

Critical and Historical Issues of National and Homeland Security Affairs¹

Outline prepared and written by:

Dr. Jason J. Campbell:
<http://www.jasonjcampbell.org/blog.php>

Youtube Playlist Link:
http://www.youtube.com/view_playlist?p=8E9FC63E0F362F82

Alperen, Martin J. [Foundations of Homeland Security: Law and Policy](#). Edited by Ted E. Lewis, Wiley Series on Homeland Defense and Security. New Jersey: John Wiley, 2011.

§1:

The Vision of Homeland Security [HS]:

The United States, through a concerted national effort that galvanizes the strengths and capabilities of Federal, State, local, and Tribal governments; the private and non-profit sectors; and regions, communities, and individual citizens – along with our partners in the international community – will work to achieve a secure Homeland that sustains our way of life as a free, prosperous, and welcoming America.²

Strategic Approach to Homeland Security:

HS is 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”³

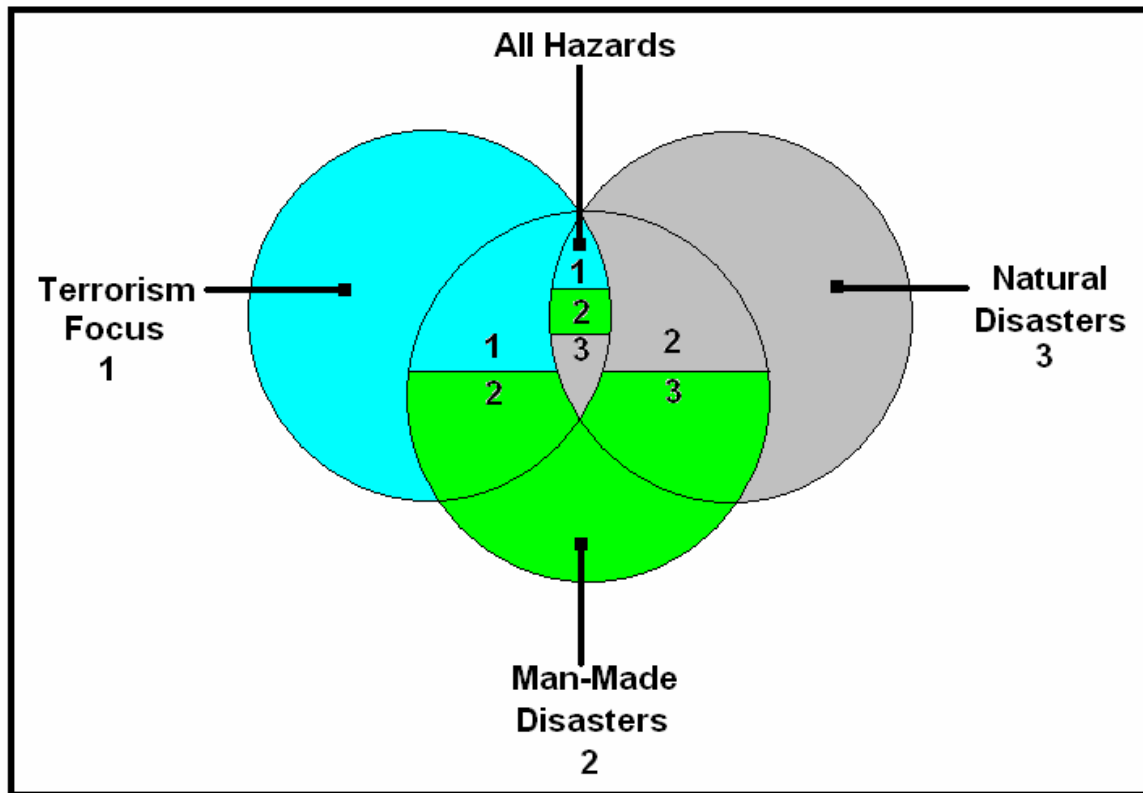
Practitioner Disagreements:

1. Terrorist focus:
 - a. “They believe that focusing on anything additional dilutes, distracts, and weakens the...mission.” (p. 1).
2. All hazards focus:
 - a. “Terrorism, man-made disasters, and natural disasters” (p. 2).

¹ President Obama has denied a distinction between homeland security and national security. “My highest priority is to keep the American people safe. I believe that Homeland Security is indistinguishable from National Security -- conceptually and functionally, they should be thought of together rather than separately. Instead of separating these issues, we must create an integrated, effective, and efficient approach to enhance the national security of the United States. The White House must be organized in ways that reflect this reality. [Reference HERE](#)

² http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf, g 13.

³ Ibid, pg. 3.



Hazard Term	Threats	Source	Temporal Impact	Societal Impact
Traditional “All-Hazards”	1	“External” What is one to us	Urgent	3
Emerging “Generational Hazards”	2	“Internal” What we do to ourselves	Belated	4

Figure Reference⁴

1. Major – Terrorism (nuclear, radiological, bio-agent, chemical, high explosives) or Natural (flooding, earthquakes, hurricanes); Other – Wildfires, hazardous materials, tornados/windstorms, winter storms, drought, social disturbances.
2. Major – Soaring federal fiscal and current accounts debts, global warming, inferior Mathematics /science/ engineering education, decaying physical infrastructure; Other – Mass privatization of government services, foreign energy dependence, demographic pressures of low birth-rates/aging population and mass immigration.
3. Deaths and/or physical injury, significant negative impacts to regional and/or national economy; social destabilization.
4. Significant negative impacts to national economy/living standards; social destabilization

⁴ Massey, Patrick J. “Generational Hazards.” *Homeland Security Affairs* III, no. 3 (September 2007): <http://www.hsaj.org/?download&mode=dl&h&w&drm=resources%2Fvolume3%2Fissue3%2Fpdfs%2F&f=3.3.3.pdf&altf=3.3.3.pdf>

Two Models of Emergency Management:⁵

1. Emergency Services Model:

a. “primarily concerned with the coordination of emergency services”

b. Interaction between E-S providers only.

i. Problem:

1. “This has the effect of isolating them further from the policy making functions of the jurisdiction.” p. 15.

2. Public Administration Model:

a. “emergency management is an element of the overall administration of government.”

b. Interaction between E-S providers and the broader network of emergency management.

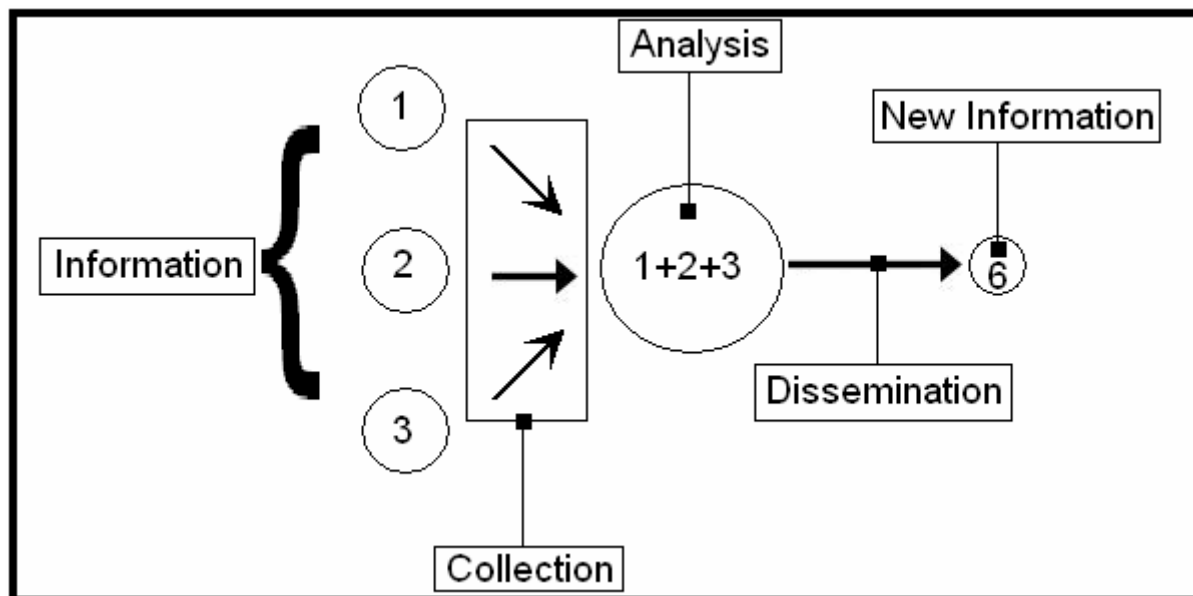
§2:

Intelligence Gathering

“The *Homeland Security Act of 2002* created DHS [The Department of Homeland Security] and intended the intelligence component of the department to be the focal point for all terrorism-related intelligence to protect the Nation”⁶

Three Phases of Intel: (1) Collection, (2) Analysis, (3) Dissemination

[C.A.D.]



⁵ Michael D. Selves: <http://training.fema.gov/emiweb/downloads/Local%20emergency%20management.doc>

⁶

http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBkQFjAA&url=http%3A%2F%2Fwww.dhs.gov%2F%2Fassets%2Fmgtmtrpts%2FOIG_07-49_Jun07.pdf&rct=j&q=collection%20analysis%20Dissemination%20intelligence%20site%3A.gov&ei=CJm5TbGnD4jqgQeLrr3oAg&usq=AFQjCNE06LaBa_hs-DU9qwRyK3EDgXOmMw&cad=rja

Application of C.A.D. Intelligence Model to the DHS Initiative: Intelligence Architecture:

3 Component Part of National Intelligence Architecture:

1. Federal Level/Government: [NSC, CIA, FBI, DOD ect]
2. Regional Clearing Houses:⁷

- i. **Joint Terrorism Task Force (JTTF):**

1. Divided into **56** “Divisions” or “Field Offices”.⁸
 2. “Conduct Investigations”⁹
 3. “The FBI has 56 field offices (also called divisions) centrally located in major metropolitan areas across the U.S. and Puerto Rico. They are the places where we carry out investigations, assess local and regional crime threats, and work closely with partners on cases and operations. Each field office is overseen by a special agent in charge, except our offices in Los Angeles, New York City, and Washington, D.C., which are headed by an assistant director in charge due to their large size. Within these field offices are a total of about 400 resident agencies located in smaller cities and towns. Resident agencies are managed by supervisory special agents.”¹⁰

- ii. **DHS Fusion Centers: (DHSFC):**

1. Divided into **72 National DHSFC**.¹¹
 2. “Analyze and share intelligence”¹²
 3. “*These centers analyze information and identify trends to share timely intelligence with federal, state, and local law enforcement including DHS, which then further shares this information with other members of the Intelligence Community. In turn, DHS provides relevant and appropriate threat information from the Intelligence Community back to the fusion centers. Today, there are 72 state- and locally-run fusion centers in operation across the nation, up from a handful in 2006. Our goal is to make every one of these fusion centers a center of analytic excellence that provides useful, actionable information about threats to law enforcement and first responders.*”¹³

3. Local Law Enforcement [LLE]/ **S**tate, **L**ocal, **T**ribal, and **T**erritorial (**SLTT**) Authorities.¹⁴

⁷ I had willfully not included the “Joint Regional Intelligence Center” and other regional Clearing Houses.

⁸ <http://www.fbi.gov/contact-us/field>

⁹ http://www.dhs.gov/files/programs/gc_1298911926746.shtm

¹⁰ Ibid

¹¹ <http://www.nfcausa.org/default.aspx/MenuItemID/117/MenuGroup/Map.htm>

¹² http://www.dhs.gov/files/programs/gc_1298911926746.shtm

¹³ <http://www.nfcausa.org/default.aspx/MenuItemID/131/MenuGroup/Home+New.htm>

¹⁴ <http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionIX.html>

Part II, Section 2.3 and 2.6 of Executive order 12333, United States Intelligence Activities States: [Collection Phase of C.A.D.]

“**2.3 Collection of Information** Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by [Part 1 of this Order](#). Those procedures shall permit collection, retention and dissemination of the following types of information:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
- (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;
- (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;
- (e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting;
- (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
- (g) Information arising out of a lawful personnel, physical or communications security investigation;
- (h) Information acquired by overhead reconnaissance not directed at specific United States persons;
- (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and
- (j) Information necessary for administrative purposes.

In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.”¹⁵

2.6 Assistance to Law Enforcement Authorities. “Agencies within the Intelligence Community are authorized to:

- (a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community;
- (b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
- (c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency; and
- (d) Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.”¹⁶

¹⁵ <http://www.archives.gov/federal-register/codification/executive-order/12333.html#2.3>

¹⁶ <http://www.archives.gov/federal-register/codification/executive-order/12333.html#2.6>

Title I, Section 102A(g-h) of the Intelligence Reform and Terrorism Prevention Act [IRTPA] of 2004 States: [**Analysis Phase** of C.A.D.]

(g) INTELLIGENCE INFORMATION SHARING.—(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

“(A) establish uniform security standards and procedures;

“(B) establish common information technology standards, protocols, and interfaces;

“(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

“(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

“(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and

“(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program.

(h) ANALYSIS.—To ensure the most accurate analysis of intelligence is derived from all sources to support national security needs, the Director of National Intelligence shall—

“(1) implement policies and procedures—

“(A) to encourage sound analytic methods and tradecraft throughout the elements of the intelligence community;

“(B) to ensure that analysis is based upon all sources available; and

“(C) to ensure that the elements of the intelligence community regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements;

“(2) ensure that resource allocation for intelligence analysis is appropriately proportional to resource allocation for intelligence collection systems and operations in order to maximize analysis of all collected data;

“(3) ensure that differences in analytic judgment are fully considered and brought to the attention of policymakers; and

“(4) ensure that sufficient relationships are established between intelligence collectors and analysts to facilitate greater understanding of the needs of analysts.”¹⁷

¹⁷ http://www.gpoaccess.gov/serialset/creports/pdf/108-796/titlei_reform_intel.pdf

Executive Order 13356 of August 27, 2004 [Dissemination Phase of C.A.D.] States:

By the authority vested in me as President by the Constitution and laws of the United States of America, and in order to further **strengthen the effective conduct of United States intelligence activities** and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

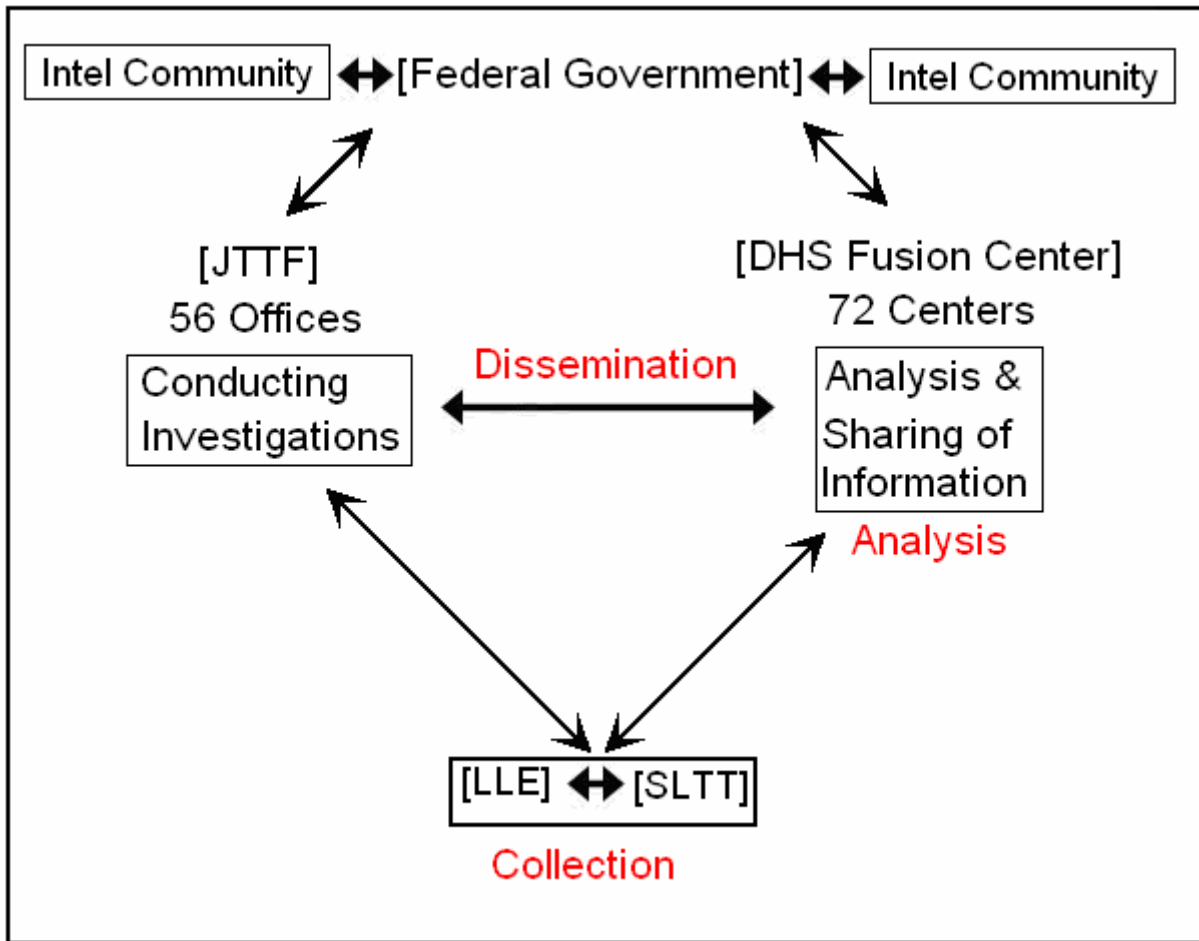
Section 1. Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the **dissemination of information among agencies**:

(a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and (b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a)...

Sec. 3. Preparing Terrorism Information for Maximum Distribution within Intelligence Community. To assist in expeditious and effective implementation by agencies within the Intelligence Community of the policy set forth in section 1 of this order, the Director of Central Intelligence shall, in consultation with the Attorney General and the other heads of agencies within the Intelligence Community, set forth not later than 90 days after the date of this order, and thereafter as appropriate, common standards for the sharing of terrorism information by agencies within the Intelligence Community with (i) other agencies within the Intelligence Community, (ii) other agencies having counterterrorism functions, and (iii) through or in coordination with the Department of Homeland Security, appropriate authorities of State and local governments. These common standards shall improve information sharing by such methods as: (a) requiring, at the outset of the intelligence collection and analysis process, the creation of records and reporting, for both raw and processed information including, for example, metadata and content, in such a manner that sources and methods are protected so that the information can be distributed at lower classification levels, and by creating unclassified versions for distribution whenever possible; (b) requiring records and reports related to terrorism information to be produced with multiple versions at an unclassified level and at varying levels of classification, for example on an electronic tearline basis, allowing varying degrees of access by other agencies and personnel commensurate with their particular security clearance levels and special access approvals; (c) requiring terrorism information to be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any other agency to which it has been made available, to the maximum extent permitted by applicable law, Executive Orders, or Presidential guidance; (d) minimizing the applicability of information compartmentalization systems to terrorism information, to the maximum extent permitted by applicable law, Executive Orders, and Presidential guidance; and (e) ensuring the establishment of appropriate arrangements providing incentives for, and holding personnel accountable for, increased sharing of terrorism information, consistent with requirements of the Nation's security and with applicable law, Executive Orders, and Presidential guidance.¹⁸

¹⁸ <http://www.fas.org/irp/offdocs/eo/eo-13356.htm>

National Intelligence Architecture:



Intelligence Dissemination

- Vertical Intelligence Dissemination: [explain]
- Horizontal Intelligence Dissemination: [explain]

§2.1:

Fundamentals of Intelligence Handling

16 Elements of the Intelligence Community: [defined at 50 U.S.C. 401a(4)]

Independent Agencies

1. [Central Intelligence Agency \(CIA\)](#)

United States Department of Defense

2. [Air Force Intelligence, Surveillance and Reconnaissance Agency \(AFISRA\)](#)
3. [Army Intelligence and Security Command \(INSCOM\)](#)
4. [Defense Intelligence Agency \(DIA\)](#)
5. [Marine Corps Intelligence \(MCI\)](#)

6. [National Geospatial-Intelligence Agency \(NGA\)](#)
7. [National Reconnaissance Office \(NRO\)](#)
8. [National Security Agency \(NSA\)](#)
9. [Office of Naval Intelligence \(ONI\)](#)

United States Department of Energy

10. [Office of Intelligence and Counterintelligence \(OICI\)](#)

United States Department of Homeland Security

11. [Office of Intelligence and Analysis \(I&A\)](#)
12. [Coast Guard Intelligence \(CGI\)](#)

United States Department of Justice

13. [Federal Bureau of Investigation \(FBI\)](#)
14. [Drug Enforcement Administration \(DEA\)](#)

United States Department of State

15. [Bureau of Intelligence and Research \(INR\)](#)

United States Department of the Treasury

16. [Office of Terrorism and Financial Intelligence \(TFI\)](#)

Keithly, David M. "Intelligence Fundamentals." In *Homeland Security and Intelligence*, edited by Keith Gregory Logan. Santa Barbara: Praeger 2010.

Three Forms of Intelligence:¹⁹

1. **Basic intelligence**, which is concerned with the past and is relatively permanent.
2. **Current intelligence**, which deals with the present.
3. **Intelligence estimates**, which concern the future or the unknown but possible present.

Five Intelligence Disciplines:²⁰

1. **Geospatial Intelligence (GEOINT)**: “(5) The term "geospatial intelligence" means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.”²¹
 - a. Headed by Letitia A. Long, the “first woman to head a major intelligence agency” ([ref](#)).

¹⁹ Keithly, David M. "Intelligence Fundamentals." In *Homeland Security and Intelligence*, edited by Keith Gregory Logan. Santa Barbara: Praeger 2010, p. 44

²⁰ Ibid., p. 45.

²¹ <http://uscode.house.gov/download/pls/10C22.txt>

2. **Human Intelligence (HUMINT)**: “the oldest intelligence discipline”²²

HUMINT is the collection of information by a trained HUMINT collector from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources **as a tool** and a variety of collection methods, both passively and actively, to gather information to satisfy the commander’s intelligence requirements and cross-cue other intelligence disciplines.²³

a. **Problem**: “HUMINT alone is seldom capable of producing sufficient information for accurate decision making” (p. 49).

3. **Signals Intelligence (SIGINT)**: “intelligence derived from the interception and exploitation of foreign electromagnetic emissions,” (p. 49). / Susceptible to counterfeit enemy messages.

a. **Three Elements of SIGINT**:

i. **Communications Intelligence (COMINT)**:

“Intelligence derived from foreign communications systems by other than the intended recipients” (p.50).

1. **Forms of COMINT**:

i. **Voice**

ii. **Morse Code**

iii. **Radioteletype**

ii. **Electronic Intelligence (ELINT)**: “intelligence derived from foreign, noncommunications, electromagnetic radiation emanating from other than nuclear detonations or radioactive sources” (p. 50).

1. **Two forms of ELINT**:

i. **Operational ELINT (OPELINT)**:

ELINT is information derived primarily from electronic signals that **do not contain** speech or text (which are considered **COMINT**)²⁴

ii. **Technical ELINT (TELINT)**:

TELINT is technical and intelligence information derived from the intercept, processing, and analysis of foreign telemetry.²⁵

iii. **Foreign Instrumentation Signals Intelligence (FISINT)**:

²² <http://fpc.state.gov/documents/organization/158484.pdf>

²³ <http://www.state.gov/documents/organization/150085.pdf>

²⁴ http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/elint.pdf

²⁵ http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/elint.pdf

Intelligence information derived from electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems. Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients. Foreign instrumentation signals intelligence is a category of signals intelligence. *Note:* Foreign instrumentation signals include but are not limited to signals from telemetry, beaconry, electronic interrogators, tracking/fusing/ arming/firing command systems...²⁶

4. **Measurement and signature intelligence (MASINT):**

“Measurement and Signature Intelligence (MASINT) is technically derived intelligence (excluding traditional imagery and signal intelligence) which when collected, processed, and analyzed, results in intelligence that detects, tracks, identifies, or describes the signatures (distinctive characteristics) of fixed or dynamic target sources.”²⁷

Examples:

Measurement and Signatures Intelligence (MASINT) is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities. MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems. Telemetry Intelligence (TELINT) is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence (ELINT) can indicate electronic emissions picked up from modern weapons and tracking systems. Both TELINT and ELINT can be types of SIGINT and contribute to MASINT.²⁸

MASINT includes:²⁹

- Radar Intelligence (RADINT)
- Acoustic Intelligence (ACOUSTINT)
- Nuclear Intelligence (NUCINT)
- Radio Frequency/Electromagnetic Pulse Intelligence (RF/EMPINT)
- Electro-optical Intelligence (ELECTRO-OPTINT)
- Laser Intelligence (LASINT)
- Materials Intelligence
- Unintentional Radiation Intelligence (RINT)
- Chemical and Biological Intelligence (CBINT)
- Directed Energy Weapons Intelligence (DEWINT)
- Effluent/Debris Collection
- Spectroscopic Intelligence
- Infrared Intelligence (IRINT)

²⁶ http://www.its.bldrdoc.gov/projects/devglossary/foreign_instrumentation_signals_intelligence.html

²⁷ <http://www.access.gpo.gov/congress/house/intel/ic21/ic21007.html>

²⁸ http://www2.fbi.gov/intelligence/di_ints.htm

²⁹ <http://www.fas.org/irp/program/masint.htm>

5. Open source intelligence (OSINT):

OSINT is drawn from publicly available materials:³⁰

1. The Internet
2. Traditional mass media (e.g. television, radio, newspapers, magazines)
3. Specialized journals, conference proceedings, and think tank studies
4. Photos
5. Geospatial information (e.g. maps and commercial imagery products)

2 Reasons for Undervaluing OSINT

1. “The Intelligence Community’s principal mission is to discover and steal secrets; relying on open sources runs counter to that mission”³¹
2. “It is suggested that the Intelligence Community views clandestine-collected information as being more valuable because it is more difficult to collect.”³²

The Defense Intelligence Agency's Central MASINT Office (CMO),

is the principal user of MASINT data. Measurement and Signatures Intelligence has become increasingly important due to growing concern about the existence and spread of weapons of mass destruction. MASINT can be used, for example, to help identify chemical weapons or pinpoint the specific features of unknown weapons systems. The FBI's extensive forensic work is a type of MASINT. The FBI Laboratory's Chem-Bio Sciences Unit, for example, provides analysis to detect traces of chemical, biological, or nuclear materials to support the prevention, investigation, and prosecution of terrorist activities.³³

§2.2:

Fundamentals of Intelligence Handling (continued)

Four Steps to Transform Information into Intelligence [EAI]:³⁴

1. **Evaluation**: “collected information is appraised as a contribution to a specific goal, its credibility, reliability, relevance, accuracy, or usefulness”

³⁰ <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html>

³¹ <http://fpc.state.gov/documents/organization/98105.pdf>

³² Ibid.

³³ <http://www.fbi.gov/about-us/intelligence/disciplines>

³⁴ <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html> p. 45-48.

2. **Analysis**: “an attempt is made to determine the veracity of the facts in the report...and determining the relationship of the facts”.
 - i. **Hypotheses**: development of plausible explanation.
 - ii. **Evidence**: assessment of relevant data.
 - iii. **Assumptions**: assumptions used to explain missing information.
3. **Integration**: “the analyst assembles the facts and relationships identified during the analysis step into a unified whole”
4. **Interpretation**: “The meaning or significance of the new intelligence pattern is determined by viewing all the processed information in the perspective of an overall intelligence appraisal” / What is the importance?

5 Phases of HUMINT Collection:³⁵

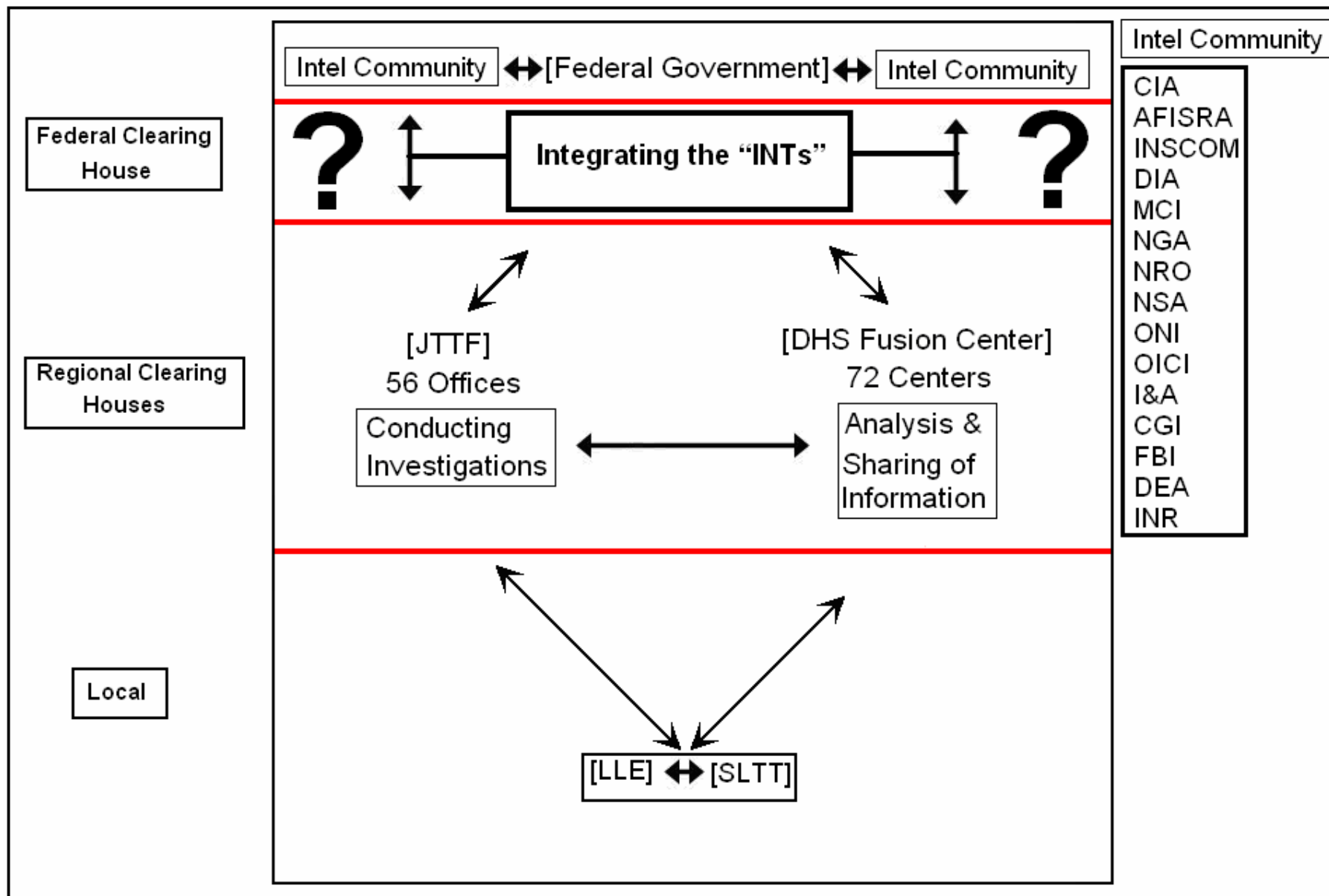
1. **Planning and Preparation**: During this phase, the HUMINT collector **conducts the necessary research** and operational planning in **preparation for** a specific collection effort with a specific source.
2. **Approach**: During the approach phase, the HUMINT collector establishes the conditions of control and rapport to gain the cooperation of the source and to facilitate information collection.
3. **Questioning**: During the questioning phase, the HUMINT collector uses an interrogation, debriefing, or elicitation methodology to ask a source questions **systematically** on relevant topics, **collect information** in response to the intelligence tasking, and ascertain source veracity.
4. **Termination**: During the termination phase, the HUMINT collector completes a questioning session and establishes the necessary conditions for future collection **from the same source** by himself or another HUMINT collector.
5. **Reporting**: During the reporting phase, the HUMINT collector writes, edits, and submits written, and possibly oral, reports on information collected in the course of a HUMINT collection effort. These reports will be reviewed, edited, and analyzed as they are forwarded through the appropriate channels. Chapter 10 discusses reporting in detail.

³⁵ <http://www.state.gov/documents/organization/150085.pdf> “FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS”

Integrating the “INTs”³⁶

The “INTs” have been the pillars of the intelligence community’s organizational structure, but analysis of threats requires that data from all the INTs be **brought together** and that analysts have **ready access to all sources of data** on a timely basis. This has proved in the past to be a substantial challenge because of technical problems associated with transmitting data and the need to maintain the security of information acquired from highly sensitive sources. Some argue that intelligence officials have tended to err on the side of maintaining the security of information even at the cost of not sharing essential data with those having a need to know. Section 1015 of the Intelligence Reform Act mandated the establishment of an Intelligence Sharing Environment (ISE) to facilitate terrorism-related information.

³⁶ <http://fpc.state.gov/documents/organization/158484.pdf> “Intelligence Issues for Congress” March 3, 2011.



§ 3.0

Intelligence and Information Sharing Standards



Image ([Source](#))

Full Intelligence Cycle:³⁷

1. **Planning and Direction:** When we are tasked with a specific job, we begin planning what we'll do and how. We move in a specific direction to get the job done, listing what we know about the issue and what we need to find out. We discuss ways to gather the necessary intelligence.
2. **Collection:** We collect information overtly (openly) and covertly (secretly). Reading foreign newspapers and magazine articles, listening to foreign radio, and watching overseas television broadcasts are examples of “overt” (or open) sources for us. Other information sources can be “covert” (or secret), such as information collected with listening devices and hidden cameras. We can even use space-age technology like satellite photography. For instance, some analysts could actually view how many airplanes are present at a foreign military base by looking at a picture taken from a satellite in space.
3. **Processing:** We take all the information that we have collected and put it into an intelligence report. This information could be anything from a translated document to a description of a satellite photo.
4. **Analysis and Production:** During this step, we take a closer look at all the information and determine how it fits together, while concentrating on answering the original tasking. We assess what is happening, why it is happening, what might occur next, and how it affects US interests.
5. **Dissemination:** In this final step, we give our final written analysis to a policymaker, the same policymaker who started the cycle. After reading the final analysis and learning the answer to the original question, the policymaker may come back with more questions. Then the whole process starts over again.

³⁷ <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html>

Common Terrorism Information Sharing Standards³⁸ (CTISS)

An Information Sharing Environment (ISE):

“The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information.”³⁹

Role of Standards:

Standards have an important role for ensuring consistency of business processes, information flows, information exchanges, and infrastructure development, and they are key decision-making factors when considering future information resource architectures and investments. (p.1)/

Five Goals of the CTISS:⁴⁰

1. Establish a self-governing, institutionalized standards adoption process across Federal, State, local, and tribal governments with common standards that guide counterterrorism information exchange related business processes and investments.
2. Engage foreign and private sector partners to promote the ISE
3. Leverage published, voluntary consensus technical standards when appropriate and available
4. Select and implement performance-driven standards
5. Ensure standards are compliant with public law, Executive Orders, and other policies

2 Examples of Broad Data Standards:

1. Global Justice XML Data Model: [GJXDM] Precursor to NIEM

Xml: [eXtensible Markup Language](#) (XML), which is platform independent.

- **Purpose:** The purpose of the Global JXDM is to provide a consistent, extensible, maintainable XML schema reference specification for data elements and types that represent the data requirements of the general justice and public safety communities. A secondary goal is to provide a baseline model for the data dictionary that can be represented in advanced technologies independently of XML Schema.⁴¹

³⁸ <http://www.ise.gov/sites/default/files/CTISSprogramManual20071031.pdf>

³⁹ White House, Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment, (White House: Washington, DC, 2005), section 2.

⁴⁰ <http://www.ise.gov/sites/default/files/CTISSprogramManual20071031.pdf> p. 3.

⁴¹ <http://it.ojp.gov/jxdm/faq.html#purpose>

- **Mechanics:** an object-oriented XML data model⁴²
 - **Three Parts:**⁴³
 - The Data Dictionary (identifying content and meaning),
 - The Data Model (defining structure and organization),
 - The Component Reuse Repository (a database).

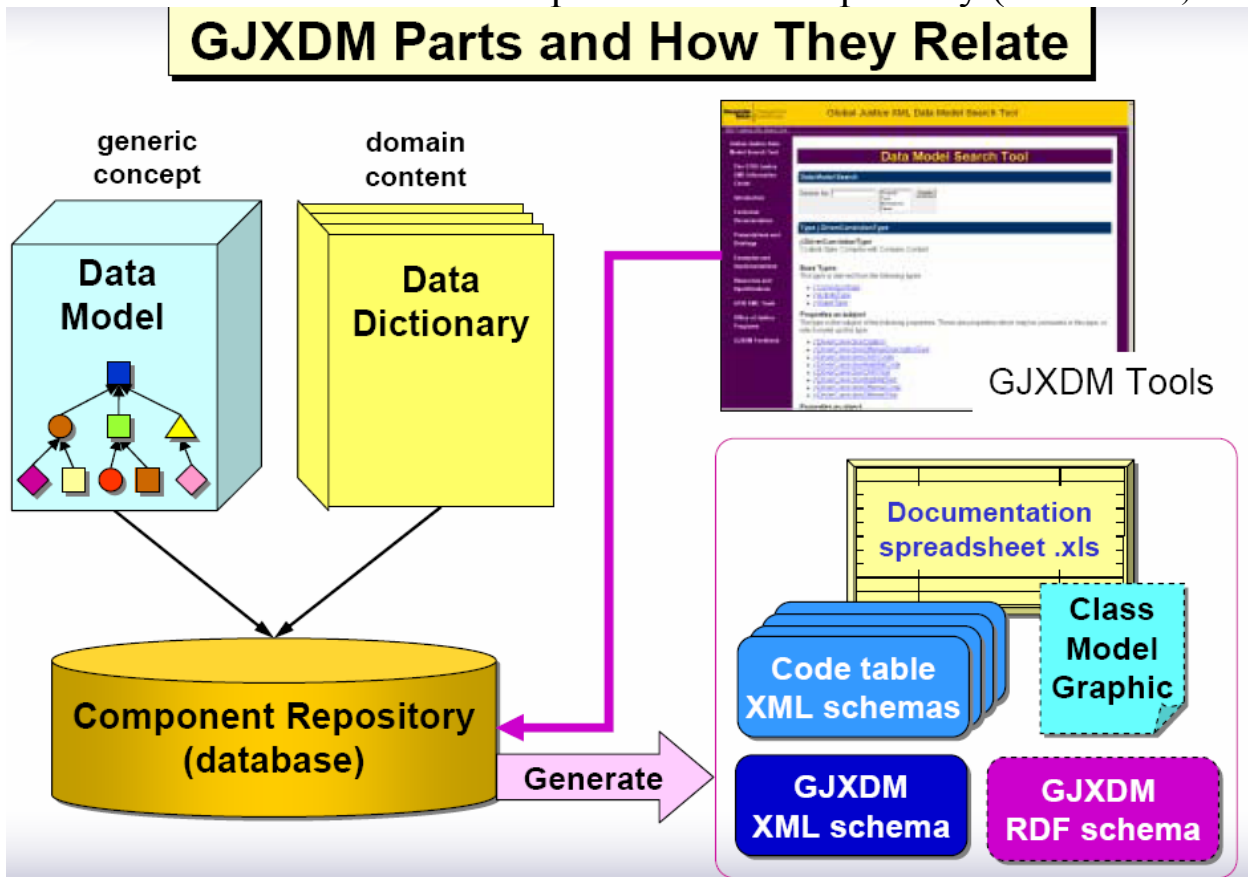


Image ([Source](#))

2. **National Information Exchange Model:** [NIEM]

- Purpose:** It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.⁴⁴
- Mechanics:** NIEM is a framework that defines how messages should be structured within information exchanges. NIEM does not influence how an information exchange is developed or implemented outside the scope of the structure of the message, nor does it attempt to influence how data is maintained.

⁴² <http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1013>

⁴³ http://justicexml.gtri.gatech.edu/workshop/Day1/2_TechnicalWalkThru.pdf

⁴⁴ <http://www.niem.gov/>

It only addresses data in motion, as demonstrated in the diagram below. NIEM sits in the middle of the information exchange and manages only the message within the information exchange. NIEM serves as the common language and structure for XML messages within the information exchange.

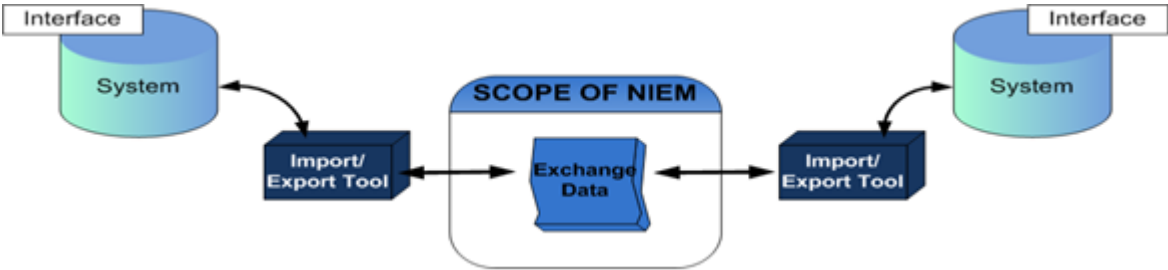
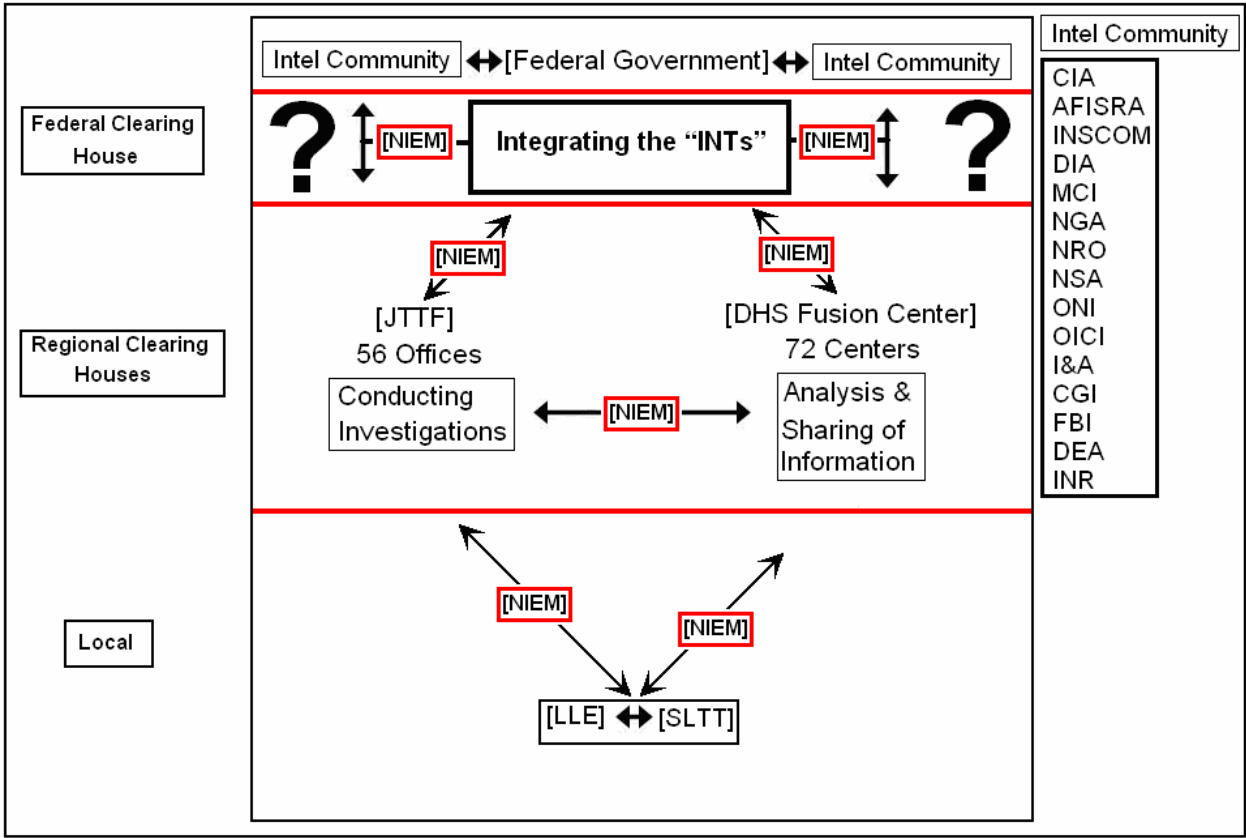


Image ([Source](#))



§4.0

National Security and Strategy Analysis

Strategy Analysis:

1. Concerned with Relationships: the relationship b/ individual policies, goals and the overarching strategy.

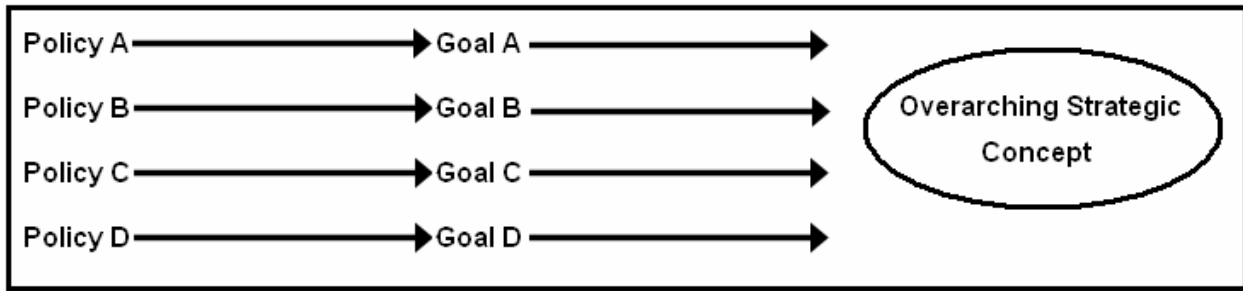


Image (Source)⁴⁵

2. Proactive Analysis: attempts to “seize the initiative and mold future situations in favorable ways” (p. 61).
3. Emergency Management Approach: “Our Nation faces threats from both natural and man-made sources. We will take an **all-hazards approach to emergency management** that allows us to respond effectively to all emergencies, whether caused by acts of nature or by our enemies”⁴⁶

The Five Strategic Goals of the Department of Homeland Security:⁴⁷

1. Protecting Our Nation from Dangerous People:⁴⁸

a. Border Control:

- i. Strengthened role of the U.S. Customs and Border Protection (**CBP**) and U.S. Immigration and Customs Enforcement (**ICE**).
- ii. Enforcement of the REAL ID Act of 2005⁴⁹
- iii. Collect biometrics “(digital finger scans and photographs) from aliens seeking to enter the United States.”⁵⁰
- iv. Enforce the The Western Hemisphere Travel Initiative (WHTI): “Beginning January 23, 2007, all United States citizens and nonimmigrant aliens from Canada, Bermuda, and Mexico departing from or entering the United States from within the Western Hemisphere at air ports-of-entry will be required to present a valid passport.”⁵¹

⁴⁵ Kugler, Richard L. *Policy Analysis in National Security Affairs: New Methods for a New Era*. Washington: National Defense University Press, 2006. p. 62.

⁴⁶ http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf

⁴⁷ http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf

⁴⁸ http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf pg. 6

⁴⁹ [http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.418:](http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.418)

⁵⁰ <http://edocket.access.gpo.gov/2008/E8-8956.htm>

⁵¹ http://www.dhs.gov/xlibrary/assets/whti_airfinalrule.pdf

- b. Enforce Immigration Laws and Immigration Services:
 - i. The National Security Investigation Division's (NSID) National Security Unit (NSU) oversees U.S. Immigration and Customs Enforcement's (ICE) participation on the Joint Terrorism Task Force (JTTF). The JTTF investigates, detects, interdicts, prosecutes and removes terrorists and dismantles terrorist organizations. ICE is involved in almost every foreign terrorism investigation related to cross-border crime. Foreign terrorists need to move money, weapons and people across international borders to conduct their operations, and ICE holds a unique set of law enforcement tools for disrupting these illicit activities.⁵²
 - ii. Enforce Enforcement and Removal Operations (ERO) ([video](#)).
- c. Strengthen Screening of Travelers / Workers:
- 2. **Protecting Our Nation from Dangerous Goods:**⁵³
 - a. [Prevent and Detect Radiological / Nuclear / Biological / Chemical/ Explosive Attacks:](#)
 - i. Detailed step-by-step guide to increase citizen preparedness. ([hyperlink above](#))
 - b. Prevent the Introduction of Illicit Contraband while Facilitating Trade ([video](#))
- 3. **Protect Critical Infrastructure:**⁵⁴
 - a. Protect and Strengthen the Resilience of the Nation's Critical Infrastructure and Key Resources:⁵⁵
 - i. [Executive Order 13231 of October 18, 2001](#)
 - ii. Critical Infrastructure and Key Resources [CI/KR]

Three Effects of Infrastructural Attacks:
[The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets](#)
 [Read from Alperen] p. 135.

 - 1. *Direct infrastructure effects:* Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.⁵⁶

⁵² <http://www.ice.gov/jttf/>

⁵³ http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf pg 10

⁵⁴ http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf pg 14

⁵⁵ Alperen, Martin J. *Foundations of Homeland Security: Law and Policy*. Edited by Ted E. Lewis, Wiley Series on Homeland Defense and Security. New Jersey: John Wiley, 2011., p. 135.

⁵⁶ http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

2. *Indirect infrastructure effects*: Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.⁵⁷
3. *Exploitation of infrastructure*: Exploitation of elements of a particular infrastructure to disrupt or destroy another target.⁵⁸
- b. Ensure Continuity of Government Communications and Operations:
- c. Improve Cyber Security.⁵⁹
Alperen's List of Cyber Security Laws: (p. 157).
 - i. Patriot Act 2001
 - ii. Homeland Security Act of 2002
 - iii. Cyber Security Research and Development Act, November 27, 2002
 - iv. The National Strategy to Secure Cyberspace, February 2003.
 - v. HSPD – 23: National Cyber Security Initiative, January 8, 2008.
- d. Protect Transportation Sectors:
4. **Strengthen our Nation's Preparedness and Emergency Response Capabilities**.⁶⁰
 - a. Ensure Preparedness:
 - i. National Preparedness.⁶¹ [PRESIDENTIAL POLICY DIRECTIVE/PPD-8] *Signed march 30, 2011*.
 1. Creating a Culture of Preparedness
 2. Definitions:

(a) The term "**national preparedness**" refers to the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation.

⁵⁷ http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

⁵⁸ http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

⁵⁹ Alperen, Martin J. *Foundations of Homeland Security: Law and Policy*. Edited by Ted E. Lewis, Wiley Series on Homeland Defense and Security. New Jersey: John Wiley, 2011., p. 157.

⁶⁰ http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf pg 18

⁶¹ http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm

(b) The term "**security**" refers to the protection of the Nation and its people, vital interests, and way of life.

(c) The term "**resilience**" refers to the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

(d) The term "**prevention**" refers to those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Prevention capabilities include, but are not limited to, information sharing and warning; domestic counterterrorism; and preventing the acquisition or use of weapons of mass destruction (WMD). For purposes of the prevention framework called for in this directive, the term "prevention" refers to preventing imminent threats.

(e) The term "**protection**" refers to those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. Protection capabilities include, but are not limited to, defense against WMD threats; defense of agriculture and food; critical infrastructure protection; protection of key leadership and events; border security; maritime security; transportation security; immigration security; and cybersecurity.

(f) The term "**mitigation**" refers to those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. Mitigation capabilities include, but are not limited to, community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred.

(g) The term "**response**" refers to those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

(h) The term "**recovery**" refers to those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.

b. Strengthen Response and Recovery:

5. **Strengthen and Unify DHS Operations and Management:**⁶²

a. Improve Department Governance and Performance

b. Advance Intelligence and Information Sharing

c. Integrate DHS Policy, Planning, and Operations
Coordination

§4.1

**Strategic Development of
Interagency Capabilities and Coordination**

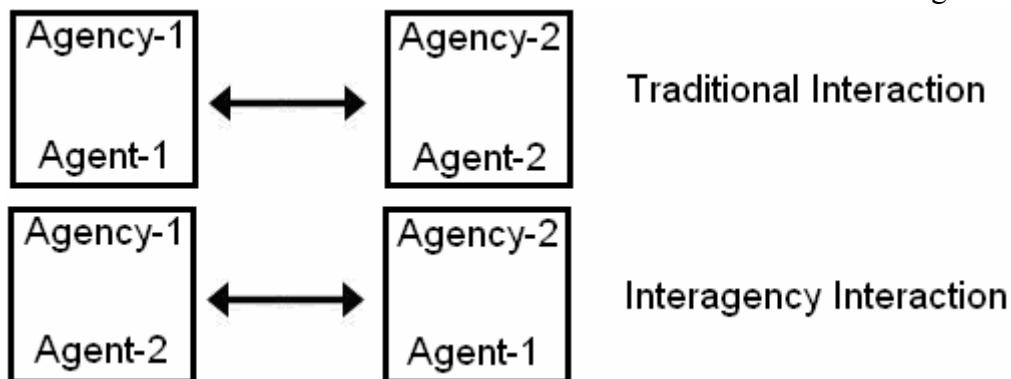
⁶² http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf pg 22.

Four Impediments to Interagency Coordination:⁶³

1. Separate statutory missions:
But the more fundamental impediments to cooperative interagency and intergovernmental management of major disasters will not be so easily resolved. That is because these problems are rooted in divergent sources of constitutional authority, in divergent statutory missions and administrative means, and thus in divergent organizational cultures.⁶⁴
2. Administrative Barriers:
3. Divergent Sources of Constitutional Authority:
4. An Interagency Entity Might not be Responsive to Congressional Oversight Committees:⁶⁵

Five Ways of Strengthening Interagency Cooperation:

1. Strengthen Interagency Cooperation between Local Law Enforcement and Public Health:⁶⁶
 - a. *The Liaison Model.* Crossover **training** and assignments of law enforcement and public health personnel can facilitate **communication of information** between the agencies and provide **on-site consultation**. This model was reported to be successful in improving cross-agency coordination in the United States and Canada. **Cross-fertilization**, gaining legitimacy in the partnering agency, and increased access and information sharing were among the benefits listed by stakeholders.⁶⁷
 - i. Using a "liaison" model, in which personnel from one agency are assigned to work at other agencies for periods of time; sharing staff in this way facilitates communication and on-site consultation across agencies.⁶⁸



⁶³ <http://fpc.state.gov/documents/organization/156509.pdf> 4 of 13

⁶⁴ http://www.google.com/url?sa=t&source=web&cd=12&ved=0CB8QFjABOAO&url=http%3A%2F%2Ftraining.fema.gov%2FEMIWeb%2Fedu%2F07conf%2Fpresentation%2FTuesday%2520-%2520Burton%2520-%2520Constitutional%2520Framework%2520for%2520All-Hazards%2520D.doc&rct=j&q=%22statutory%20missions%22%20terrorism%20definition%20site%3A.gov&ei=lq bBTcWBBcS1tweMh_zcBA&usq=AFOjCNE796oMr89HEBKQxU4Ep0drZD-mMA&cad=rja

⁶⁵ <http://fpc.state.gov/documents/organization/156509.pdf> 7 of 13

⁶⁶ <http://www.ncjrs.gov/pdffiles1/nij/grants/212868.pdf>

⁶⁷ <http://www.ncjrs.gov/pdffiles1/nij/grants/212868.pdf> 13 of 182

⁶⁸ <http://www.nij.gov/journals/260/interagency-coordination-lessons.htm>



Agent 2-1: has the same roughly the same skill set as Agent 1-2 with only variations in the *emphasis* of initial training [explain].

2. Strengthen Interagency Cooperation between Local Law Enforcement and the Intelligence Community⁶⁹

- a. SEC. 701. EXPANSION OF REGIONAL INFORMATION SHARING SYSTEM TO FACILITATE FEDERAL-STATE-LOCAL LAW ENFORCEMENT RESPONSE RELATED TO TERRORIST ATTACKS....
- b. Establishing and operating secure information sharing systems to enhance the investigation and prosecution abilities of participating enforcement agencies in addressing multi-jurisdictional terrorist conspiracies and activities.⁷⁰

3. Clearly Define the Role and Responsibilities of Key Federal Agencies:⁷¹

- a. Information MUST be shared among Federal Agencies:

Subtitle I—Information Sharing

SEC. 891. SHORT TITLE; FINDINGS; AND SENSE OF CONGRESS.

(a) SHORT TITLE.—This subtitle may be cited as the ‘‘Homeland Security Information Sharing Act’’.

(b) FINDINGS.—Congress finds the following:

(1) The Federal Government is required by the Constitution to provide for the common defense, which includes terrorist attack.

(2) The Federal Government relies on State and local personnel to protect against terrorist attack.

(3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.

⁶⁹ ‘‘provisions encouraging the exchange of law enforcement and intelligence information were included in the USA Patriot Act (P.L. 107-56)’’

⁷⁰ <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>

⁷¹ <http://www.gao.gov/new.items/d03165.pdf> 61 of 274

(4) **Some homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack.**

(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information. **[explain]**

(6) **Granting security clearances to certain State and local personnel is one way to facilitate the sharing of information** regarding specific terrorist threats among Federal, State, and local levels of government.

(7) Methods exist to declassify, redact, or otherwise adapt classified information so it may be shared with State and local personnel without the need for granting additional security clearances.

(8) State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by Federal agencies.

(9) The Federal Government and State and local governments and agencies in other jurisdictions may benefit from such information.

(10) Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response **agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.**

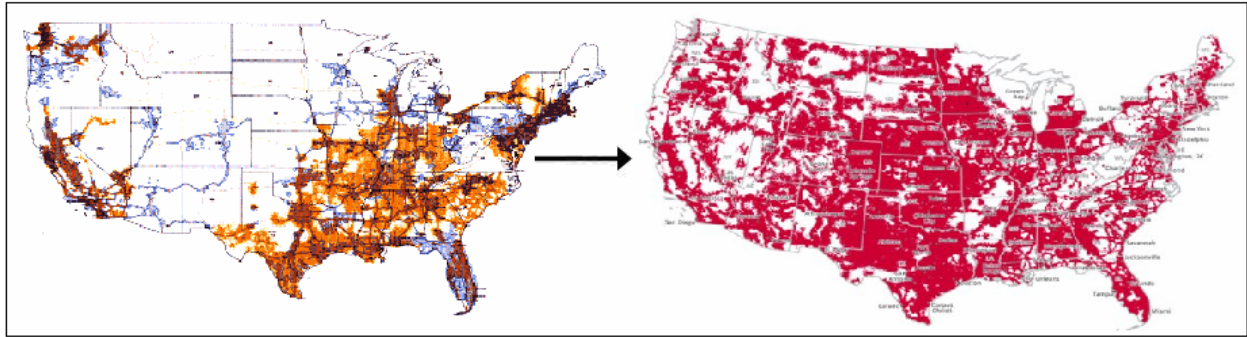
(11) Information systems, including the National Law Enforcement Telecommunications System and the Terrorist Threat Warning System, have been established for rapid sharing of classified and sensitive but unclassified information among Federal, State, and local entities.

(12) **Increased efforts to share homeland security information should avoid duplicating existing information systems.**

(c) SENSE OF CONGRESS.—It is the sense of Congress that Federal, State, and local entities should share homeland security information to the maximum extent practicable, **with special emphasis on hard-to-reach urban and rural communities.** [total coverage as underlying goal **[KEY]**]⁷²

⁷² http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf pg 2252-2253 / 118-119 of 187

Example of Enhanced “Coverage” Analogy: [explain]



4. Create an Interagency Coordination Mechanism:⁷³

a. **Importance of Coordination:**

- i. Large number of agencies
- ii. Different functions
- iii. Policy Coordination is Critical for the overall Strategic

Concept: **The National Security Council:**

1. The Council also serves as the President's principal arm for coordinating these policies among various government agencies.⁷⁴

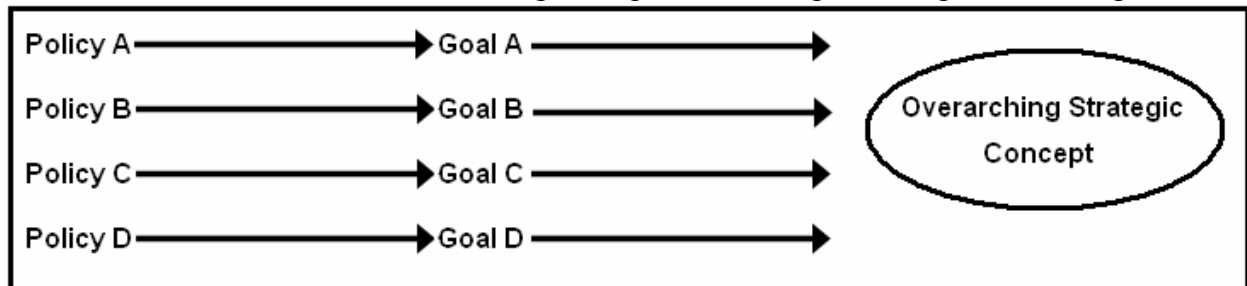


Image (Source)⁷⁵

2. The **Principals Committee** will be the “**senior interagency forum** for consideration of policy issues affecting national security” while the Deputies Committee will “review and monitor the work of the NSC interagency process” and “shall be responsible for day-to-day crisis management.”⁷⁶

[Key Weakness]: Today’s international terrorist threat can encompass not only physical attacks on U.S. physical structures such as the World Trade Center, but also cyber-attacks on critical infrastructures, the computerized communications and data storage systems on which U.S. society has become reliant. Since such systems are in most cases owned and operated by corporations and other commercial entities, the role of the NSC is necessarily constrained. Much depends on law enforcement as well as voluntary cooperation by the private sector.⁷⁷

⁷³ <http://www.gao.gov/new.items/d03165.pdf> 69 of 274

⁷⁴ <http://www.whitehouse.gov/administration/eop/nsc/>

⁷⁵ Kugler, Richard L. *Policy Analysis in National Security Affairs: New Methods for a New Era*. Washington: National Defense University Press, 2006. p. 62.

⁷⁶ <http://fpc.state.gov/documents/organization/125948.pdf> 26 of 39

⁷⁷ <http://fpc.state.gov/documents/organization/125948.pdf> 31 of 39

5. Facilitate Interagency Access to “Knowledge Banks”⁷⁸

“Sharing that Information”

[The National Counterterrorism Center] NCTC serves as the [United States Government] USG’s **central and shared knowledge bank on known and suspected terrorists and international terror groups**...NCTC collocates more than 30 intelligence, military, law enforcement and homeland security networks **under one roof** to facilitate robust information sharing. **NCTC is a model of interagency information sharing**⁷⁹

Strategic Ideological Approaches to Fighting Terrorism

§4.2 “A War without Bullets”

It is the policy of the United States to seek and support democratic movements and institutions in every nation and culture, with the ultimate goal of ending tyranny in our world...The goal of our statecraft is to help create a world of democratic, well-governed states that can meet the needs of their citizens and conduct themselves responsibly in the international system.⁸⁰

Democratic Peace Theory⁸¹

- The process of creating a more democratic world requires a **generational** approach.
- Democratization is contrasted from ideological repression/tyranny.

Championing freedom advances our interests because the survival of liberty at home increasingly depends on the success of liberty abroad. Governments that honor their citizens’ dignity and desire for freedom tend to uphold responsible conduct toward other nations, while governments that brutalize their people also threaten the peace and stability of other nations.⁸²

Global Liberty → Domestic Liberty

- The preservation of global liberties abroad strengthen domestic liberty
- As long as global liberties are strong, domestic liberties will remain strong
- Regional destabilization abroad, threatens our strategic approach to democratization.
- Thus, an investment in regional stabilization “reflects our values and advances our interests”⁸³ -----Understanding the Threat

⁷⁸ <http://publicintelligence.net/national-counterterrorism-center-nctc/>

⁷⁹ <http://publicintelligence.net/national-counterterrorism-center-nctc/>

⁸⁰ <http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/sectionI.html>

⁸¹ http://jasonjcampbell.org/uploads/International_War_and%20Terrorism.pdf pg 9-10 of 26.

⁸² <http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/sectionII.html>

⁸³ <http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/sectionII.html>

Tyranny:

Tyranny is the combination of brutality, poverty, instability, corruption, and suffering, forged under the rule of despots and despotic systems... it is a crime of man, not a fact of nature.⁸⁴

4 Steps to Promoting Democracy:

1. Defend Human Rights:
2. Responsive the “Will of the People”
3. Maintaining Order and Impartiality
4. Limit Governmental Reach

§4.3

5 Steps in Understanding the Ideological War on Terror:

1. There **IS** also an invisible [ideological] war against terrorism.
 1. “From the beginning, the War on Terror has been both a battle of arms and a battle of Ideas.”⁸⁵
 - i. **Saul Smilansky** describes al-Qaida’s ideology in the following manner: “The ideology of this group is radical: it is antidemocratic and totalitarian, utopian, opposes universal human rights and the emancipation of women, anti-Western and anti-Semitic, and in favor of a continuous violent struggle toward the establishment of universal fundamentalist Muslim rule.”⁸⁶
2. Four Misconceptions about the Causes of Terrorism:
 - i. **Not** a byproduct of poverty
 - ii. **Not** simply a result of anti-U.S. sentiments
 - iii. **Not** simply a result of Israeli-Palestinian issues.
 - iv. Terrorism is **Not** simply a response to our efforts to prevent terror attacks. The al-Qaida network targeted the United States long before the United States targeted al-Qaida. Indeed, the terrorists are emboldened more by **perceptions of weakness**⁸⁷ than by demonstrations of resolve. Terrorists lure recruits by telling them that we are decadent, easily intimidated, and will retreat if attacked.⁸⁸
3. Terrorism is grounded in an **Exclusionary Ideology:**
 1. Terrorism **IS** grounded in an exclusionary ideology and is THEREFORE subject to the

⁸⁴ Alperen, Martin J. *Foundations of Homeland Security: Law and Policy*. Edited by Ted E. Lewis, Wiley Series on Homeland Defense and Security. New Jersey: John Wiley, 2011., p. 112.

⁸⁵ Ibid, p. 112.

⁸⁶ Smilansky, S. (2004). "Terrorism, Justification, and Illusion." *Ethics* 114(4): 790-805. p. 796.

⁸⁷ http://jasonjcampbell.org/uploads/International_War_and%20Terrorism.pdf pg. 1 of 26

⁸⁸ <http://fpc.state.gov/documents/organization/71898.pdf> pg. 14 of 29.

inherent WEAKNESS of any exclusionary ideology. The “War on Terror” must seek to exploit these weaknesses.

2. Exclusionary Ideologies: [dissertation]
 - i. Dogmatic approach to truth [self referential/justified]
 1. **Exploitation of inherent Weakness**: Instill Opposition among Supporters. Embolden supporters or current members to augment their views. [Terrorist leaders cannot tolerate ANY augmentation] Augmentation = Weakness, which is False, but they have to believe this.
 2. **Disadvantage**:
 - a. If terrorist organizers recognize this they will strengthen their organization by killing any who waiver, which suggests that only the most fervent and loyal will remain.
 - ii. Requires **total domination of information** and competing narratives.
 1. **Exploitation of inherent Weakness**: Support the liberation of information and a global internet access initiative, broader telecommunication and internet coverage. Incentives corporate participation:
 - a. E.g., set an initiative to increase global internet connectivity [multinational responsibility]
 2. **Disadvantage**:
 - a. Terrorist organizations use the benefits of globalization, including technological advancement to orchestrate their networks.
 - iii. Exclusionary Ideologies are implemented to **enforce homogenous societies** [explain]
 1. **Exploitation of inherent Weakness**:
 - a. Homogeneous societies are fundamentally impossible to attain/maintain. Persons who

§4.4

feel they are members of a “Protected Population” need to recognize that they are not. Their levels of comfort should be disrupted.

2. **Disadvantage:**

a. Terrorist organizations are master manipulators because they direct and control people by giving them the belief that their beliefs aren't threatening to the organization.

They pacify their moderates. [Explain]

iv. Exclusionary Ideologies **cannot** be operationalized without support from Moderates

1. **Exploitation of inherent Weakness:** Known supporters, financiers, those who provide safe havens, even those who know but remain silent should be punished to the fullest extent, and they should be made an example of...send a message to Moderates.

2. **Disadvantage:**

a. Terrorists will use the attack, arrest, prosecution etc of moderates to embolden their cause and “reframe” the targeting of Moderates [“non participants”] as an attack on innocent people.

v. Exclusionary Ideologies assume that there are some people not worthy of moral consideration

1. Most difficult to exploit. [explain]

4. **4 Causes of Terrorism:**⁸⁹

1. Political Alienation:

2. Grievances that can be blamed on others:

3. Sub-cultures of Conspiracy and Misinformation:

i. Poses greatest threat to encouraging **Domestic Terrorist.** The willful pronouncement of

⁸⁹ Alperen, Martin J. *Foundations of Homeland Security: Law and Policy*. Edited by Ted E. Lewis, Wiley Series on Homeland Defense and Security. New Jersey: John Wiley, 2011., p. 112.

⁸⁹ Ibid, p. 113

misinformation is not only unpatriotic but it fosters terrorist ideologies.

4. An ideology that justifies murder
5. **4 Responses to the 4 Causes:**
 1. *Alienation:* **Ownership**:
 2. *Grievances:* **Dispute Resolution**:
 3. *Conspiracy and Misinformation:* **Freedom of Speech and Independent Media**
 4. *Ideology that justifies murder* [Exclusionary Ideology]: **Human Dignity**