THE INTEGRATION OF HOMELAND SECURITY AND LAW ENFORCEMENT

"They're a law enforcement agency. They're not in the business of fighting terrorism." (John Edwards)

This lecture directs attention to the challenges of integrating homeland security and law enforcement, especially as those challenges involve redefinition of the police role to encompass more effective surveillance and intelligence functions, but also as to how community policing can synthesize or permeate homeland security efforts. Many people (IACP 2002; Stephens and Hartmann 2002) believe community policing will evolve into intelligence-led policing. Changes in policing are not the sole concern, however. Daily life inside a more hardened security environment will change, and may be of immense concern. The police may have a role to play in helping citizens "feel" safer, and this may call for nothing less than community policing-like initiatives. Police are also trained, unlike the military and other institutions in society, to protect Americans' rights to privacy and due process. Civil libertarians would note that police abuses have a long history and that we should be cautious about any interplay or "integration" of policing, the military (i.e., NORTHCOM, posse comitatus issues, etc.), and federal security interests (i.e., DHS, Intelligence Community, etc.) Concerns exist over many things -- whether airport security measures are "too much" or too little; whether police ought to be using intelligence-oriented software and accessing classified surveillance data; whether "profiling" can ever be a legitimate tool; whether the PATRIOT Act gives government too many powers; and whether military assistance to law enforcement can be done without violating Posse Comitatus (an 1878 law prohibiting the military from being used to execute criminal law).

The federal government defines homeland security as: "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (Bush 2003). The key part of this definition is "concerted national effort" which means that it is not solely a federal effort, but based on the principle of partnership between governments, the private sector, and the American people. That partner known as law enforcement has always served a first responder role, and it even has some experience at counter-subversive and anti-terrorist (domestic) activities, but today's challenge involves taking on enemies (modern international terrorists) who fight in asymmetric ways that mock constitutional safeguards which balance criminal rights with police powers. Law enforcement has also always been a small-town,
decentralized phenomena in American society, and without new models, theories, and laws, it may not be up to the task of collecting, sharing, coordinating, and analyzing the intelligence necessary to successfully assess and respond to modern-day threats.

It may be time for a revolution in police affairs, much like the revolution in military affairs toward special, light brigades that are jointly coordinated in real-time. It is definitely the time to reconsider the police role in society, and to what extent police involvement in national defense and domestic security carries a risk of encroachment on civil liberties. We shall begin with an overview of three ways to approach domestic security, and discuss the implications for law enforcement throughout.

THE SUPER-AGENCY APPROACH TO DOMESTIC SECURITY

The idea of some sort of super-agency that tracks the ideological (American and un-American) commitments of its citizens has been around for a long time. It has been implemented in many nations with concerns about internal, or state security. It is implicit in most proposals to federalize, centralize, or consolidate police forces. It is explicit in most proposals to reorganize the intelligence community, such as the 1970 Huston Plan (named after White House staffer Tom Charles Huston) which advocated combining the CIA, FBI, NSA, and DIA. While far from creating a domestic intelligence super-agency (like MI5 in Britain), the creation of the Department of Homeland Security (DHS) is a significant transformation of U.S. government. Formed in the aftermath of terrorist attacks on September 11th, 2001, the new department's first priority became protection of the nation against further terrorist attacks, followed by additional duties for intelligence and threat analysis, guardianship of borders and airports, protection of critical infrastructure, and emergency response coordination. Along with the Coast Guard and Secret Service, twenty-two (22) separate agencies were consolidated into the DHS, and housed in one of four major directorates: Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Analysis and Infrastructure Protection, as follows:

1. **Border and Transportation Security directorate:** U.S. Customs Service (Treasury); Immigration and Naturalization Service (Justice); Federal Protective Service (GSA); Transportation Security Administration (Transportation); Federal Law Enforcement Training Center (Treasury); Animal and Plant Health Inspection Service (Agriculture); Office for Domestic Preparedness (Justice)
2. Emergency Preparedness and Response directorate: Federal Emergency Management Agency (FEMA); Strategic National Stockpile and the National Disaster Medical System (HHS); Nuclear Incident Response Team (Energy); Domestic Emergency Support Teams (Justice); National Domestic Preparedness Office (FBI)

3. Science and Technology directorate: CBRN Countermeasures Programs (Energy); Environmental Measurements Laboratory (Energy); National BW Defense Analysis Center (Defense); Plum Island Animal Disease Center (Agriculture)

4. Information Analysis and Infrastructure Protection directorate: Critical Infrastructure Assurance Office (Commerce); Federal Computer Incident Response Center (GSA); National Communications System (Defense); National Infrastructure Protection Center (FBI); Energy Security and Assurance Program (Energy)

The most frequent criticism of DHS is not that it's too big (America has had similar super-agencies such as LEAA, the Law Enforcement Assistance Administration, established under the 1968 Crime Control and Safe Streets Act and dismantled in 1980 with NCJRS remaining as a remnant), but that it's too small, and doesn't include two agencies, CIA and FBI, which seem like logical choices for inclusion in DHS due to their poor record of power and information sharing. Apparently, the CIA and FBI are already overwhelmed by a sea of information, and DHS is to go about using new and different intelligence to uncover threats. As the National Strategy for Homeland Security (2003) makes clear, existing agencies like the CIA and FBI are to enhance their analytic capabilities, and new agencies like the DHS are to build new capabilities. Some of those new capabilities the DHS is tasked to develop include the following:

- "smart borders" that no longer rely on two oceans and friendly neighbors; change the way we look at travel and immigration
- guard against "inside" threats to critical infrastructure and key assets; build a complete list of those assets and involve the private sector which controls or owns 85% of the infrastructure
- secure cyberspace; not only as a vehicle for terrorist attack, but something along the lines of an Open Secrets Act which other nations have that prevents open-source Internet information from being useful to terrorists
- "red team" and dual-use analysis; thinking like a terrorist or how something good could be used for evil; staging drills and simulations of worst-case scenarios
- harness scientific knowledge and expertise on countering the proliferation and use of deadly weapons, such as chemical,
biological, radiological, and nuclear; develop broad spectrum vaccines and antidotes; rapidly produce prototypes

- streamline information sharing among intelligence and law enforcement agencies; connect databases; expand extradition authority; reconsider posse comitatus restrictions on the use of military assistance in domestic security; review obligations to treaties and laws
- promote homeland security research; use 21st-century science and technology; built new capabilities to secure the homeland

The most important function of DHS will deal with domestic counterterrorism, an idea that encompasses the notion of an informed and proactive citizenry (informed via new Alertness and Awareness systems) who see something unusual and report it to the appropriate authorities. This is very similar to the voluntary cooperation that police need from citizens for crime reporting, or by another stretch of the imagination, to the idea of community policing. It begs the question, however, of how far law enforcement ought to go with investigating suspicious, non-criminal activity. Clearly, the purpose is to identify, halt, and where appropriate, prosecute terrorists as well as those who provide them logistic support. It primarily involves a tracking mission for law enforcement, and only secondarily a prosecutorial mission, or bringing terrorists to justice. It is, in short, what Jonathan White (2004) calls the "Eyes and Ears" approach to the role of police in intelligence gathering. It is a system of detecting hostile intent. A number of initiatives have been designed to promote individual citizen involvement, such as the following:

- **Citizen Corps** - volunteers who participate in community-level homeland security efforts
- **Volunteers in Police Service** (VIPS) - civilian police who perform non-sworn functions of policing
- **Medical Reserve Corps** - retired healthcare providers who augment disaster responses
- Operation TIPS (Terrorist Information and Prevention System) - [now-defunct program](http://faculty.ncwc.edu/TOConnor/427/427lect05.htm) for reporting of suspicious activities
- **Community Emergency Response Teams** (CERT) - training programs in local communities
- **Neighborhood Watch** - incorporation of terrorism prevention into its mission via local sheriffs
- **Infragard** - private sector and academic partnering for cyberspace security
- **National Identification Card schemes** - [now-defunct idea](http://faculty.ncwc.edu/TOConnor/427/427lect05.htm) of
high-tech, biometric ID cards

The most frequent criticism of initiatives like the above (especially Operation Tips) is that they smack of police state measures, reminiscent of Nazi Germany, Stalinist Russia, or America's own sorry experience with COINTELPRO ("counterintelligence program") of the 1960s that collected files on some 62,000 suspicious Americans. The magazine, *Mother Jones*, has a good retrospective piece on the furor over Operation Tips, if you are interested, and *EPIC* has a chronology of the National ID Card movement which basically dissolved into a crackdown on driver's licenses. The central dilemma remains of how to incorporate citizen reporting of suspicions behavior into a system of intelligence and law enforcement. Without guidelines, laws, constitutional safeguards, and perhaps training of civilians (Hillyard 2003), the citizen role in domestic counterterrorism may be doomed to defeat on fears that it is dangerous domestic spying.

Whole books have been written about Operation CHAOS and COINTELPRO (Donner 1980) during the Hoover period (1939-1971) when the FBI was a domestic intelligence agency that tracked "subversives" regarded as future threats to the undermining of government. The bureau perfected the theory and practice of counter-subversion, providing policymakers with intelligence on persons, organizations, and places where political agitation or unrest existed, or at least the gossip of such behavior existed. After a "vetting" process (a term for validating the truthfulness of information) of 90 days, in which informant tips were collaborated by record searches, mail opening, surveillance, and pretext contacts, agents frequently took proactive measures, such as raids, break-ins, detention without right to counsel, and blackmail. Liaisons were made with Military Intelligence, and the FBI established an international presence, but used MI domestically as well (the "greening" of intelligence), even after 1961 when National Guard intelligence functions were deactivated. College campuses, and their surveillance and infiltration, were a favorite target, with Hoover going after criminal justice departments in particular. Hoover distinguished general (strategic) files from intelligence (line) files, the former being kept secret in field offices until destruction orders were given, and of course, Hoover destroyed most of his own files before he left. Such was the domestic spy network set up under Operation CHAOS, which Hoover regarded as penetrative intelligence. Under COINTELPRO, the goal was disruption, or what Hoover called aggressive intelligence, which involved planting lies and deceptions into subversive organizations, putting a "snitch jacket" on someone (leaking that they were an FBI informer), spreading false rumors, getting people evicted, promoting marital discord, and other dirty tricks bordering on the unimaginable, often borrowed from the CIA. Hoover made regular use of his contacts in the IRS.
and ATF (then part of IRS but later moved to Treasury in 1972) to trigger tax audits on groups and individuals, as well as to spy on what books they were checking out of libraries. The private sector was enlisted to help the bureau in a number of ways, via recruitment of security firms like Pinkerton and Wackenhut, the local Chamber of Commerce, vigilante and militia groups, the John Birch Society, and even clergymen (Methodists in particular).

THE LEGAL REFORM APPROACH TO DOMESTIC SECURITY

Some history on the post-Hoover era and Watergate is in order first. In 1967, a Supreme Court decision (the Katz case) condemned warrantless electronic surveillance, and the following year, the Omnibus Crime Control and Safe Streets Act established probable cause as the standard for obtaining a wiretap against U.S. citizens. A 1969 case (the Alderman case) ruled that the methods and transcripts of a wiretap should be open in court for public and adversarial scrutiny. This jeopardized exposure of ongoing intelligence operations, so Attorney General Mitchell established the "Mitchell Doctrine" as it came to be called, which insisted that the President, acting through the Attorney General, had the inherent constitutional power to authorize warrantless, secret surveillance in the name of national security or for purposes of pure or preventive intelligence. A number of court cases followed, all along the lines of the judiciary warning the executive branch of government to avoid using foreign intelligence techniques in domestic cases. In 1972, the Court (in the Keith case) disposed of the Mitchell doctrine, and in the 1973 acquittal of Daniel Ellsberg (who released the Pentagon Papers to the press), the President was determined not to be immune from civil liability for authorizing an illegal wiretap. Watergate, which is closely connected to the Ellsberg case, but technically refers to a 1972-1974 period most remembered for a break-in and bugging of Democratic Party headquarters, signaled an end to abuses in the name of national security along with claims of executive immunity. In 1974, Congress passed the Privacy Act which forbade any federal agency from collecting information about the political and religious beliefs of individuals unless in connection with a bona fide criminal investigation, and in 1975, the Freedom of Information Act, allowed individual access to any personal information which might be secret in the name of national security, and applied it to the FBI. The final separation of domestic and foreign intelligence came in 1978 with the Foreign Intelligence Surveillance Act (FISA), which brings us up to amendments in FISA and the Patriot Act of 2001, foundations for modern-day legal approaches to domestic security.
The U.S.A. PATRIOT Act of 2001 can be seen as another amendment to FISA because under the latter, agencies don't need probable cause to gather intelligence if their targets are operating as agents of foreign powers, and modern (sub-national) terrorists don't usually work for a foreign power, but for some nebulous cause. Specifically, the Patriot Act enhances roving surveillance authority and streamlines wiretap authorizations, sets up anti-terrorism asset forfeiture procedures, approves detention of suspected terrorists, removes obstacles to investigating terrorism, increases the penalties for terrorist crimes, removes any statute of limitations, encourages federal involvement in domestic preparedness exercises, and supports activities by the Department of Homeland Security. More significantly, Title I (Intelligence Gathering) of the Patriot Act permits disclosure of foreign intelligence information to any domestic or law enforcement intelligence operation. It permits foreign intelligence techniques to be used for criminal justice purposes, and it maintains the secrecy of the intelligence apparatus (the Mitchell Doctrine) as well.

The Patriot Act replaces probable cause with a showing of need for an ongoing terrorism investigation, and goes a step further by placing a gag order on the person served with the warrant. They cannot notify the real target of the investigation, or in any way disclose what information law enforcement was seeking. It amends the Family Educational Rights and Privacy Act, and forces school officials to release information, as well as allows law enforcement officials to obtain information on use of library resources, books, and Internet usage. Again, school officials are prohibited from disclosing what law enforcement was looking for. Some experts think the Patriot Act was rushed too quickly through Congress, and violates the Fourth Amendment as well as the Balance of Powers principle in the Constitution. When the Department of Justice announced it would eavesdrop on attorney-client conversations with suspected terrorists, many experts thought that crossed the line of reasonableness.

The basic dilemma, as White (2004) points out, is a legal dilemma. Law enforcement has for years been accustomed to working within legal constraints, collecting evidence that can be used for prosecution in a criminal court. There is a natural terminus to a criminal investigation. The intelligence community has for years been accustomed to working with few legal constraints, and there is no natural terminus, or end, to an intelligence investigation. Criminal intelligence is governed by constitutional rules of evidence; national security intelligence is not. Going to trial in a terrorism investigation often means exposing the intelligence sources for the sake of a criminal conviction. This irony, as
well as other twists having to do with military tribunals, has produced some rather strange effects in the war on terrorism -- American citizens being detained like prisoners of war and foreigners being treated like citizens in criminal courts. To be sure, terrorist groups (according to al Qaeda's training manual) instruct their captured agents to make a mockery of justice systems - to insist they were tortured or mistreated, to learn the names of their captors and lie about them, and to use religion at every turn to their advantage. Nonetheless, this is not sufficient reason to proceed in a constitutional vacuum, or make up the rules as you go along. There are other factors that dampen the prospects for successful use of law enforcement for intelligence purposes, and here is a standard list of the limitations on using police that White (2004) implies may present problems:

- Police do not have the academic credentials or higher order critical thinking skills to understand the root causes of terrorism, its complexities, or the ability to distinguish between terrorist sympathizers and criminal terrorists
- Police are trained in reasonable suspicion and probable cause to make stops, ask questions, detain, infiltrate, and collect information, but intelligence work requires neither standard in the ongoing collection of vast amounts of non-criminal information
- Police agencies are fiercely autonomous, competitive, turf-conscious, mistrustful, and attuned to local politics with little or no interest in thinking outside their jurisdiction and/or partnering with non-police agencies seen as outsiders
- Police agencies are focused on publicity and getting the word out about their effectiveness at crime-fighting while intelligence work is focused on secrecy and never letting intelligence successes be known
- Police are taught that criminal justice record keeping should be clear and concise, with writing crisp and to the point, while there is no such thing as too much excess or irrelevant information for intelligence work
- Police organizations are bureaucracies where power struggles and personal rivalries abound, combined with a stifling tendency toward stagnation and lack of creativity whereas intelligence work rewards eccentricity and creativity
- Police are prone to negative stereotyping and abuse of power, and any intelligence shared with them may be misused
- Police are prone to leaks and the leaking of information may occur, tipping the terrorists off about an ongoing operation
- Police often act officiously and rudely when enforcing security
precautions on ordinary citizens, creating a sense of insecurity and giving the public the impression of a police state

- Police are not psychologically equipped to deal with the kind of massive casualties that weapons of mass destruction can cause
- Police are not prepared to face a terrorist enemy who uses criminal means to obtain military objectives

THE COMPUTER DATABASE APPROACH TO DOMESTIC SECURITY

The National Strategy for Homeland Security (2003) calls for connecting computer databases used in federal law enforcement, immigration, intelligence, public health surveillance, and emergency management, and further, DARPA's plan for Total Information Awareness (TIA) is to merge some of these interconnections into a data mining system of systems involving the private sector, the finance/credit system, and the Internet. Most of the databases involved would be government owned, where they are not so different from one another, and can probably be interconnected. Some, such as CDC's (Center for Disease Control) epidemiology program, continuously scan disease patterns throughout the nation's healthcare system for signs of an outbreak. Others, such as the Department of State's TIPOFF system compiles information on suspected terrorists collected by consular offices overseas, and is already interconnected. There's some rather large databases involved, two of the largest being those from Immigration (the Border Patrol uses a two-finger fingerprint system while the FBI uses a ten-finger fingerprint system) and the FBI (NCIC, or the National Crime Information Center, tracks everything greater than a Class C misdemeanor and is already overburdened by the size of graphics on some items). The following is a list of government databases related to homeland security:

- **AFIS** - Fingerprint system to identify citizens
- **CCD** - Consolidated Consular Database; records of non-immigrant visa entries and exits
- **CLASS** - Consular Lookout and Support System; program for running background checks for visas
- **CODIS** - Combined DNA Index System used for solving crimes
- **IBIS** - Interagency Border Inspection System; immigration program used at ports of entry
- **IDENT** - Fingerprint system to identify aliens
- **JITF-CT** - Joint Intelligence Task Force Combating Terrorism; DIA database
- **LEO** - Law Enforcement Online; VPN with exclusive interactive briefings, alerts, and discussions
The problem with government databases is not with the federal government's integration of "watch lists," but with any integration at the state and local level of law enforcement. Real-time information sharing may take place among federal agencies, but it's not going to get to the larger law enforcement community in real-time. Some of this is due to federal bias or suspicion against local law enforcement, and another problem is that some state and municipal police departments are as far behind as five years in such basic things as updating parking ticket records. A greater problem arises when one tries to integrate, or commingle (the proper term), government databases with those in the private sector, such as credit card companies, e-commerce firms, retailers, etc. You would need about 15,000 fields just for merging the header (demographic) information across these databases, which would represent about 300,000 bytes per person. If you multiply this by 500 million people, the header records alone would require approximately 150,000,000,000,000 bytes (136 terabytes) and almost five years to stabilize. Then, there's the key identifier fields (also called crosswalk tables) which contain numerical records such as social security numbers or driver's license numbers which link the different databases together, and one of these has to be a unique identifier (pivot table) to put an
interface on it. Since terrorists are likely to use fake IDs, a new unique identifier system may have to be developed, and this will require about ten years of data input time. Then, the transaction data is brought in, which generally produces crashes and errors, generating the need for continual validation, de-duplication, and normalization. The computer database approach is doable, but it will take years to get it right, lots of improvements in technology, and something a whole lot faster than T1 Internet connections for law enforcement. Subcontracting vendors like InferX are already at work on distributed data mining solutions.

Secure intranets (on the .gov domain) and secure videoconferences will most likely remain the federal government's main way of information sharing with state and local governments, along with renaming the 93 Anti-Terrorist Task Forces (ATTFs) throughout the federal court districts into Homeland Security Task Forces (HSTFs). The ATTF/HSTF approach simply involves prosecutors, but Joint Terrorist Task Forces (JTTFs), which have a longer history, going back to Chicago in the late 1970s, are a different thing, and now exist in all 56 FBI field offices where some elite state and local police are picked to be temporarily federalized, and true, joint cooperation exists between the levels of government since the power of arrest is equalized. The FBI also has about 10 stand-alone JTTFs in its largest satellite offices, known as resident agencies.

A more promising approach to information sharing would build upon what few successes law enforcement has had with "vertical" integration - crossing federal, state, and local levels of government. Bodrero (2002) as well as White (2004) recommend using the six-region information network known as RISS (Regional Information Sharing Systems). The RISS network was designed for sharing criminal intelligence, primarily about gang crime, hate crime, and cybercrime, and would provide a model that works and makes effective use of existing intelligence analysts who work for police departments. RISS is the closest thing to a nationwide criminal investigation network.

Another idea is to build on the War on Drugs as an intelligence model, and NDIC (National Drug Intelligence Center) holds some promise for development because it has always involved excellent cooperation between levels of government. In addition, America has several identified High Intensity Drug Trafficking Areas (HIDTAs), the El Paso Intelligence Center (EPIC) being most notable, which represent excellent working models of how intelligence analysts, from both law enforcement and the military, can come together to work on a common problem.
In addition, there are numerous states with highly-developed criminal intelligence units, such as the New Jersey State Police Intelligence Services which has long had an effective intelligence gathering and analysis capability. Most state police intelligence units maintain liaisons with INTERPOL (International Criminal Police Organization), EUROPOL, the RISS network, FINCEN (Financial Crime Enforcement Network), IALEIA (International Association of Law Enforcement Analysts), and LEIU (Law Enforcement Intelligence Unit, another association that holds annual seminars). It makes little sense for the federal government to ignore these resources as they represent the "best and brightest" that local law enforcement has to offer.

HOMELAND SECURITY THREAT AND VULNERABILITY ANALYSIS

The type of intelligence that DHS hopes to produce is warning intelligence, the kind that eliminates surprise. This kind of intelligence is used by policymakers not so much to inform citizens via reverse-911 or other civil defense measures, but so that preemptive action can be taken against the would-be attackers. This is an intense form of intelligence that will primarily require informers and infiltrators (HUMINT, or human intelligence) crossing every known subcultural and foreign-language barrier. In the language of risk assessment, this type of intelligence is known as tactical threat analysis, and is sometimes called actionable or flash intelligence. It is the first priority of DHS, and it places the Secretary of DHS on the same footing as the DCI (Director of Central Intelligence) and Attorney General (or Director of FBI as proxy) in being able to order action such as strikes and raids on would-be attackers. It will require data collection and analysis systems that share information in real-time or near-real-time.

The second type of intelligence product sought by DHS is strategic analysis of the enemy, which is a deep, almost-academic understanding of motives, goals, identities, organizational structure, sources of support, capabilities, and points of vulnerability. It is optimistically aimed at the sources of terrorism - those seething hotbeds of extremism and fanaticism that typically characterize the world's trouble spots. At this level, also, the Secretary of DHS is on equal footing with the DCI and AG, but disagreements can be expected on the basis of human differences among interpretations of background information. Where DHS has a monopoly is with the area of vulnerability assessment - the constant measurement and monitoring of how vulnerable America's critical infrastructure is. This is the area that DHS hopes to automate with remote sensors and computer modeling, and it is also the area that is part of the Advisory system for warning the private sector and public.
However, the hardest task is going to be involving law enforcement in the intelligence work.

To integrate homeland security with law enforcement, much more training beyond SLATT (State and Local Anti-Terrorism Training) will be needed. Police will need to learn how to collect and analyze intelligence. Police will need to improve their profiling skills, and learn, for example, how to monitor their communities for sudden shifts and expansions in anti-American rhetoric. More bi-lingual and multi-lingual police will surely be needed. Police will have to read a lot of radical literature, and investigate every charity. They will have to infiltrate alienated groups that kill without the slightest compunction, and are often well-financed. They will have to infiltrate religious groups, and pick up on squabbles that go on within such organizations. Police will have to improve their ability at computer forensics, because terrorists often are fairly sophisticated at encryption and computer use. Police will have to become sensitive to trends and indicators in community tension, especially as these tensions are tied into international tensions. If new groups come to town, and keep to themselves, or try hard to blend in, either of these should arouse police suspicion. It will seem like an impossible job, but maybe with a few tweaks, police can do it. In any event, it should portend a new role for police in society - a role that involves America learning how to spy on itself.

THE RISE OF FUSION CENTERS

Fusion centers are the latest, greatest thing in homeland security. They do "fusion" intelligence, which involves joint or collaborative efforts between jurisdictions (in this case, federal and local law enforcement, and sometimes the private sector and/or other "tribes"). Fusion centers can (and do) exist internationally, where they have bigger problems. Theoretically, they are compatible with other notions in homeland security, like interoperability and unified command. Analytically, they are derivative from the process known as cross-cueing. Federal funding is available for states to create their own fusion centers (build them, but not staff them - grant money cannot be used to pay salaries), and it is hoped that by 2007, each state will have one. Many states (including Arizona, Colorado, Georgia, Illinois, Kansas, Maryland, Massachusetts, and New York) have developed fusion centers. They combine and analyze anti-terrorism information from multiple sources, and are intended to provide a better pipeline between federal officials and state and local officials.

It is likely that some state fusion centers will take on different shapes
and sizes, but in many cases they will look very similar to Emergency Operations Centers (EOCs) - see Lecture on Emergency Management - or they will look like "cube farms" where analysts are hired to sit and work while visitors are dazzled by the big screens which fill the walls. Information sharing should be independent of who staffs a center, anyway, as well as who the political leaders are. Networks of inter-governmental intelligence gathering and sharing operate in a less than ideal fashion sometimes because of the personalities involved. Strong personalities at the local level (for political reasons) typically want more detail than can be provided (for analytic or security reasons). Better information sharing is going to take much-needed realignment at the bottom as well as the top, such as by figuring out the role of governors and mayors and enhancing DHS's Office of Intelligence and Analysis.

INTERNET RESOURCES
ACLU Report on the Dangers of Domestic Spying
ACLU Report on How Patriot Act enables Law Enforcement to use Intelligence to Invade Privacy
Anser Institute for Homeland Security
Britain's MI5 Intelligence Agency (Home Office/MOD)
DARPA Information Awareness Office
Data Mining and Homeland Security Applications
Electronic Privacy Information Center Page on DARPA
Existing and Pending Anti-Terrorism Laws
FindLaw's Special Coverage on Civil and Criminal Terrorism Cases
GovExec Website on Homeland Security
House Select & Subcommittees on Homeland Security
Journal of Homeland Security
Law Enforcement Intelligence Guide
Texas A&M's Homeland Security Web Resources
The USA Patriot Act
Watergate Remembrance Page

PRINTED RESOURCES


Wadsworth.

Last Updated: 01/19/06
Syllabus for JUS 415 (Homeland Security)
Syllabus for JUS 427
MegaLinks in Criminal Justice