. Evidence gathering vs intelligence collection
        b. Reactive vs proactive
        c. Known vs unknown
        d. Police cases vs intelligence requirements
        e. Specifics vs open-ended generalities
        f. Action (solving crimes, making arrests, recovering stolen goods) vs knowledge expansion
        g. Information to be released in court vs perpetual secrecy
        h. Many legal rules vs few legal rules
    4. But in war on terror, distinctions are not always so sharp
        a. Intelligence needs to much more ‘actionable’
        b. Law enforcement must pay more attention to broad (and sometimes seeming impractical) understanding of foreign groups, cultures,

motivations

c. External CI: Counterespionage
    i. Don't wait for the opposition to come to you — you take the war to the opposition
    ii. Recruit agents inside the opposition intelligence service (or other targeted clandestine organization, e.g., terrorist group)
    iii. Recruited agents within opposition intelligence services are called *moles*
        1. Also called *penetrations*, or simply *agents*
    iv. Aggressive external CI (counterespionage) is critical for a successful overall CI program
    v. Properly placed CI agents in opposition intelligence service can provide:
        1. Identities of opposition agents within your own intelligence service or other friendly institutions
            a. Helps answer the question, "Are we penetrated?"
            b. Aldrich Ames example
        2. Plans and operations of enemy intelligence
        3. Playback on your own disinformation efforts
    vi. Nothing simple about this — the "wilderness of mirrors"
    vii. How do you know your CI agent is genuine, and not controlled by the opposition service?
d. Coordinating internal and external CI
    i. Ideally, internal and external CI efforts are coordinated
        1. Within intelligence services (where the CI naturally function resides), the two normally are coordinated
        2. Between intelligence services and other gov't agencies, the coordination is weaker
        3. With the private sector, coordination between internal corporate security and the national intelligence

service is typically nonexistent, at least in the U.S.

ii. Mutual support
    1. External CI can provide key information to internal CI, leading to the discovery (and neutralization) of enemy penetrations
    2. Internal CI can provide clues, leads, and sometimes double agent candidates to external CI

e. Case Study: The Trust (aka Monarchist Association of Central Russia)
    i. Founded just after the Bolsheviks (i.e., communists) took power in Russia
    ii. Started to fully operate against Western intelligence services in 1921
    iii. Brilliant deception operation
        1. Deceiving the opposition intelligence services is a key component of external CI (i.e., clandestine warfare)
    iv. Western intelligence services (British, French) were led to believe the Trust was a secret anti-communist organization operating inside the newly-founded Soviet Union, but it was really a deception operation created by Feliks Dzierzhinski, the head of Soviet intelligence
    v. The Trust was able to trick the Western intelligence services into providing millions of dollars in hard currency and gold to the fledgling Soviet government, all the while believing they were aiding a secret anti-communist conspiracy
    vi. By the late 1920s, Western intelligence had begun to believe something was not right with the Trust and suspected it was a Soviet counterintelligence operation
    vii. The Trust finally ended in 1929, when a top Trust official “defected” in Finland and told Western intelligence that the whole thing was a counterintelligence (deception) operation

1. In an interesting twist, this “defector” later returned to the Soviet Union and lived out his live there in comfort — his revelation of the Trust was evidently itself part of plan
    a. The Soviets, knowing the West was catching on anyway, apparently decided that a clear revelation to Western intelligence would be of some advantage — maybe as a way of trying to intimidate the West with Soviet espionage prowess

6. Week 6 (10 October 2006) — Notes from guest lecturer Randy Leben of FBI Foreign Counterintelligence
    a. I’d like to start with a question: What is the oldest organized intelligence service continuing almost without interruption to the present day?
        i. Keep in mind that “spying” is the world’s second oldest profession, indeed from Old Testament Biblical times. Also keep in mind some of the issues inherent for any society and its intelligence service.
        ii. The OPRICHNINA was created in February 1565 by Ivan Grozniy or Ivan the Terrible as his political police.
        iii. “Oprichnina” comes from the Russian word for “apart” or “beside” in that it would be directed entirely at the Tsar’s own discretion over those territories he administered directly.
        iv. For effect, these OPRICHNIKI dressed in black and rode black horses. The Oprichnina was comprised initially of about a thousand, but grew to six thousand before “official dissolution” seven years later in 1572.
        v. Over the next four centuries, the Russian security service evolved into the Preobrazhenskiy Prikaz under Peter the Great at the end of the 17th Century and eventually into the

so called “Third Section” under Tsar Nikolas I in the first half of the 19th Century.

vi. When Europe was in collective upheaval with political dissent and revolution peaking in 1848, arguably the marker date for the demise of monarchies, the Third Section was patting itself on the back .

vii. With additional reorganization in the later half of the 19th Century, various Russian intelligence functions came collectively to be called the OKHRANA.

viii. At this time nascent European services operated with oversight and within the law. The Okhrana continued as a law unto itself.

ix. With the Russian Revolution came the CHEKA (“ChK” for Extraordinary Committee). Through several permutations it became the NKVD, MGD, MVD and (in March 1954) the KGB

b. If I may go for a G E S T A L T

i. Why are there intelligence agencies ?

ii. What is the ultimate goal of any intelligence service?

iii. Brief conceptual survey of HUMINT and the technical collection INTs, i.e., SIGINT (Signals Intelligence); ELINT (Electronic; IMINT (Imagery Intelligence); and MISUR (Microphone Surveillance)

iv. Information assurance & perception management

v. Active measures & disinformation (Bhopal, India)

vi. Any technical means of collection provides a current picture from which we analytically project progress or likely outcomes

vii. But, which effort ultimately gives you future intent and the reasons? Answer: HUMINT

c. Brief history of the US Intelligence Community

i. US Secret Service, 19th Century
ii. FBI, founded in 1908 and matured in the 1930s and ‘40s
iii. Office of Strategic Services (OSS), World War II
iv. CIA, 1947 by act of Congress
v. NSA, Nov 1952 by Executive Order
vi. Department of Defense — it just grows
vii. Conducting traditional HUMINT assessment
    1. After assessment, the approach — formal, smile campaign, target of opportunity, walk-ins, dangles, double agents
    2. Finite resources
    3. Imperfect operational environment, including internal bureaucratic imperatives
    4. Weakness to be exploited

d. Collection needs vary by country — What is any particular country’s vital interest?
    i. For a CI perspective, we need to put ourselves in their shoes and ask what do they need or want. But also we need to ask what are their:
        1. Perceptions & Blind spots
        2. Cultural biases and historical imperatives
e. The 1980s and the post-Soviet evolution of the Russian Intelligence Service
    i. In 1986, despite the West’s love affair with Gorbachev, Reagan and Thatcher had to expel Soviet intelligence officers
    ii. The US itself passed the ECONOMIC ESPIONAGE ACT OF 1996
    iii. KGB after the post-Soviet reduction-in-force: leaner and meaner SVR and FSB w/FAPSI (16th) out and back
    iv. GRU is Russian military intelligence, with a difference in

corporate culture from the old KGB and the new SVR

1. GRU recruits its officers from the ‘hinterlands’
2. Less political and more patriotic toward *Mat’ Rossiya* (Mother Russia)

7. Week 7 (17 October 2006)
    a. Discussion of first 10 chapters of Spy: The Inside Story of How the FBI’s Robert Hanssen Betrayed America
    b. Review for next week’s midterm
8. Week 8 (24 October 2006)
    a. Midterm