Intel-Cyclopedia

A Guide to Sources of Information for the Intelligence Community

Michael Chesbro (Editor)
Intel-Cyclopedia

A Guide to Sources of Information for the
Intelligence Community

Michael Chesbro (Editor)

September 2011
Intel-Cyclopedia is intended to be a Guide to Sources of Information for the Intelligence Community. It is compiled from multiple and various sources of information which are either in the public domain or the inclusion of which complies with the Fair Use Doctrine.

The information found in the Intel-Cyclopedia may not have been fully validated.

Intel-Cyclopedia is a living document which is regularly updated and changed. Intel-Cyclopedia not intended to be an exhaustive compilation of all sources of information available to the intelligence community. The specific sources of information included in the Intel-Cyclopedia exemplify the types of information available, and that which may have proven useful in the past.

Intel-Cyclopedia is distributed in accordance with Title 17 U.S.C. Section 107, without profit or payment to those who have expressed a prior interest in receiving this information for non-profit research and educational purposes only.

The inclusion of specific products or services should not be viewed as an endorsement by any agency, organization, or person.

Some of the resources listed may require DOD PKI or other registration to access.
Advanced Global Intelligence Learning Environment

URL: http://www.agile.mil

AGILE is an IC-Wide collaborative learning environment that encourages the sharing of learning solutions and enables the IC training community to operate cohesively as a single enterprise. Using a "best of breed" shared services model, technical and functional experts throughout the Community are working together to deliver relevant, timely and cost effective learning solutions to the worldwide workforce; in-turn enhancing professional and personal development and workforce planning.

Advanced Intelligence Analyst Course (AOC 35D/MOS 350B/D/L and MOS 96B)

US Army Correspondence Course
301 D17
United States Army Intelligence Center & Fort Huachuca
Fort Huachuca, AZ 85613-6000

Advanced Intelligence Analyst Course


The course contains the subsources listed below.

IT0478, Intelligence Support of Division Operations
IT0480, Intelligence in Support of Internal Defense Operations
IT0583, Strategic Intelligence
Advanced Technical Intelligence Association (ATIA)

URL: http://atia-assn.org/

In 2008, the MASINT Association reorganized to become the Advanced Technical Intelligence Association (ATIA). This change occurred in recognition of the growing utility of traditional MASINT and MASINT-related capabilities and their emergence into new capabilities such as Advanced Geospatial Intelligence, etc., throughout our homeland security, defense and intelligence communities. The Association was organized in November 1998 and incorporated on January 1999 in Washington, DC as a nonprofit trade association (501-6c). The Advanced Technical Intelligence Association provides education, awareness and training, but does not lobby, and membership dues are 100% deductible as a business expense. Members range from the largest aerospace corporations to small businesses, all with a common interest in advancing the maturity, applications, and benefits of MASINT technologies.

Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISR)

URL: http://www.afisr.af.mil/

Air Force Language, Region & Culture Program

URL: http://culture.af.edu/index.html
AKO Foreign Language Resources
URL: https://www.us.army.mil/suite/doc/5987514&inline=true

AKO Intelligence
URL: https://www.us.army.mil/suite/page/6

American Cryptogram Association
URL: http://cryptogram.org/
The American Cryptogram Association (ACA) is a non-profit organization dedicated to promoting the hobby and art of cryptanalysis -- that is, learning to break ciphers.

American Military University - Intelligence Program
URL: http://www.amu.apus.edu/lp/intelligence/index.htm
Intelligence Studies is one of the flagship programs at American Military University. These well balanced and academically rigorous programs are well respected throughout the intelligence community and prepare students to enter into or advance their careers in the areas of intelligence analysis, collections, operations or a variety of intelligence related fields. All courses are conducted using open source materials, so no security clearance is required. Course discussions are highly relevant because our faculty have extensive experience in intelligence and students are drawn from a variety of backgrounds.

If you are, or want to be an intelligence professional, American Military University’s intelligence degrees and certificates provide you with the knowledge, critical thinking, and analytic skills that will help you advance your career in national security intelligence, law enforcement intelligence, or a supporting field.

- Available Programs

Michael Chesbro
- Undergraduate Certificate in Intelligence Analysis
- Graduate Certificate in Intelligence Analysis
- B.A. in Intelligence Studies
- M.A. in Intelligence Studies
- Graduate Certificate in Intelligence Studies

- Related Programs

- A.A. in Counter-Terrorism Studies
- Homeland Security Degrees & Certificates
- International Relations Degrees
- National Security Studies Degrees & Certificates

Anacapa Web-based Training

URL:  http://www.anacapatraining.com/webtraining/index.html

This free web-based training is provided as an introduction to Anacapa’s scheduled and on-site courses in intelligence analysis. Upon completion of all three training modules, you may obtain a certificate of completion.

**Introduction to Intelligence Analysis** (1 to 2 Hours)

This session provides an overview of the intelligence process and shows where and how intelligence analysis fits into this process. We will examine the various types of information ranging from surveillance reports to data from an internet site, from physical evidence to financial records, and from informant reports to the reports of other analysts. The purpose of the intelligence process is to develop inferences that explain the Who, What, Why, When, Where and How of the activity of interest, leading to an inference that can be acted on with confidence.

**Data Collection Tradeoffs** (2-3 Hours)

This session provides solutions to a common dilemma faced by intelligence analysts—whether to report an inference based on available information or to collect additional information. More information might produce a better inference but at greater costs and at a loss of timeliness. In short, the decision to seek additional information requires tradeoffs among value, cost and risk. We want to get the greatest value at the least cost and without risking the timeliness of the intelligence product.

**Critical Thinking Strategies** (2-3 Hours)
In this third session we address critical thinking—the interpretation, assessment and reasoning skills required for success in intelligence analysis. We will, first, examine some of the types of challenges that face analysts by providing issues and problems that demonstrate critical thinking. Second, we will review the context in which critical thinking must take place. Then, we will present the types of human limitations that must be overcome and a model that illustrates the various factors and components of critical thinking. Finally, we present and discuss strategies that will lead to the most effective critical thinking.

**Analysis of Competing Hypotheses Software**

URL: [http://www2.parc.com/istl/projects/ach/ach.html](http://www2.parc.com/istl/projects/ach/ach.html)

Analysis of Competing Hypotheses (ACH) is a simple model for how to think about a complex problem when the available information is incomplete or ambiguous, as typically happens in intelligence analysis. The software downloadable here takes an analyst through a process for making a well-reasoned, analytical judgment. It is particularly useful for issues that require careful weighing of alternative explanations of what has happened, is happening, or is likely to happen in the future. It helps the analyst overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult. ACH is grounded in basic insights from cognitive psychology, decision analysis, and the scientific method. It helps analysts protect themselves from avoidable error, and improves their chances of making a correct judgment.

This software was developed by Palo Alto Research Center (PARC) in collaboration with Richards J. Heuer, Jr. It was developed for use by the U.S. Intelligence Community with funding from the Intelligence Community's Advanced Research and Development Activity (ARDA) and the Office of Naval Research (ONR).

In distributing ACH, PARC is making the presently downloadable version of the program available to the general public at no cost when used for non-commercial or educational purposes subject to the terms and conditions of its end user license.

**Analyst Toolbox**


Provides intelligence analysts with information on the tools they need to effectively and efficiently perform their duties and produce useful intelligence products. The tools examined in
this document represent the basic toolbox that the intelligence analyst will need to provide the vital intelligence service expected in today’s law enforcement environment.

**Analyst’s Style Manual**  
**Mercyhurst College Institute for Intelligence Studies**


**Analytic Learning Community of Practice** (on Intellink)  


The Analytic Learning Community of Practice (ALCOP) is an outgrowth of the Analytic Training Pilot funded in 2010-2011 by the Joint Forces Intelligence Training Council (JFITC). It is designed to bring all analytic faculty across the Defense Intelligence Enterprise (DIE) and Intelligence Community (IC) into a collaborative environment.

Using websites, communications, conferences, and publications, it will share curricula, syllabi, course materials, ideas and visions with each other such that the community will be enriched by this synergy and our student body will likewise be enriched. There are mirror or similar websites for ALCOP on SIPR and JWICS level Intellipedias as well. Although the ALCOP germinated at the Joint Military Intelligence Training Center through its collaborative work, the ALCOP will be furthered by faculty at the Combatant Commands, the Service intelligence schools, defense colleges and universities, other combat support agencies (CSAs) and our colleagues in the Intelligence Community.

**Analytical Investigative Tools (Course)**


This course provides an overview of analytical investigative tools and techniques. The course introduces the role of the analyst and the analytical process for narcotic law enforcement officers. A brief overview of drugs of abuse is followed by a set of analytical 'tools' including methods for acquiring information, techniques for representing and analyzing information, and
an overview of financial investigations. Produced by MCTFT in partnership with the United States Army Military Police School, and the National Guard Bureau Counterdrug Directorate.

Course Objectives

- Understand the role of the analyst, the components of the analytical process, and the importance of critical thinking.
- Identify drugs of abuse, their primary sources and the primary methods of distribution.
- Identify sources of information, including federal state and local sources, major computer databases and confidential sources.
- Understand the purpose of flowcharting, and learn to create event, commodity, and activity flowcharts.
- Learn the purpose of link analysis, how to organize data into an association chart, and how to create a link analysis chart.
- Understand the purpose of telephone toll analysis, identify methods of electronic surveillance and procedures to perform telephone toll analysis.
- Describe the purpose of financial analysis, money laundering, and procedures to launder money.
- Learn about the Posse Comitatus Act.

Course Length: 4 hours

Anti-Keylogging Software

URL: http://www.qfxsoftware.com/

KeyScrambler Personal - Recommended by PC World as one of the "15 Great, Free Privacy Downloads" - Protects your login credentials, credit card numbers, passwords, search terms, Java, Flash, PDF Forms, web email and more in IE, Firefox, and Flock against known and unknown keyloggers. Download Free

Anti-Terrorism Intelligence Awareness Training Program

URL: http://cop.spcollege.edu/Training/WMDCourses/AIATP-WMD.htm

Module One - Terrorism Overview: You will learn broad definitions of terrorism, specific international and domestic terrorist events that have occurred in the U.S., and historical examples of how everyday officers have made a difference in combating terrorism. You will learn to differentiate between the ordinary criminal and terrorist based motivating factors and goals. You will be able to describe the organization,
composition, operations, goals and financial networks types and forms of regional, national and international terrorist groups.

**Module Two - Criminal Intelligence Process:** You will learn to identify standardized terms and the applicable legal authority upon which the intelligence process is based. You will identify both the characteristics and the differences between criminal information and intelligence. You will be able to describe the components of criminal information / intelligence and how they are processed and evaluated via that Intelligence Cycle. Finally, you will be able to identify the law enforcement officer’s responsibilities in the collection and reporting of criminal information and intelligence and identify the federal agencies that are collecting the information.

**Module Three - Indicators of Terrorist Activity:** You will learn to identify the tools terrorists use to perpetrate terrorist activities. You will be able to describe behavioral patterns exhibited by terrorists during the planning and implementation stages. Further, you will identify media that are used by terrorists to facilitate their activities and / or circumvent discovery. You will be able to articulate instances when an indicator should be reported.

**Module Four - Internet Assisted Terrorism:** You will be able to identify the electronic tools and media which international and domestic terrorists use and the best practices identified for properly seizing computer hardware and peripherals.

---

**Anti-Terrorism - FM 3-37.2 (February 2011) (FOUO)**

URL: [https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/fm3_37x2.pdf](https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/fm3_37x2.pdf) (AKO Log-in Required)

Field Manual (FM) 3-37.2 establishes fundamental operations for antiterrorism (AT) operations across the full spectrum of military operations. It is based on lessons learned from terrorist attacks, wartime engagements, and existing and developing AT strategies (military, federal, state, and local), policies, and doctrine.

---

**Anti-Terrorism - JP 3-07.2 (24 November 2010)**


- Provides an introduction to antiterrorism
- Covers the terrorist threat
• Discusses intelligence, counterintelligence, threat analysis, and countersurveillance
• Covers legal considerations
• Describes the antiterrorism program
• Discusses preventative measures and considerations
• Covers incident response and consequence management

Anti-Terrorism Level-1 Training

URL: https://atlevel1.dtic.mil/at/

Department of Defense anti-terrorism awareness training program. The purpose of this training is to increase your awareness of terrorism and to improve your ability to apply personal protective measures. Completion of this training meets the annual requirement for Level I anti-terrorism training prescribed by DoDI 2000.16.

Anti-Terrorism Level-II Refresher Training

URL: https://www.blackboard.wood.army.mil/ (Requires AKO Log-in)

Anti-Terrorism Officer (ATO) refresher training contains 4 lessons that must be completed in sequential order.

• Prepare a Threat Matrix
• Prepare the MSHARPP and CARVER Matrices
• Prepare a Vulnerability Assessment
• Prepare a Risk Assessment

A certificate of completion will be available when the final lesson is completed.
Anti-Terrorism | Unit ATO Handbook (September 2010)

URL:  https://www.us.army.mil/suite/page/605757  (AKO Login Required)

The Unit ATO Handbook is a technical publication focused on operating force unit antiterrorism officers (ATOs) at the brigade and battalion levels. It establishes a unit AT framework for operating force ATOs to use in identifying and reducing terrorist threats to their unit operations, whether in garrison or a combat zone; provides unit-level ATOs with detailed implementation guidance for the AT tasks and relevant unit standards in specific mission environments; and also provides detailed knowledge and procedures that will help them do their jobs more effectively.

Anti-Terrorism (A Self-Help Guide) (1 September 2010)


Aristotle (DTIC)

URL:  https://www.dtic.mil/aristotle/

Aristotle is a powerful, web-based social networking tool along the lines of LinkedIn, MySpace, or Facebook, designed specifically for Department of Defense (DoD) science and technology (S&T) workers. Unlike MySpace or Facebook, Aristotle enables you to extend your professional network and learn about the technical and professional interests and capabilities of others across our whole enterprise. While most social networking systems are focused on just individuals, Aristotle works with People, Projects, Topics, and Documents.

The Aristotle tool is a collaborative learning and discovery system that allows you to gather, prioritize, and utilize vast amounts of information. It allows you to build networks of people, projects and topics. Aristotle also makes it easy to find people, understand technical topics, and learn about or advertise technical projects.

Who can access Aristotle?

Aristotle can potentially be accessed by all Department of Defense (DoD) employees. Aristotle is hosted by the Defense Technical Information Center (DTIC) and should be available to everyone.
employed by a DoD agency or organizations. DoD employees include Military, Civilian, and Contractors.

**Armed Forces Communications & Electronics Association (AFCEA)**

URL:  [http://www.afcea.org/](http://www.afcea.org/)

The Armed Forces Communications and Electronics Association (AFCEA) established in 1946, is a non-profit membership association serving the military, government, industry, and academia as an ethical forum for advancing professional knowledge and relationships in the fields of communications, information technology, intelligence, and global security. AFCEA supports local chapters, sponsors events, publishes the award-winning SIGNAL Magazine, promotes education, and provides member benefits – all with the purpose of equipping its members to meet government’s challenges and to further their careers.

**Armed Forces Communications and Electronics Association - Intelligence**


AFCEA Intelligence was established in 1981 as part of AFCEA International to enhance the Association’s outreach to the U.S. Intelligence Community and to support intelligence professionals in the government, military and private sector.

AFCEA Intelligence strives to be the premier intelligence association, providing the structure and interactive forum for networking and sharing ideas in order to strengthen the public/private partnership and to advocate for foreign and domestic intelligence in support of improved national security.

AFCEA Intelligence provides intelligence professionals with an association focused on intelligence challenges and opportunities. As part of the extended AFCEA International family, AFCEA Intelligence also provides linkage with an international association with over 32,000 individual members and over 1,900 corporate members highlighting command, control, communications and intelligence...and their interconnectedness.

**Armed Forces Medical Intelligence Center (AFMIC)**

See: National Center for Medical Intelligence (NCMI)
Army Crime Records Center - See: Crime Records Center (US Army - USACIDC)

Army Intelligence and Security Command (INSCOM)
URL: http://www.inscom.army.mil/

Art of Deception: Controlling the Human Element of Security
by: Kevin D. Mitnick & William L. Simon
URL: http://blaeks.com/crtice/Kevin%20Mitnick%20-%20The%20Art%20of%20Deception.pdf
URL: http://www.thehackademy.net/madchat/esprit/textes/The_Art_of_Deception.pdf

Art of Intrusion:
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers
by: Kevin D. Mitnick & William L. Simon

Association of Former Intelligence Officers (AFIO)
URL: http://www.afio.com/

The Association of Former Intelligence Officers (AFIO), formerly known as the Association of Retired Intelligence Officers is a non-profit, non-partisan advocacy organization founded in 1975 by David Atlee Phillips to counter widespread criticism of the United States intelligence community coming from the media and Congress. It is registered with the IRS as a 501(c)(3) tax-exempt charity and sees its primary mission as educational. The AFIO has 5,000 members in 24 active chapters, most of whom are a mix of former or current intelligence officers, academicians, students, and the general public; it is not necessary to be an intelligence officer to be an associate member of AFIO if one supports its principles and abides by its code of ethics.
Association of Old Crows (AOC)

URL: http://www.crows.org/

The Association of Old Crows is a nonprofit international professional organization of about 30,000 members specializing in electronic warfare, tactical information operations, and related topics. The organization's headquarters are located in Alexandria, Virginia. The name "Old Crows" emerged from the first use of electronic warfare in World War II to disrupt Axis communications and radars. Allied equipment and operators were known by the code name "Raven". Common jargon changed the name to "Crows" and those engaged in the profession became known as "Old Crows". The organization draws expertise and information from a pool of thousands of individuals, including technology specialists and actual military personnel. It is involved in advancing electronic warfare and information-gathering techniques, disseminating information on these topics, and supporting the education of personnel in related matters.

--------- B ---------

BATCO

URL: http://www.acompanyacf.co.uk/training-aids/doc_download/276-batco-powerpoint

BATCO, short for Battle Code, is a hand-held, paper-based encryption system used at a low, front line (platoon, troop and section) level in the British Army during the late Cold War period.

A BATCO sheet is composed of a double-sided sheet of about A5 that fits in a specially made BATCO wallet, and is used at unit and formation level. Each single side is usually valid for 24 Hours.

In addition to the code card there is:

- Authentication table
- Callsign Indicator chart
- Spelling box

The use of BATCO is still taught to Royal Signals Communication Systems Operators as a back-up should secure equipment fail or be unavailable. It is also taught to Army Cadets and Combined Cadets as part of the Signal Classification qualification. BATCO documents are classified as "Restricted" information.
BBC Country Profiles
URL: http://news.bbc.co.uk/2/hi/country_profiles/default.stm

Bomb Arson Tracking System
URL: https://www.bats.gov/batsnet/

ATF United States Bomb Data Center
Telephone: 800-461-8841
E-mail: USBDC@atf.gov

The Bomb Arson Tracking System (BATS) is a web-based case management system which provides you, State and local arson & explosives investigators, access to up-to-date arson and explosives investigative data from across the nation. Unlike anything you may currently use, it's not just limited to your local jurisdiction or state. BATS provides you access to national arson and explosives incident information.

Bomb Threat Stand-Off Distances

1. These capacities are based on the maximum weight of explosive material that could reasonably fit in a container of similar size.

2. Personnel in buildings are provided a high degree of protection from death or serious injury; however, glass breakage and building debris may still cause some injuries. Un-strengthened buildings can be expected to sustain damage that approximates five percent of their replacement cost.

3. If personnel cannot enter a building to seek shelter they must evacuate to the minimum distance recommended by Outdoor Evacuation Distance. The distance is governed by the greater hazard of fragmentation distance, glass breakage or threshold for ear drum rupture.
### Brain - Mind Mapping & Brainstorming Software

**URL:**  [http://www.thebrain.com/](http://www.thebrain.com/)

Includes a free application for personal use.

### Bump Fire

Bump firing is a method of using the recoil of a semi-automatic firearm to fire multiple shots in rapid succession, simulating the effect of a fully-automatic firearm. Bump firing technique involves pushing the firearm forward to contact the trigger finger while keeping the trigger finger itself stationary. The recoil of the firearm, combined with forward pressure by the operator, causes it to rapidly recoil off the operator's stationary trigger finger resulting in very rapid semi-automatic fire.
Bump Key

URL: http://www.aloa.org/pdf/bkpressroom.pdf

Bump keys are lock picking tools that are commonly used to open pin tumbler locks. Pin tumbler locks are those locks that use pins of varying length to prevent the lock opening unless the proper key is inserted into the lock and turned. Pin tumbler locks are usually used in cylinder locks but can also be used in other locks. They are the types of locks that you usually find in a standard front door, making bump keys a serious security hazard.

Bump keys are simply blank keys. They are mostly different for different brands of lock, but the general shape of it is the same. Bump keys are filed down so that their cuts are all at their maximum depth.

A bump key works by pushing the pins in a pin tumbler lock up for a split second every time you "bump" the blank key into the lock. In the split second where they have been bumped up you can turn the lock a bit. Therefore, with a couple of bumps you will be able to turn the lock the whole way around and unlock it, even though you don't have the proper key.

(http://www.ehow.com/way_5724385_bump-key-tutorial.html)

Bureau of Diplomatic Security - Diplomatic Security Service

As the Department of State's security and law enforcement arm, the Bureau of Diplomatic Security plays an essential yet behind-the-scenes role: To provide a safe and secure environment for the conduct of U.S. foreign policy. Not only is Diplomatic Security a unique organization in
the foreign affairs community--it is the only law enforcement agency with representation in nearly every country in the world.

Diplomatic Security has offices throughout the United States staffed with special agents and contract investigators. These agents form the backbone of DS's investigative mission, conducting criminal, counterterrorism, and background investigations. Agents assigned to field and resident offices assist in providing support to the protection of the Secretary of State, the U.S. Ambassador to the United Nations, and visiting foreign dignitaries. In addition, they are charged with security support for resident foreign diplomats and assistance to the private sector through the Overseas Security Advisory Council. Liaison with federal and local law enforcement, foreign mission personnel, local officials, and the private sector complements their major responsibilities. DS Investigative Field Offices http://www.state.gov/m/ds/rls/rpt/18892.htm

Bureau of Intelligence and Research | US Department of State

URL: http://www.state.gov/s/inr/

--------- C ---------

CARVER - A special operations forces acronym used throughout the targeting and mission planning cycle to assess mission validity and requirements. The acronym stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability.

CARVER Software - Center for Infrastructure Expertise

http://www.ni2cie.org/default.asp

The NI2 Center for Infrastructure Expertise is a not-for-profit applied research group that is currently funded under a grant from the National Institute of Standards & Technology (NIST). The mission of the Center is to help ensure that our nation’s built critical infrastructures and key resources can meet the security threats of the 21st century. The Center works in partnership with federal state, and local government agencies, as well as private industry and non-government organizations, to develop and apply best practices, creative ideas, and cost-efficient solutions to protect our nation’s built critical infrastructure from terrorist attacks and other catastrophic events.
events. To accomplish this, the Center focuses on testing and implementing practical applications rather than theoretical models.

Free CARVER Software

The Center has developed CARVER2, a free software tool that provides a non-technical method of comparing and ranking critical infrastructure and key resources. It is the only assessment tool that ranks critical infrastructure across sectors.

The CARVER2 vulnerability assessment tool is designed to quickly and easily identify and compare potential natural disaster and/or terrorist targets at the local, state and national levels in order to assist government officials in the allocation of protective resources.

The CARVER2 target analysis tool is available free of charge to federal, state, and local government officials and agencies, as well as non-profit and educational institutions. See below to request the installation package.

http://www.ni2cie.org/CARVER2.asp

CARVER + Shock Software - Food and Drug Administration (FDA)

URL:  http://www.fda.gov/Food/FoodDefense/CARVER/default.htm

CARVER+Shock is an offensive targeting prioritization tool adapted from the military version (CARVER) for use in the food industry. The tool can be used to assess the vulnerabilities within a system or infrastructure to an attack. It allows the user to think like an attacker to identify the most attractive targets for an attack. By conducting a CARVER + Shock assessment of a food production facility or process, the user can determine the most vulnerable points in their infrastructure, and focus resources on protecting the most susceptible points in their system.

This software tool represents the Agency's (FDA) current thinking on the kinds of vulnerabilities that food establishments may encounter and some measures to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. The accuracy of these vulnerabilities cannot be guaranteed for all food establishments without proper validation studies. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public and should be considered educational in use. Not all of the vulnerabilities portrayed in this software tool may be appropriate for every food establishment, particularly smaller facilities and distributors. FDA recommends that operators review the material in each section that relates to a component of their operation, and assess which are suitable. These educational examples should not be regarded as minimum standards. Nor should the examples provided be considered an inclusive list of all potential vulnerabilities and approaches to achieving the goal. FDA recommends that operators consider their
vulnerabilities, the goal of the preventive measures, assess whether the goal is relevant to their operation, and, if it is, design an approach that is both efficient and effective to accomplish the goal under their conditions of operation.

**Center for Advanced Operational Culture Learning (CAOCL)**


Marine Corps Training and Education Command  
Telephone: 703-432-1504  
Fax: 703-432-1463  
Email: caocladmin@usmc.mil

**Center for Development of Security Excellence (DoD)**

URL: [https://cdsetrain.dtic.mil/](https://cdsetrain.dtic.mil/)

Course Catalog: [http://cdse.dss.mil/seta/courses.html](http://cdse.dss.mil/seta/courses.html)

- **Thwarting the Enemy: Providing Counterintelligence and Threat Awareness to the Defense Industrial Base**  

  This training provides awareness of potential threats directed against U.S. technology, examples of common suspicious activities, and emphasis reporting requirements under NISPOM 1-302.

  The course includes a printable certificate which can serve as evidence that a student completed the course. When a student takes the course using this link, DSS will not maintain any record of that student by name or any personally identifiable information. If the student needs documentation that he or she has completed the course he or she will have to print the certificate at the end of the course. The training will take approximately 35-40 minutes to complete.

- **OPSEC Awareness for Military Members, DoD Employees and Contractors**  
This is an interactive web-based course that provides OPSEC awareness for military members, government employees, contractors and dependents. The course provides information on the basic need to protect unclassified information about operations and personal information to ensure safe and successful operations and personal safety.

The course includes a printable certificate which can serve as evidence that a student completed the course. When a student takes the course using this link, DSS will not maintain any record of that student by name or any personally identifiable information. If the student needs documentation that he or she has completed the course he or she will have to print the certificate at the end of the course. This training will take approximately 45 minutes to complete.

Center for Homeland Defense and Security

URL:  http://www.chds.us/

The Center for Homeland Defense and Security (CHDS) is located at the Naval Postgraduate School in Monterey, CA. Since 2002, CHDS has conducted a wide range of programs focused on assisting current and future leaders in Homeland Defense and Security to develop the policies, strategies, programs and organizational elements needed to defeat terrorism in the United States. The programs are developed in partnership with and are sponsored by the National Preparedness Directorate, FEMA.

All CHDS programs are focused on leadership development to enable the United States to win the war on terrorism. Through graduate- and executive-level coursework, seminars, and research, homeland security leaders gain the analytic skills and substantive expertise they need to counter terrorism. The programs also prepare leaders to bridge gaps in interagency and civil-military cooperation by bringing together a diverse range of participants to share perspectives and lay the foundation for long-term homeland security collaboration.

Mission

To strengthen the national security of the United States by providing graduate level educational programs and services that meet the immediate and long-term leadership needs of organizations responsible for homeland defense and security.

Vision
The Center will become the nation's leading educational institution for the innovation and refinement of highly relevant curricula, the creation of depositories of applicable knowledge and the national center for the distribution, transfer and exchange of homeland defense and security information and educational products.

**Program Goals**

Strengthen national capacity for homeland security by advancing the study of homeland security as a substantive field of research, scholarship, and professional discipline.

Create a “multiplier effect” to maximize federal investment—share program content, research results, and educational resources with organizations across the nation to build national homeland security preparedness through education.

**Self-study Courses in Homeland Security**

The Naval Postgraduate School Center for Homeland Defense and Security offers non-credit, self-study courses online. These courses are developed by the NPS CHDS teaching faculty and are derived from course content (lecture material and course readings) from the Center's homeland security master's degree curriculum. The courses, offered at no cost, are designed for homeland defense and security professionals who wish to enhance their understanding of key homeland security concepts and require the flexibility of self-paced instruction. NPS does not provide graduate credit for the courses; however, participants are encouraged to check with their professional associations regarding continuing education units/credits. Upon completing each course, participants can download a record of completion.

Five Courses Currently Available:

- Intelligence for Homeland Security: Organizational and Policy Challenges
- Homeland Security in Israel
- The Global Jihadi Threat
- Critical Infrastructure: Vulnerability Analysis and Protection
- Technology for Homeland Security: Inspection and Detection Technologies

**Center for Intelligence Studies**

URL:  [http://www.centerforintelligencestudies.org/](http://www.centerforintelligencestudies.org/)

The Center for Intelligence Studies was formally chartered on March 1, 1988 as a non-partisan public policy institution dedicated to the research and dissemination of substantive information regarding the threat posed by foreign intelligence services to the United States, and the proper
role, scope, and function of America's national intelligence services in protecting the national security.

**Center for International and Security Studies at Maryland**

URL:  [http://www.cissm.umd.edu/](http://www.cissm.umd.edu/)

4113 Van Munching Hall, School of Public Policy
University of Maryland
College Park, MD 20742
Telephone: 301-405-7601

**Central Intelligence Agency (CIA)**

URL:  [https://www.cia.gov/](https://www.cia.gov/)

Office of Public Affairs
Washington, D.C. 20505
Telephone: 703-482-0623
Fax: 703-482-1739


CIA YouTube Channel - [http://www.youtube.com/user/ciagov](http://www.youtube.com/user/ciagov)


Centre for Counterintelligence and Security Studies (CI CENTRE)

URL:  http://www.cicentre.com/

PO Box 11221
Alexandria, VA 22312
Telephone: 703-642-7450 / 1-800-779-4007
Fax: 703-642-7451

Centre for the Protection of National Infrastructure (UK)

URL:  http://www.cpni.gov.uk/default.aspx

CPNI was formed from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC). Although CPNI was only formed on 1 February 2007, providing security advice has always been part of government strategy to disrupt threats to national security. Our advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK’s essential services (delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors) safer.

Certified in National Threat Analysis, CNTA

URL:  http://www.abchs.com/certificate/cnta.php

With the ever-growing threat of terrorism abroad and at home, the Certified in National Threat Analysis, CNTA credential is designed to bring together terrorism experts with homeland security professionals to teach the intricacies of the international terror network. This comprehensive program will provide the tools and knowledge to identify and analyze terrorist threats in a variety of settings and applications.

*This certification is completed by combining one required and four elective modules.
Challenge of Domestic Intelligence in a Free Society
A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency

by: Brian A. Jackson (Editor)

URL:  http://www.rand.org/pubs/monographs/MG804.html

Whether U.S. terrorism-prevention efforts match the threat continues to be central in policy debate. Part of this debate is whether the United States needs a dedicated domestic counterterrorism intelligence agency. To inform future policy decision making, this book examines, from a variety of perspectives, the policy proposal that such an agency be created. These include its possible capabilities, comparing its potential effectiveness with that of current efforts, and its acceptability to the public, as well as various balances and trade-offs involved in creating such an agency. Reflecting the limits in the data available and the significant uncertainty associated with this policy area, if there is a unifying message from the study, it is one of caution and deliberation. In an area in which direct assessment and analysis are limited, there is a need to carefully consider the implications and potential outcomes of such significant policy changes. In doing so, examination from different perspectives and through different approaches — to ideally capture a sufficient picture of the complexity to see not just the benefits we hope to gain from policy change but the layers of effects and interactions that could either help or hurt the chances of those benefits appearing — is a critical ingredient of policy deliberation and design.

CIA World Factbook

URL:  https://www.cia.gov/library/publications/the-world-factbook/

Clandestine Radio

URL:  http://www.clandestineradio.com/

ClandestineRadio.com is the only online portal dedicated to the study of clandestine and subversive radio - a field where politics, diplomacy, espionage and broadcast media collide. Clandestine broadcasting is a highly effective weapon in the arsenal of psychological warfare, which, when analyzed, can assist observers to cut through the fog of war and ascertain the strength and capabilities of opposition groups as well as actual on-the-ground military strategies. For the casual Web surfer this site may seem exotic and, at times, conspiratorial. Regular and "professional" users, however, will find an intelligence bonanza.
Al Qaeda newscast video, Voice of the Caliphate, circa 2005

Launched in 1996 ClandestineRadio.com has developed into a resource regularly used by radio monitors, academics and historians, journalists, and military and intelligence analysts to track psywar developments across the globe. We have been featured in The Wall Street Journal, Washington Post, Christian Science Monitor, US News & World Report, and on BBC, Fox News, ABC, NBC, CBS, NPR, CBC, and numerous international media outlets. Issues of our bi-weekly Clandestine Radio Watch reports are included in the digital archives of the U.S. Library of Congress, and Washington, DC's Newseum, which re-opens in 2006, will feature excerpts of our sound library in its permanent exhibits. Global Crisis Watch, our news podcast, launched in May 2005.

ClandestineRadio.com is a non-partisan and international project headquartered in Washington, DC, and Germany with principal correspondents in North America, Europe, Africa and Asia. Media inquiries are welcome.

**Clandestine Radio Equipment**


**Clandestine Radio Links**


**COLISEUM**  See: Community On-Line Intelligence System for End-Users and Managers

**Columbia University - U.S. Intelligence Community: Information Resources**

URL:  [http://library.columbia.edu/indiv/lehman/guides/intell.html](http://library.columbia.edu/indiv/lehman/guides/intell.html)
Combating Terrorism Center at West Point

URL:  [http://www.ctc.usma.edu/](http://www.ctc.usma.edu/)

Situated at the nexus of theory and practice, the Combating Terrorism Center serves as an important national resource that rigorously studies the terrorist threat and provides policy-relevant research while moving the boundaries of academic knowledge. The CTC’s distinguished scholars, international network of experts, and access to senior U.S. government leadership set it apart from any other like enterprise.

Combating Terrorism Technology Support Office

URL:  [http://www.cttso.gov/](http://www.cttso.gov/)

CTTSO fields rapid combating terrorism solutions to meet continually evolving requirements defined by end users. Working closely with over 100 Government agencies, State, and local government, law enforcement organizations, and national first responders, CTTSO leverages technical expertise, operational objectives, and interagency sponsor funding. This collective approach to resource and information sharing positions the CTTSO to gather front line requirements that service multiple users — a distinct advantage in the combating terrorism community.
Combating Trafficking in Persons

URL:  http://ctip.defense.gov/

Common Competencies for State, Local, and Tribal Intelligence Analysts

URL: http://it.ojp.gov/docdownloader.aspx?ddid=1296

Identifies common analytic competencies that should be exhibited by state, local, and tribal intelligence analysts working in state or major urban area fusion centers or similar analytic law enforcement entities. These competencies are essential for analysts to effectively perform their job duties and are required in their unique operating environments.

Community On-Line Intelligence System for End-Users and Managers (COLISEUM)

URL: http://www.globalsecurity.org/intell/systems/coliseum.htm

The Community On-Line Intelligence System for End-Users and Managers (COLISEUM) is a Defense Intelligence Agency (DIA) automated production/requirements management system. It provides the mechanism for registering and validating requirements, deconfliction of requirements, assigning and scheduling production, and provides the capability to track and manage overall production activities across operational and national planners and consumers.

COLISEUM is a database application designed to support the national intelligence community for registration, validation, tracking and management of Production Requirements (PRs). It provides a user-friendly "point and click" mechanism for scheduling, deconflicting, and assigning production assets. Most importantly, it provides the capability to track and manage overall production activities across operational and national planners. COLISEUM is designed to function as an application under the JDISS Program, which provides additional connectivity and interoperability with other intelligence systems. Read-only access is now also available through Intelink TS.

COLISEUM is installed at all unified commands, military services, DOD production centers, DIA, Central Intelligence Agency (CIA), National Security Agency (NSA), National Military Joint Intelligence Centers, and national support teams. As of October 1996 more than 1,684 intelligence community users had access to COLISEUM, with more than 5000 requirements registered with another 5000 Intel products scheduled for production.

Compendium of Analytic Tradecraft Notes
Central Intelligence Agency- Directorate of Intelligence

URL: http://clark.cam.muskingum.edu/analysis_folder/di_catn_Folder/contents.htm
Computational Analysis of Social and Organizational Systems

URL:  http://www.casos.cs.cmu.edu/projects/ora/

ORA is a dynamic meta-network assessment and analysis tool developed by CASOS at Carnegie Mellon. It contains hundreds of social network, dynamic network metrics, trail metrics, procedures for grouping nodes, identifying local patterns, comparing and contrasting networks, groups, and individuals from a dynamic meta-network perspective. *ORA has been used to examine how networks change through space and time, contains procedures for moving back and forth between trail data (e.g. who was where when) and network data (who is connected to whom, who is connected to where …), and has a variety of geo-spatial network metrics, and change detection techniques. *ORA can handle multi-mode, multi-plex, multi-level networks. It can identify key players, groups and vulnerabilities, model network changes over time, and perform COA analysis. It has been tested with large networks (106 nodes per 5 entity classes). Distance based, algorithmic, and statistical procedures for comparing and contrasting networks are part of this toolkit.

Based on network theory, social psychology, operations research, and management theory a series of measures of “criticality” have been developed at CMU. Just as critical path algorithms can be used to locate those tasks that are critical from a project management perspective, the *ORA algorithms can find those people, types of skills or knowledge and tasks that are critical from a performance and information security perspective. Each of the measures we have developed are calculated by *ORA on the basis of network data like that in the following table.

ORA can be applied both within a traditional organization or on covert networks.

Applying *ORA to an organization, key actors who by virtue of who they know, what they know, and what they are doing are potential risks to the security of a company can be determined. Applying *ORA to a covert network, key actors whose removal will damage the adaptability or performance of the covert network can be determined. A critical feature that is currently being built is a “sensitivity” indicator for each threat metric which estimates, given the level of accuracy of the underlying network, how sure we can be that the person identified as key really is key.

Computer Online Forensic Evidence Extractor

URL:  https://cofee.nw3c.org/

Microsoft COFEE is being made available to individuals employed by law enforcement agencies within the United States and Canada. COFEE means the Computer Online Forensic Evidence
Extractor tool that fits on a USB drive and automates the execution of commands for data extraction and related documentation. Distribution is limited to law enforcement agencies. Access to the COFEE product requires verification of employment with a law enforcement agency and agreement to the terms and conditions of the Microsoft/NW3C Sublicense Agreement.

The verification process is automated if you have an email account with RISS.NET or LEO.GOV, or have an account with NW3C.

**Computer Security Evaluation Tool**

URL: [http://www.us-cert.gov/control_systems/satool.html](http://www.us-cert.gov/control_systems/satool.html)

The Department of Homeland Security (DHS) has released its latest cyber system assessment tool to the Critical Infrastructure/Key Resources (CI/KR) community. The Computer Security Evaluation Tool (CSET) is a desktop software tool that guides users through a step-by-step process to evaluate their cyber systems and network security practices against recognized industry standards.

According to DHS, the benefits of CSET include:

- Contributing to an organization's risk management and decision-making process;
- Raising awareness and facilitating discussion on cyber security within the organization;
- Highlighting vulnerabilities in the organization's systems and providing recommendations on ways to address those vulnerabilities;
- Identifying areas of strength and best practices being followed in the organization;
- Providing a method to systematically compare and monitor improvement in the cyber systems; and
- Providing a common industry-wide tool for assessing cyber systems.

**Conflict Analysis - Certificate Course**


Academics and professionals in the field of conflict management face extraordinary challenges in dealing with the various phases of conflict, whether it is rebuilding in the aftermath, stopping conflict in progress, or preventing conflict before it begins.
In these efforts, successful educators and practitioners follow a simple precept: effective action depends upon insightful analysis.

This course presents an introduction to the subject of conflict analysis, illustrating analytical tools used, with reference to two extended case studies, the conflict in Kosovo and the genocide in Rwanda.

Certificate of Completion: Yes
Cost: No charge
In completing this course, you will gain proficiency in the following skills:

- Classifying phases of conflict using the curve of conflict
- Identifying interventions appropriate to different phases of a conflict
- Analyzing the conflict in Kosovo and the genocide in Rwanda using terms and concepts from the curve of conflict
- Generating a thorough set of characteristics for describing conflict using an analytical framework
- Analyzing the conflict in Kosovo and the genocide in Rwanda using terms and concepts from the framework
- Analyzing unfamiliar conflicts using terms and concepts from the curve and framework

**Consumer Sentinel**

URL: [http://www.ftc.gov/sentinel/index.shtm](http://www.ftc.gov/sentinel/index.shtm)

Consumer Sentinel is the unique investigative cyber tool that provides members of the Consumer Sentinel Network with access to millions of consumer complaints. Consumer Sentinel includes complaints about:

- Identity Theft
- Do-Not-Call Registry violations
- Computers, the Internet, and Online Auctions
- Telemarketing Scams -- Advance-fee Loans and Credit Scams
- Sweepstakes, Lotteries, and Prizes
- Business Opportunities and Work-at-Home Schemes
- Health and Weight Loss Products
- Debt Collection, Credit Reports, and Financial Matters

Consumer Sentinel is based on the premise that sharing information can make law enforcement even more effective. To that end, the Consumer Sentinel Network provides law enforcement
members with access to complaints provided directly to the Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.

**Controlled Unclassified Information (CUI)**

URL: [http://www.archives.gov/cui/](http://www.archives.gov/cui/)

Executive Order 13556 “Controlled Unclassified Information,” (the Order), issued on November 4, 2010, established the CUI program, which is a system that standardizes and simplifies the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. The program emphasizes the openness and uniformity of government-wide practices. Its purpose is to address the current inefficient and confusing patchwork that leads to inconsistent marking and safeguarding as well as restrictive dissemination policies, which are often hidden from public view. The President has designated the National Archives and Records Administration (NARA) as the CUI Executive Agent (EA). In this role, NARA has the authority and responsibility to oversee and manage the implementation of the CUI program and will issue policy directives and publish reports on the status of agency implementation.

**Counterinsurgency**

**Counterinsurgency (FM 3-24 / MCWP 3-33.5)**


**Counterinsurgency Guide (U.S. Government) January 2009**

URL: [http://www.state.gov/documents/organization/119629.pdf](http://www.state.gov/documents/organization/119629.pdf)

**Counterinsurgency Operations (JP 3-24, 5 OCT 2009)**


**Counterintelligence**

**Counterintelligence (FM 34-60) October 1995**

URL: [http://www.fas.org/irp/doddir/army/fm34-60/](http://www.fas.org/irp/doddir/army/fm34-60/)
Counterintelligence Field Activity (CIFA)

URL: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/index.htm

A highly secret office located within the Department of Defense (DoD), the Counterintelligence Field Activity (CIFA) was charged with protecting US military personnel and facilities against spying and acts of terrorism. CIFA’s primary mission was to identify and track down suspected terrorists.

The Counterintelligence Field Activity (CIFA), also known for a time as the Joint Counterintelligence Assessment Group (JCAG), was established by Department of Defense Directive 5105.67 in February 2002. A Defense Department background paper traces CIFA's origins to Presidential Decision Directive (PDD)- 75, "U.S. Counterintelligence Effectiveness - Counterintelligence for the 21st Century," signed by President William Clinton on January 5, 2001. PDD-75 called for a predictive and proactive counterintelligence (CI) system with integrated oversight of counterintelligence issues across national security agencies.

CIFA's functions, according to the February 2002 directive were to include:

- evaluating DoD counterintelligence activities to determine the extent to which counterintelligence policies and resources adequately protect the Defense Department against the threats of "espionage, terrorism, sabotage, assassination, and other covert or clandestine activities, including those of foreign intelligence services,"
- providing counterintelligence threat assessments, advisories, and risk assessments to the heads of DoD components,
- providing "tailored analytical and data-mining support" to DoD counterintelligence field elements and activities,
• conducting "Domestic Threat Analyses and Risk Assessments," and identifying and tracking "technologies requiring protection."

In 2005 CIFA's authority was expanded when it received mission tasking authority (MTA) over the counterintelligence organizations of the military departments, such as the Air Force Office of Special Investigations and the counterintelligence components of Defense Department agencies. An even more extensive expansion of CIFA's authority had been proposed earlier that year by The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, also known as the Robb-Silberman Commission. The Commission suggested that CIFA "should have operational and investigative authority to coordinate and conduct counterintelligence activities throughout the Defense Department."

After consultations with the National Security Council staff members responsible for implementing the Commission's recommendations, the Defense Department expanded CIFA's authority, but not to the extent suggested by the Commission. The tasking authority assigned to CIFA does not allow it to conduct counterintelligence agencies throughout the Defense Department but allows it to task any military department or DoD agency counterintelligence component to "execute a specific CI mission or conduct a CI function within that organization's charter."

CIFA had about 400 full-time employees and provided work for 800-900 contractor personnel. In August 2008 CIFA'S activities were folded into the Defense Intelligence Agency (DIA).

Counterintelligence Glossary (2 May 2011)
Terms & Definitions of Interest for DOD Counterintelligence Professionals

Office of Counterintelligence
Defense CI & HUMINT Center


Counter-Terrorism Operations Support (CTOS)
U.S. Department of Energy's Nevada Test Site (NTS)

URL:  http://www.ctosnnsa.org/

The Counter Terrorism Operations Support (CTOS) Program at the NNSS develops and delivers the training for emergency first responders. This training prepares the responders to take immediate, decisive action to prevent or mitigate terrorist use of radiological or nuclear WMDs, such as Improvised Nuclear Devices (INDs) and Radiological Dispersal Devices (RDDs or “dirty bombs”).

Country Reports on Terrorism 2010

URL:  https://www.hSDL.org/?view&did=684974

"U.S. law requires the Secretary of State to provide Congress, by April 30 of each year, a full and complete report on terrorism with regard to those countries and groups meeting criteria set forth in the legislation. This annual report is entitled Country Reports on Terrorism. Beginning with the report for 2004, it replaced the previously published Patterns of Global Terrorism. […] Al-Qa'ida (AQ) remained the preeminent terrorist threat to the United States in 2010. Though the AQ core in Pakistan has become weaker, it retained the capability to conduct regional and transnational attacks. Cooperation between AQ and Afghanistan- and Pakistan-based militants was critical to the threat the group posed. In addition, the danger posed by Lashkar-e Tayyiba (LeT) and increased resource-sharing between AQ and its Pakistan-based allies and associates such as Tehrik-e Taliban Pakistan (TTP) and the Haqqani Network meant the aggregate threat in South Asia remained high."

Country Studies

See:

- CIA World Factbook
- BBC Country Profiles
- Economist Intelligence Unit
- Library of Congress - Country Studies
- Marine Corps Intelligence Activity - Country handbooks
- U.S. Department of State - Countries & Regions
- World-Check
- World Health Organization - Country Profiles
- World News Connection
Crime Records Center (US Army - USACIDC)

URL:  http://www.cid.army.mil/crc.html

The U.S. Army Crime Records Center is co-located with the USACIDC Headquarters at Fort Belvoir Virginia. The CRC is a multi-functional center, supporting not only the Army and the command, but also foreign, federal, state and local law enforcement agencies.

The CRC receives, safeguards, maintains and disseminates information from Army law enforcement records. The center has accumulated more than 2.5 million reports. It also serves as CID's Freedom of Information and Privacy Act authority and annually responds to more than 2,000 requests for information. Another major function of the center is to manage the Army law enforcement Polygraph Program.

The CRC director is Mr. Phillip McGuire.

Email address: CRCFOIAPA@conus.army.mil

Mailing Address:
Director U.S. Army Crime Records Center USACIDC
U.S. Army Criminal Investigation Command
U.S. Army Crime Records Center
ATTN: CICR-FP
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134-2253
CrimeStat III
URL: http://www.icpsr.umich.edu/CrimeStat/

CrimeStat III is a spatial statistics program for the analysis of crime incident locations, developed by Ned Levine & Associates under the direction of Ned Levine, PhD, that was funded by grants from the National Institute of Justice. The program is Windows-based and interfaces with most desktop GIS programs. The purpose is to provide supplemental statistical tools to aid law enforcement agencies and criminal justice researchers in their crime mapping efforts. CrimeStat is being used by many police departments around the country as well as by criminal justice and other researchers. The latest version is 3.3.

The program inputs incident locations (e.g., robbery locations) in 'dbf', 'shp', ASCII or ODBC-compliant formats using either spherical or projected coordinates. It calculates various spatial statistics and writes graphical objects to ArcGIS®, MapInfo®, Surfer for Windows®, and other GIS packages.

Criminal Intelligence File Guidelines

These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity.

Criminal Intelligence Resources Guide (June 2011)
Criminal Intelligence Systems Operating Policies (28 CFR Part 23)

http://www.ncirc.gov/28cfr/

28 Code of Federal Regulations (CFR) Part 23 was developed to ensure the protection of the constitutional and privacy rights of individuals during the collection and exchange of criminal intelligence information. The standards in 28 CFR Part 23 apply to all criminal intelligence systems operating under funding from the Omnibus Crime Control and Safe Streets Act of 1968, as amended. This online training is an introductory-level training on the regulation's core principles, which provide an understanding of privacy and civil liberties concerns related to criminal intelligence information sharing.

Critical Thinking

Critical Thinking Handbook
by: Michael O'Rourke
Under the auspices of the UI Critical Thinking Advisory Committee
© 2005 University of Idaho

URL: http://www.class.uidaho.edu/crit_think/

Critical Thinking and Intelligence Analysis
by: David T. Moore


Critical Thinking Strategies (Anacapa On-line Course)


Crypto-Gram Newsletter

URL: http://www.schneier.com/crypto-gram.html

Crypto-Gram is a free monthly e-mail newsletter from security expert Bruce Schneier. Each issue is filled with interesting commentary, pointed critique, and serious debate about security. As head curmudgeon at the table, Schneier explains, debunks, and draws lessons from security stories that make the news. After nine years of publication and with 125,000 readers, Crypto-Gram is the most popular and influential publication on security technology.
CyberCop

URL:  http://www.cybercopportal.org/

Member Log-in --  https://cybercop.esportals.com/

The CyberCop Portal is designed to bridge system stovepipes between organizations by providing a separate means to collaborate over the web using the security controls necessary to handle sensitive but unclassified law enforcement information. The CyberCop Portal created and hosted by The ESP Group, is entirely Web-based, meaning that no additional software clients need to be downloaded onto users' machines. That allows CyberCop users to enter the portal from any machine, anywhere. The Portal allows users to share libraries of documents and case studies, send secure e-mail, participate in ongoing threaded discussions, create and distribute surveys and share online briefings. The Cybercop mission is to provide individuals an ultra-secure web-based environment to promote and facilitate the sharing of sensitive information among a cohesive network of cyber security, law enforcement, first responders, homeland defense and law enforcement related professionals from all levels of government; international, federal, state, local and the private sector, regardless of department affiliation and jurisdictional boundaries. CyberCop is committed to providing a safe and secure environment where ideas can be freely exchanged to aid individual efforts and foster cooperative efforts in the fight against crime, terrorism and the security of our homeland.

---------- D ----------

DAIIS  -  Department of the Army Intelligence Information Service

Data Ferrett

URL:  http://dataferrett.census.gov/

DataFerrett is a unique data mining and extraction tool. DataFerrett allows you to select a databasket full of variables and then recode those variables as you need. You can then develop and customize tables. Selecting your results in your table you can create a chart or graph for a visual presentation into an html page. Save your data in the databasket and save your table for continued reuse. DataFerrett helps you locate and retrieve the data you need across the Internet to
your desktop or system, regardless of where the data resides. DataFerrett: lets you receive data in the form in which you need it (whether it be extracted to an ascii, SAS, SPSS, Excel/Access file); or lets you move seamlessly between query, analysis, and visualization of data in one package; lets data providers share their data easier, and manage their own online data.

**Data Wrangler**

URL: [http://vis.stanford.edu/wrangler/](http://vis.stanford.edu/wrangler/)

Data Wrangler is an interactive tool for data cleaning and transformation.

Too much time is spent manipulating data just to get analysis and visualization tools to read it. Wrangler is designed to accelerate this process: spend less time fighting with your data and more time learning from it.

Wrangler allows interactive transformation of messy, real-world data into the data tables analysis tools expect. Export data for use in Excel, R, Tableau, Protovis, ...

**DEA** - See: Drug Enforcement Administration

**DECMAT – Decision Matrix Software**

URL: [http://www.dcswift.com/military/software.html](http://www.dcswift.com/military/software.html)

**Decrypto 8.5**

URL: [http://www.blisstonia.com/software/WebDecrypto/](http://www.blisstonia.com/software/WebDecrypto/)

Decrypto is a fast and automated cryptogram solver by Edwin Olson. It can decode word games often found in newspapers, including puzzles like cryptoquips and patristocrats. You can also download a stand-alone version. [We have also found this program useful for quickly breaking simple substitution ciphers used by some criminal gangs.]
Defense Advanced Research Projects Agency (DARPA)


3701 North Fairfax Drive
Arlington, VA 22203
DARPA General Information 703-526-6630
DARPA Staff Locator 703-526-6624
Director's Office 703-696-2400

DARPA is the research and development office for the U.S. Department of Defense. DARPA’s mission is to maintain technological superiority of the U.S. military and prevent technological surprise from harming our national security. We also create technological surprise for our adversaries. DARPA’s Operational Liaisons serve as points of contact for the Military Services. Service members with technical questions or needs are encouraged to contact a liaison or program manager.

DARPA’s Operational Liaisons serve as points of contact for the Military Services. Service members with technical questions or needs are encouraged to contact a liaison or program manager.

Army: COL Valerie Jacocks 571-218-4349
Navy: CAPT John Murphy 571-218-4590
Air Force: Lt Col Tony Bauernfeind 703-696-6619
Marines: Col Thomas C. Moore 571-218-4387
National Geospatial-Intelligence Agency: Mr. Fred Schnarre 571-218-4597

In addition, DARPA has a representative located at the U.S. Special Operations Command (USSOCOM): Ms. Kathy MacDonald 813-828-9366

The Operational Liaisons may also be contacted via SIPRNET at [username]@darpa.smil.mil.
DSN: 696 numbers-426 plus last 4 digits. All others-426-4469, then last 4 digits

Defense Human Resources Activity (DHRA)
Antiterrorism and Force Protection (ATFP)

URL:  http://www.dhra.mil/website/headquarters/info/hqInfo_atfp.shtml
Defense Intelligence Agency

URL:  http://www.dia.mil/

The Defense Intelligence Agency is a Department of Defense combat support agency and an important member of the United States Intelligence Community. With more than 16,500 military and civilian employees worldwide, DIA is a major producer and manager of foreign military intelligence. We provide military intelligence to warfighters, defense policymakers and force planners, in the Department of Defense and the Intelligence Community, in support of U.S. military planning and operations and weapon systems acquisition.

Defense Language Institute Foreign Language Center

URL:  http://www.dliflc.edu/index.html

The Defense Language Institute Foreign Language Center (DLIFLC) is regarded as one of the finest schools for foreign language instruction in the nation. As part of the Army Training and Doctrine Command (TRADOC), the Institute provides resident instruction at the Presidio of Monterey in 24 languages and several dialects, five days a week, seven hours per day, with two to three hours of homework each night. Courses last between 26 and 64 weeks, depending on the difficulty of the language.

DLIFLC is a multi-service school for active and reserve components, foreign military students, and civilian personnel working in the federal government and various law enforcement agencies.

Defense Language Institute - Headstart-2

URL:  http://hs2.lingnet.org/

Headstart-2 consists of ten modules, each including two Sound and Script and five Military Tasks. Sound and Script teaches the basics of the target language script. Each Military Task focuses on fifteen language drills based on a given topic or theme, such as greetings and introductions, or gathering intelligence. Headstart-2 also features over 100 PDFs with writing drills that provide the user with the opportunity to practice writing the target script. Other features include a writing tool, a sound recorder, a glossary, and cultural resources section. Headstart-2 exposes users to 750 key terms and phrases, and provides them with important communication tools they need in preparation for deployment.
Headstart-2 is available for a growing number of languages, including:

- Chinese (Mandarin)
- Dari
- European Portuguese
- French
- German
- Iraqi
- Korean
- Pashto
- Persian-Farsi
- Russian
- Spanish
- Urdu
- Uzbek

New languages will be added to the menu as they become available.

**Defense Security Service Academy**


The DSS Academy provides security education and training to DoD and other U.S. Government personnel, DoD contractors, and sponsored representatives of foreign governments. Its professional staff of instructors, technology professionals, and education support personnel combine expertise to create, collaborate and facilitate delivery of quality education and training across the security disciplines.

**Defense Threat Reduction Agency**


DTRA is the U.S. Department of Defense’s official Combat Support Agency for countering weapons of mass destruction. Our people are Subject Matter Experts on WMD, and we address
the entire spectrum of chemical, biological, radiological, nuclear and high yield explosive threats. DTRA’s programs include basic science research and development, operational support to U.S. warfighters on the front line, and an in-house WMD think tank that aims to anticipate and mitigate future threats long before they have a chance to harm the United States and our allies. SCC-WMD, the U.S. Strategic Command Center for Combating Weapons of Mass Destruction, synchronizes Combating Weapons of Mass Destruction efforts across our military’s geographic commands and leverages the people, programs and interagency relationships of DTRA at a strategic level. We work with the military services, other elements of the United States government, and countries across the planet on counterproliferation, nonproliferation and WMD reduction issues with one goal in mind: Making the World Safer.

Since DTRA stood up in October 1998 and SCC-WMD in August 2005, the Department of Defense and other federal agencies have increasingly looked to both for support and advice. Both organizations’ responsibilities span the full range of activities necessary to combat and respond to WMD proliferation and use. At home and abroad, DTRA and SCC-WMD deliver mission success against a very real and growing threat.

**Delphi Method: Techniques and Applications**
by: Harold A. Linstone and Murray Turoff, Editors

URL: [http://is.njit.edu/pubs/delphibook/index.html](http://is.njit.edu/pubs/delphibook/index.html)

**Department of the Army Intelligence and Security Programs Oversight and Management**


The Department of the Army Intelligence and Security Programs Oversight and Management Website was developed to support Army security professionals (military, civilian and government contractors) who desire knowledge of Army security programs, policies, reports, databases, related products and services. This site promotes security awareness, enhances the Army security posture by functioning as an army-wide clearinghouse for the dissemination of security-related information and facilitates product and services integration into Army security programs.
Department of the Army Intelligence Information Services (DAIIS)

URL:  https://www.intelink.gov/sharepoint/default.aspx
URL:  https://www.us.army.mil/suite/page/132281

The Department of the Army Intelligence Information Services (DAIIS) has road-mapped the Internet by country. These Country Research Pages are provided as a courtesy to the community. Each page contains hyperlinks to Internet websites that are grouped by categories.

Department of Defense Cyber Crime Center (DC3)

URL:  http://www.dc3.mil/
Commercial - 410-981-1181
Outreach Requests - 410-981-0127
Toll Free - 877-981-3235 DSN - 622-2595

The Department of Defense Cyber Crime Center (DC3) sets standards for digital evidence processing, analysis, and diagnostics for any DoD investigation that requires computer forensic
support to detect, enhance, or recover digital media, including audio and video. The center assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DoD counterintelligence activities. It also supports safety investigations and Inspector General and commander-directed inquiries. DC3 aids in meeting intelligence community document exploitation objectives from a criminal law enforcement forensics and counterintelligence perspective. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DoD members who must ensure Defense information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 remains on the leading edge of computer technologies and techniques through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.

The Defense Cyber Investigations Training Academy (DCITA) develops and delivers cyber investigation training courses for DoD organizations, Defense Criminal Investigative Organizations, military counterintelligence agencies, and law enforcement organizations.

The Academy is the only government organization solely dedicated to cyber investigations training, development, and delivery. Students are trained in the latest digital forensic techniques using state-of-the-art equipment, classrooms, and technologies. DCITA training includes:

- Computer search and seizure techniques
- Network intrusion investigations
- Forensic computer media analysis to support criminal, fraud, and counterintelligence investigations
- Basic and advanced forensic examinations
- Online undercover techniques

DCITA is accredited through the Council of Occupational Education (COE). Recognized by the U.S. Department of Education, COE’s mission is to assure quality training in career and technical development.

**Department of Defense Foreign Clearance Guide**

URL: [https://www.fcg.pentagon.mil/](https://www.fcg.pentagon.mil/)

703-614-0130, 703-614-0225, and 703-614-0259
Department of Homeland Security
URL:  http://www.dhs.gov/index.shtm

DHS Contacts
URL:  http://www.dhs.gov/xutil/contactus.shtm

DHS/FEMA Cyber-Security Training
URL:  http://www.teexwmdcampus.com/index.k2#

DHS/FEMA Certified Cyber-Security Training is designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure.

The 10 courses are offered through three discipline-specific tracks targeting everyday non-technical computer users, technical IT professionals, and business managers and professionals.

These courses are offered at no cost and students earn a DHS/FEMA Certificate of completion along with Continuing Education Units (CEU) at the completion of each course.

IA General / Non-Technical

- AWR-175-W Information Security for Everyone
- AWR-174-W Cyber Ethics
- AWR-168-W Cyber Law and White Collar Crime

IA Technical / IT Professional

- AWR-173-W Information Security Basics
- AWR-178-W Secure Software
- AWR-138-W Network Assurance
- AWR-139-W Digital Forensics Basics

IA for Managers and Business Professionals

- AWR-176_W Business Information Continuity
- AWR-177-W Information Risk Management
- AWR-169-W Cyber Incident Analysis and Report
Directorate of Regional Studies and Education

U.S. Army John F. Kennedy Special Warfare Center and School

URL:  http://www.soc.mil/swcs/organization.html

DRSE produces agile, adaptive and reflective thinking Soldiers while acting as an intellectual repository as well as an incubator of emerging thought and creative ideas in Regional Studies, foreign language, culture, adaptive thinking, leadership, behavioral science and education.

One of the key areas of training is the Foreign Language Initial Acquisition Program, which is second only to the Defense Language Institute in its throughput. Annually, more than 1,500 CA, PO and SF Soldiers go through the program's 17 core languages, which require a minimum of a 1/1 as measured by the two-skill OPI for graduation.

Once Soldiers graduate from training, they continue to have access to language and culture training through the contingency and sustainment language support program, which is a network of satellite training facilities wherever ARSOF are located. The program has as its mission the maintenance of ARSOF operational skills at a minimum of 1/1 up to a 2/2, level of understanding. More than 8,500 students are trained through this program each year.

The directorate's newest initiative is the development of a new series of intermediate language courses starting with Pashto, Dari, Urdu and Arabic-Iraqi languages. The goal of the program is to raise the proficiency of Soldiers with an entrance competency of 1+/1+ to that of a 2/2 as well as to provide a commensurate degree of competency in culture and regional studies. Eventually, this program will include an advanced capability to the 3/3/3 level and include all core languages taught at SWCS.

The foundational program for ARSOF civilian education is the SWCS Associate's Program. The SWCS Associate's Program provides experiential credit for qualification-course completion along with accredited partner-civilian-school select classes to award all qualification course graduates associates degrees, producing academically grounded ARSOF Soldiers to the force. This program primarily addresses entry-level enlisted soldiers.

The intermediate civilian education program is the SWCS Bachelor's Program. The SWCS Bachelor's Program builds on the 60 credit hour associates degree awarded through the SWCS associates program and forwards those credits for full acceptance with SWCS SOCAD partner schools for continuation with select accredited bachelors programs. This 2 + 2 credit concept allows for maximum efficiency and decreases the nonlinear progression of previous degree programs. This program produces operational-level academically credentialed ARSOF Soldiers and the force. This program primarily addresses mid-career enlisted and entry-level warrant officers.
The advanced civilian education program is the SWCS Master's Program. The SWCS Master's Program aligns eligible ARSOF candidates (officer, NCO and warrant officer) with desirable master-level programs producing strategic-level academically credentialed ARSOF Soldiers for the force. The program primarily addresses senior enlisted and mid-career level officers and warrant officers.

The SWCS Permanent Professorship Program provides terminal degree (doctorate) level SWCS cadre to provide academic credentialing and interaction with civilian academia, modeled after the USMA Professor Program.

**Discovery and Dissemination or Retrieval of Information within the Intelligence Community.**


**DNA Initiative**


The President’s DNA Initiative provides funding, training, and assistance to ensure that forensic DNA reaches its full potential to solve crimes, protect the innocent, and identify missing persons. The web-site offers extensive information, including free on-line training.

**Doctrine Networked Education & Training (DOCNET)**


Drawn directly from joint publications without interpretation, each DOCNET course represents an authoritative source of information for use by the Armed Forces of the United States and other Government professionals who require joint doctrine knowledge. DOCNET can be used as an information source, to supplement Professional Military Education, or for college credit.

**Domestic Extremism Lexicon**

Domestic Intelligence in a Free Society

URL: http://www.rand.org/pubs/monographs/MG804.html

Drug Enforcement Administration (DEA)

URL: http://www.justice.gov/dea/index.htm

Mailstop: AES
8701 Morrissette Drive
Springfield, VA 22152

DEA Field Offices

URL: http://www.usdoj.gov/dea/agency/domestic.htm

The DEA has 227 Domestic Offices in 21 Divisions throughout the U.S. and 87 Foreign Offices in 63 countries.

DRYAD Numeral Cipher/Authentication System (KTC 1400D)

URL: http://en.wikipedia.org/wiki/DRYAD
The DRYAD Numeral Cipher/Authentication System (KTC 1400 D) is a simple, paper cryptographic system currently in use by the U.S. military for authentication and for encryption of short, numerical messages. Every unit with a radio is given a set of DRYAD code sheets. A single sheet is valid for a limited time (e.g. 6 hours), called a crypto-period.

A DRYAD code sheet contains 25 lines or rows indexed by the letters in a column on the left of the page. Each row contains a random permutation of the letters A through Y. The letters in each row are grouped into 10 columns labeled 0 through 9. The columns under 0, 1, 2 and 5 have more letters than the other digits, which have just two each.

While crude, the DRYAD Numeral Cipher/Authentication System has the advantage of being fast, relatively easy and requires no extra equipment (such as a pencil). The presence of more cipher-text columns under the digits 0, 1, 2 and 5, is intended to make cipher-text frequency analysis more difficult. But much of the security comes from keeping the crypto-period short.

DRYAD can be used in two modes, authentication or encryption.

**Authentication**

For authentication, a challenging station selects a letter at random from the left most column followed by a second (randomly selected) letter in the row of the first chosen letter. The station
being challenged would then authenticate by picking the letter directly below the row and position of the second letter selected.

For example, using the example cipher sheet, Victor could challenge Peggy by transmitting the letters "Alpha" and "Bravo". Peggy’s correct response would then be "Yankee".

Another form used involves selecting the third letter to the right of the second letter chosen by the challenging station (Victor’s "Bravo" letter). Both the directional offset (up, down, left or right) and numeral offset can be different values then the examples given here; but must be agreed upon and understood by both parties before authentication. The offset number can even remain secret between Victor and Peggy creating a Two-factor authentication. Authentication then would require something you have (the DRYAD cipher sheet) and something you know (the secret offset value). Oscar, who is attempting to penetrate the network by posing as Peggy, would both need a copy of the DRYAD cipher sheet as well as knowledge of secret offset value.

One problem presented is that Oscar has a one in 25 chance of guessing the correct response. A solution to this is for Victor to require Peggy to authenticate twice; lowering Oscar’s odds of guessing the correct response to one in 625 possible guesses. The downside to this method is reduced longevity of the current DRYAD page (since the page is getting twice as much use as a single-authentication scheme).

**Encryption**

The second mode is used to encrypt short numeric information (such as map coordinates or a new radio frequency). The coder selects two letters at random. The first selects a row in the current active page. The second letter is used as in the authentication mode, except the adjacent letter to the right is the one selected; and is called the "SET LETTER."

Numbers are enciphered one digit at a time. A cipher-text letter is chosen from the selected row in the column under the plain text digit. If the digit occurs more than once in the number, the coder is instructed to choose a different letter in the same column. All the digits in a single plaintext number are encoded from the same row.
An enhanced MultiSearch tool is now available on DTIC Online

This tool allows you to search across multiple resources, and is even more efficient and easier to use. Features include the ability to automatically repeat a search and have new results emailed to you.

In addition to the DTIC's Technical Reports and a number of Department of Defense databases, MultiSearch queries collections from the Department of Energy, Environmental Protection Agency, Food and Drug Administration, National Aeronautics and Space Administration, National Institutes of Health, National Science Foundation, Department of Agriculture and international collections such as Scitopia, and World Wide Science.

MultiSearch is the ideal tool for saving time and resources for scientists, researchers, engineers, librarians, program managers, students and anyone looking for science, technical, research and engineering information.

----------------- E -----------------

**Economist Intelligence Unit**


The Economist Intelligence Unit is the foremost research and analysis resource in the world. Founded in 1946 as an in-house research unit for The Economist, we now deliver trusted business intelligence and advice to over 1.5 million decision-makers from the world’s leading companies, financial institutions, governments and universities.

The Economist Intelligence Unit provides analysis and forecasts for 187 countries and a Global Forecasting Service for free.

**eCountry Clearance (US Department of State)**

URL: [https://ecc.state.gov](https://ecc.state.gov)
According to 2 FAM 116.1-6(b) all DoS and agencies with a.mil, or .gov email address, as well as ndu.edu, frb.org, or si.edu, must send country clearance requests though eCC. All classified clearance requests will still be sent by cable.

Anyone with a .gov, .mil, ndu.edu, si.edu, or frb.org email address can access eCC. Non-OpenNet and AIDNet users must register prior to accessing eCC.

**Electronic Surveillance Laws**


The Wire and Electronic Communications Interception and Interception of Oral Communications Act (formally known as the “Title III” Wiretap Act, 18 U.S.C §§ 2510-2520), typically requires a court order issued by a judge who must decide that there is probable cause to believe that a crime has been, is being or is about to be committed. Wiretaps can also be ordered in suspected cases of terrorist bombings, hijackings and other violent activities are crimes. The government can wiretap in advance of a crime being perpetrated. Judges seldom deny government requests for wiretap orders.

Electronic surveillance involves the traditional laws on wiretapping--any interception of a telephone transmission by accessing the telephone signal itself--and eavesdropping--listening in on conversations without the consent of the parties.

More recently, states have extended these laws to cover data communications as well as telephone surveillance. For example, in Florida, interception and disclosure of wire, oral, or electronic communications is prohibited. State and federal policymakers face the challenge of balancing security needs via electronic surveillance against individual privacy.
El Paso Intelligence Center

URL:  http://www.usdoj.gov/dea/programs/epic.htm

Access:  https://www.esp.gov

The El Paso Intelligence Center was established in 1974 in response to a study by the Justice Management Division of the U.S. Department of Justice entitled, "A Secure Border." Recommendation number 7 of this study suggested the establishment of a southwest border intelligence center to be led by the Drug Enforcement Administration (DEA) and staffed by representatives of that agency, as well as the U.S. Customs Service. The initial focus of the Center was to assist in the identification of drug traffickers and alien traffickers along the U.S. - Mexico border.

In 2001, immediately after the terrorist attacks in New York and Washington, DC, the multiagency environment of EPIC was called upon to support investigations to find those responsible. EPIC’s mission evolved from its experience in supporting interdiction efforts and investigations regarding drug trafficking, alien and weapon smuggling, and other criminal activities, by adding counterterrorism to its efforts.

EPIC is now staffed with over 300 personnel and liaison officers from 15 agencies. Agencies currently represented at EPIC include the Drug Enforcement Administration; Department of Homeland Security; Customs & Border Protection; Immigration & Customs Enforcement; U.S. Coast Guard; Federal Bureau of Investigation; Bureau of Alcohol, Tobacco, Firearms and Explosives; U.S. Secret Service; U.S. Marshals Service; National Drug Intelligence Center; Internal Revenue Service; U.S. Department of the Interior; National Geospatial–Intelligence Agency; U.S. Department of Defense; Joint Task Force–North; Joint Interagency Task Force–South; Texas Department of Public Safety; Texas Air National Guard; and the El Paso County Sheriff’s Office.

EPIC’s vision is to continue to provide timely and expeditious support to Federal, State, local, tribal, and international law enforcement agencies and to remain the premier tactical operational intelligence center in the nation.

E-mail Encryption

Web-Based Email Encryption Services

NeoMailBox - http://www.neomailbox.com/ : Supports OpenPGP encryption and digital signatures, it will hide your IP on the headers and you can choose to host your email in the US or Switzerland.
4SecureMail - http://www.4securemail.com/ : Support for wemail PGP encryption and signing, all emails get scanned with a ICSA-Certified antivirus, your computer IP is hidden and not forwarded with the messages.

AnonymousSpeech - https://www.anonymousspeech.com/ : PGP email encryption supported, IP is hidden in the headers, the servers are located outside the US and Europe, guarantee not to reply to correspondence of foreign Governments.

Countermail - https://countermail.com/ : Supports OpenPGP encryption and digital signatures for webmail, it also hides your IP on the headers, servers located in Sweden.


Cryptoheaven - http://www.cryptoheaven.com/ : It uses its own encrypted servers instead of OpenPGP, the other user will need to have a CryptoHeaven email address too for the email messages to remain encrypted end to end.


Safe-Mail - http://www.safe-mail.net/ : It supports PGP email encryption and digital signatures as well as using of digital certificates for sending encrypted messages using the web interface. Safe-Mail DOES NOT hide your computer IP on the headers.

KeptPrivate - http://www.keptprivate.com/ : All of your email messages are kept encrypted in their servers using the Blowfish algorithm, no support for PGP, the person you are emailing to will need a KeptPrivate email account too in order to sent emails encrypted.

Embassies, Consulates, and Diplomatic Missions of the United States

URL: http://www.usembassy.gov/

Embassies and Foreign Consular Offices

URL: http://www.state.gov/s/cpr/rls/

The Office of the Chief of Protocol publishes the Diplomatic List, which contains a complete list of the accredited diplomatic officers of foreign embassies within the United States, and publishes Foreign Consular Offices, a complete listing of the foreign consular offices in the United States.
Emergency Management Institute - FEMA Independent Study Program (ISP)

URL:  http://training.fema.gov/IS/

The Emergency Management Institute (EMI) offers self-paced courses designed for people who have emergency management responsibilities and the general public. All are offered free-of-charge to those who qualify for enrollment. To get a complete listing of courses, click on Course List link above.

FEMA’s Independent Study Program offers courses that support the nine mission areas identified by the National Preparedness Goal.

- Incident Management
- Operational Planning
- Disaster Logistics
- Emergency Communications
- Service to Disaster Victims
- Continuity Programs
- Public Disaster Communications
- Integrated Preparedness
- Hazard Mitigation

Emergency Operations Training Academy

URL:  http://eota.doeal.gov/

EOTA exists to conduct training. Training success depends on the curriculum and how it is developed, delivered, tested, and evaluated. A key feature is EOTA's use of state-of-the-art instruction techniques and technologies, leading to the benefit of higher levels of knowledge retention. Another key feature is EOTA's factoring in of lessons learned from across the complex, which ensures that the experiences communicated to students are up-to-date and implemented complex-wide. Several courses are available on-line as well as in classroom settings.
Encryption - JavaScrypt

Fourmilabs Switzerland

URL: http://www.fourmilab.ch/javascrypt/

Fourmilabs is a web-site developed and maintained by John Walker, founder of Autodesk, Inc. and co-author of AutoCAD. While this web-site offers many interesting items, from the security viewpoint we are interested in the ‘Cryptography and Steganography’. The JavaScript Browser Based Cryptography Tools are easy to use, work on any computer that can handle JavaScript, and offer a good level of security for e-mail communication. The encryption program is provided free of charge and has according to the web-site has been placed into the public domain.

From the web-site: "JavaScrypt runs entirely in your browser--nothing is sent to any Web site when you use it. You can, if you wish, download JavaScrypt to your own computer and use it when not connected to the Internet. JavaScrypt's encryption facilities use the Advanced Encryption Standard (AES) adopted by the United States as Federal Information Processing Standard 197. AES supports key lengths of 128, 192, and 256 bits; JavaScrypt uses 256 bit keys exclusively."

Encryption Wizard (EW)
DoD Software Protection Initiative

URL: http://spi.dod.mil/ewizard.htm

EW is an SPC implementation of the Advanced Encryption Standard (AES) (Rijndael) augmented with a file manager Graphical User Interface (GUI) for ease of use. The 128-bit encryption/decryption algorithm used by Encryption Wizard is considered cryptographically strong and is routinely used in National Security Agency (NSA) and National Institute of Standards and Technology (NIST) certified products. Encryption Wizard is designed to protect data at rest and in transit (such as email attachments).

EW is an easy to use tool for protecting sensitive (but not classified) documents, and for protecting files before transmission via email. It allows a user to encrypt files using a 128-bit implementation of the Advanced Encryption Standard (AES) with simple drag-and-drop efficiency. Encryption Wizard can significantly increase an organization’s security posture at little to no cost to protect sensitive data in transit (E-mail, FTP, or shared web folders) or at rest on a removable storage device. The primary version for government users utilizes a FIPS 140-2 validated encryption engine licensed from RSA Security.
Español for Law Enforcement: An Interactive Training Tool

URL: http://www.ojp.usdoj.gov/nij/pubs-sum/201801.htm

This online training was developed to help law enforcement officers obtain a working knowledge of Spanish and apply it to law enforcement situations. The course walks viewers through English translations, phonetic spellings and pronunciations of Spanish words in situations involving interviews, crime scenes, motor vehicles and domestic violence. Free registration.

Estimative Language

An Explanation of Estimative Language

We use phrases such as we judge, we assess, and we estimate—and probabilistic terms such as probably and likely—to convey analytical assessments and judgments. Such statements are not facts, proof, or knowledge. These assessments and judgments generally are based on collected information, which often is incomplete or fragmentary. Some assessments are built on previous judgments. In all cases, assessments and judgments are not intended to imply that we have “proof” that shows something to be a fact, or that definitively links two items or issues.

In addition to conveying judgments rather than certainty, our estimative language also often conveys 1) our assessed likelihood or probability of an event; and 2) the level of confidence we ascribe to the judgment.

Estimates of Likelihood. Because analytical judgments are not certain, we use probabilistic language to reflect the Community’s estimates of the likelihood of developments or events. Terms such as probably, likely, very likely, or almost certainly indicate a greater than even chance. The terms unlikely and remote indicate a less than even chance that an event will occur; they do not imply that an event will not occur. Terms such as might or may reflect situations in which we are unable to assess the likelihood, generally because relevant information is unavailable, sketchy, or fragmented. Terms such as we cannot dismiss, we cannot rule out, or we cannot discount reflect an unlikely, improbable, or remote event whose consequences are such that it warrants mentioning. The chart provides a rough idea of the relationship of some of these terms to each other.
Confidence in Assessments. Our assessments and estimates are supported by information that varies in scope, quality and sourcing. Consequently, we ascribe high, moderate, or low levels of confidence to our assessments, as follows:

- **High confidence** generally indicates that our judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A “high confidence” judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.

- **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

- **Low confidence** generally means that the information’s credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have significant concerns or problems with the sources.


EUROPOL


Europol is the European Law Enforcement Agency which aims at improving the effectiveness and co–operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of organized crime.

Evaluation of Information Sources

Louisiana State University - Evaluation of Information Sources - Tutorial (20 minutes)

This tutorial is intended to give you a foundation in the evaluation of Information Sources. Once you find information, you need to evaluate it, to determine it's value with respect to your information needs. This tutorial is presented in two parts. Part I will discuss understanding what type of information source you have and Part II will cover the criteria by which you may evaluate an information source.

Part I, Types of Information Sources - [http://www.lib.lsu.edu/instruction/evaluation/evaluation00.html](http://www.lib.lsu.edu/instruction/evaluation/evaluation00.html)
Excluded Parties List System (EPLS)

URL:  http://www.epls.gov/

Includes information regarding entities debarred, suspended, proposed for debarment, excluded or disqualified under the non-procurement common rule, or otherwise declared ineligible from receiving Federal contracts, certain subcontracts, and certain Federal assistance and benefits. This information may include names, addresses, DUNS numbers, Social Security Numbers, Employer Identification Numbers or other Taxpayer Identification Numbers, if available and deemed appropriate and permissible to publish by the agency taking the action. Please be aware that although GSA operates this system, individual agencies are responsible for the timely reporting, maintenance, and accuracy of their data.

--------- F ---------

Factbook on Intelligence (2002)
Office of Public Affairs, CIA

URL:  http://permanent.access.gpo.gov/lps63587/CIA_Factbook_on_Intelligence_2002/textonly.htm

URL:  http://www.fas.org/irp/cia/product/facttell/index.html

FAS – See: Federation of American Scientists

FBI - See: Federal Bureau of Investigation
FBI Analysts

Since 9/11, the FBI has worked hard to establish career paths for intelligence analysts and senior positions they can aspire to.

After an intensive 10-week basic training course, intelligence analysts (IAs) specialize in one of three analytic areas—tactical, strategic, or collection/reporting. They may work at FBI Headquarters, in one of our 56 field offices, or internationally in one of our legal attaché offices.

As they gain experience and subject matter expertise, IAs can move up the career ladder to intermediate and advanced positions such as supervisory intelligence analysts and senior intelligence officers.

Intelligence Analysts - Part 1: Central to the Mission


Intelligence Analysts - Part 2: The Subject Matter Experts


Intelligence Analysts - Part 3: A Rewarding Career


FBI Citizens' Academy

URL:  http://www.fbi.gov/hq/ood/opca/outreach/academy.htm

The FBI Citizen’s Academy is an outreach program of the Federal Bureau of Investigation which affords business and community leaders an inside look at Federal law enforcement in general and the FBI family in particular. The Academy allows you to meet and interact with personnel of the FBI in a positive and informal setting sharing ideas and information.

The FBI Citizen’s Academy creates a closer connection between the FBI and the surrounding community through an educational process; fosters greater understanding of the role of FBI policies and programs through frank interactive discussions; and expands the pool of community leaders who understand first-hand the complex challenges of Federal law enforcement through examination of actual FBI investigations.
FBI Law Enforcement Bulletin

URL:  http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/leb

The FBI Law Enforcement Bulletin is published monthly by the Federal Bureau of Investigation.

FBI Virtual Academy

URL:  https://fbiva.fbiacademy.edu/

The FBI Virtual Academy (FBIVA): a structured, efficient, electronically delivered system of learning that adds value to the forensic science, law enforcement, and judicial communities by providing a single, comprehensive learning solution that offers a web-based means of accessing and acquiring the essential knowledge, skills, and competencies (through relevant and consistent training and materials) needed to support the worldwide criminal justice community.

Federal Bureau of Investigation

URL:  http://www.fbi.gov

J. Edgar Hoover Building
935 Pennsylvania Avenue,
NW Washington, D.C. 20535-0001
Telephone: 202-324-3000

FBI Field Offices

URL:  http://www.fbi.gov/contact-us/field/field-offices

The FBI has 56 field offices centrally located in major metropolitan areas across the U.S. and Puerto Rico. The FBI also maintains about 400 resident agencies in smaller cities and towns across the nation. 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 managed by an Assistant Director in Charge due to their large size.

Federal Bureau of Prisons Inmate Locator

(includes all inmates from 1982 to present)

URL:  http://www.bop.gov/iloc2/LocateInmate.jsp
Federal Communications Commission - Universal Licensing System


The ULS License Search enables you to search for a wide range of licenses in the Universal Licensing System. The License Search here provides access to the most basic attributes of a license. You can also specify more attributes combinations with the Advanced Search and search within services like Amateur using service-specific criteria.


Federal Law Enforcement Training Center (FLETC)

URL:  [http://www.fletc.gov/](http://www.fletc.gov/)

The FLETC serves as an interagency law enforcement training organization for more than 80 Federal agencies. The Center also provides services to state, local, and international law enforcement agencies. The Center is headquartered at Glynco, GA, near the port city of Brunswick, halfway between Savannah, GA, and Jacksonville, FL.

In addition to Glynco, the FLETC operates two other residential training sites in Artesia, NM, and Charleston, SC. The FLETC also operates a non-residential in-service re-qualification and advanced training facility in Cheltenham, MD, for use by agencies with large concentrations of personnel in the Washington, D.C., area.

The FLETC has oversight and program management responsibility for the International Law Enforcement Academy (ILEA) in Gaborone, Botswana; San Salvador, El Salvador; and Lima, Peru. The FLETC also supports training at other ILEAs in Hungary and Thailand.
Federation of American Scientists - Intelligence Resource Program

URL:  http://www.fas.org/irp/

A "comprehensive resource on the past and future of the American intelligence community," from the Federation of American Scientists, it includes sections on Intelligence Systems and Programs, Intelligence Agencies and Budgets, Worldwide Intelligence Agencies, Documents and Records, Congressional Material, News Reports and Analysis, and more.

Federation of American Scientists
1725 DeSales Street NW, 6th floor
Washington, DC 20036

FEMA

URL:  http://www.fema.gov/index.shtml

Federal Emergency Management Agency
U.S. Department of Homeland Security
500 C Street SW, Washington, D.C. 20472
Telephone:  202-646-2500

FEMA Regions
Mission

Serves as the Agency’s Office through which all policy, managerial, resource and administrative actions that affect or impact the Regions receive effective coordination between headquarters and the Regional Offices.

The Office of Regional Operations also ensures that FEMA policies, programs, administrative and management guidance are implemented in the Regions in a manner consistent with the Agency’s overall goals.

The principal functions of the Office of Regional Operations are:

- Liaison between the Regional Administrators and Headquarters leadership
- Advising the headquarters leadership on matters affecting or impacting the Regions
- Providing guidance to Regional Administrators on policy, programs, operations, and administrative matters

FEMA Independent Study Program

See: Emergency Management Institute - FEMA Independent Study Program

FEMA Security Risk Management Series (RMS) Publications


The Risk Management Series (RMS) is a FEMA series directed at providing design guidance for mitigating multi-hazard events. The series includes a large cadre of man-made disaster publications directed at strengthening the building inventory to reduce the potential impact from the forces that might be anticipated in a terrorist assault. The objective of the series is to reduce physical damage to structural and nonstructural components of buildings and related infrastructure, and to reduce resultant casualties from impact by conventional bombs, chemical, biological, and radiological (CBR) agents; earthquakes; floods; and high winds. The underlying issue is that by improving mitigation and security of high occupancy buildings, we will be better positioned to protect the nation from potential threats and hazards. The intended audience includes architects and engineers working for private institutions, building owners/operators/managers, and state and local government officials working in the building sciences community.

- FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 427 - Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks
- FEMA 428 - Primer to Design Safe School Projects in Case of Terrorist Attacks
- FEMA 429 - Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings
- FEMA 430 - Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks
- FEMA 452 - A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 453 - Safe Rooms and Shelters: Protecting People Against Terrorist Attacks
- FEMA 455 - Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks
- FEMA 459 - Incremental Protection for Existing Commercial Buildings from Terrorist Attack: Providing Protection to People and Buildings

**FINRA Investment Broker License Check**

URL:  [http://www.finra.org/Investors/ToolsCalculators/BrokerCheck/index.htm](http://www.finra.org/Investors/ToolsCalculators/BrokerCheck/index.htm)

Financial Industry Regulatory Authority (FINRA), is the largest non-governmental regulator for all securities firms doing business in the United States.

FINRA BrokerCheck is a free online tool to help investors check the professional background of current and former FINRA-registered securities firms and brokers. It should be the first resource investors turn to when choosing whether to do business with a particular broker or brokerage firm.

Features of FINRA BrokerCheck include:

- Search capabilities for both a broker and brokerage firm
- Online delivery of a report on a broker or brokerage firm
- Explanatory information to help investors better understand the content, context and source of the information provided
- Links to additional resources and tools

The information made available through FINRA BrokerCheck is derived from the Central Registration Depository (CRD®), the securities industry online registration and licensing database, as reported on industry registration/licensing forms brokers, brokerage firms and regulators complete. BrokerCheck features professional background information on approximately 660,000 currently registered brokers and 5,100 currently registered securities firms. Information is also available on thousands of formerly registered firms and brokers.

For questions regarding BrokerCheck, FINRA provides a toll-free hotline, (800) 289-9999, available Monday through Friday from 8 a.m. until 8 p.m., Eastern Time.
Firearms Manuals Online

URL:  http://www.stevespages.com/page7b.htm

The website lists nearly every firearm and its corresponding manual. The website also includes manuals for flashlights, metal detectors, optics, cameras, and reloading tools. Stephen Ricciardelli from Saint Marie, Montana runs the website and continually updates more information about firearms and their accessories.

First Observer

URL:  http://www.firstobserver.com/

“First Observer” is a national safety and security program that uses the skills, experiences and "savvy" of America's transportation professionals to help protect the critical transportation function that moves the goods and services and people across America.

“First Observer” is operated by Team HMS under a Cooperative Agreement with the Department of Homeland Security (DHS) Trucking Security Program (TSP). The program's mission is to administer an anti-terrorism and security awareness program for highway professionals in support of the National Preparedness Guidelines. A key component of the program is to recruit volunteers from the Trucking, Motor Coach Carriers and School Bus industries to act as our “First Observer” in reporting suspicious activities of either a criminal or potential terroristic nature to authorities.

Foreign Area Officer Association (FAOA)

URL:  http://www.faoa.org/

FAOA is a professional organization serving the interests of Foreign Area Officers in all services of the U.S. Armed Forces: active duty, reserve component, and retired.Founded in 1995, FAOA provides advocacy, networking, and mentorship.

Foreign Broadcast Information Service

The Foreign Broadcast Information Service is a United States government agency which translates the text of daily radio and television broadcasts, newspapers and periodicals,
government statements, books, and other sources of unrestricted information such as databases and gray literature from non-English sources around the world. Reports with translations are issued for eight world regions daily and cover such topics as military affairs, politics, the environment, societal issues, economics, and science and technology. Reports are available from 1941 to the present. In November 2005, it was announced that FBIS would become the newly-formed Open Source Center, tasked with the collection and analysis of freely-available intelligence.

**Foreign Clearance Guide**
See: Department of Defense Foreign Clearance Guide

**Foreign Language Training** - See: Language & Culture Training

**Foreign Military Studies Office - Joint Reserve Intelligence Center (FMSO-JRIC)**

URL: [http://fmso.leavenworth.army.mil](http://fmso.leavenworth.army.mil)
URL: [http://www.intelink.gov/fmso](http://www.intelink.gov/fmso)

731 McClellan Ave
Ft. Leavenworth, KS 66027-1350
Tel: 913-684-5946
Fax: 913-684-5960

The Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas, is an open source research organization of the U.S. Army. Founded as the Soviet Army Studies Office in 1986, it was an innovative program that brought together military specialists and civilian academics to focus on military and security topics derived from unclassified, foreign media. The results were unclassified articles and papers that provided new understandings and broad access to information from a base of expertise in the U.S. Army, Department of Defense, and foreign and U.S. defense communities and universities.

Today FMSO maintains this research tradition of special insight and highly collaborative work. FMSO conducts unclassified research of foreign perspectives of defense and security issues that are understudied or unconsidered but that are important for understanding the environments in which the U.S. military operates. FMSO’s work today is still aimed at publication in unclassified journals and its research findings are taught in both military and civilian venues in the United
States and around the world. FMSO is organized in the U.S. Army Training and Doctrine Command under the TRADOC G-2.

**Foreign Service Institute Language Courses**

URL: [http://fsi-language-courses.org/Content.php](http://fsi-language-courses.org/Content.php)

These courses were developed by the United States government and are in the public domain.

**Foundations of Intelligence Analysis Training (FIAT)**

URL: [http://www.nw3c.org/ocr/courses_desc.cfm?cn=FIAT](http://www.nw3c.org/ocr/courses_desc.cfm?cn=FIAT)

The FIAT course was developed by a consortium that included the National White Collar Crime Center (NW3C), Law Enforcement Intelligence Unit (LEIU), the International Association of Law Enforcement Intelligence Analysts (IALEIA), and the Regional Information Sharing System (RISS).

FIAT is approved for the use of state DHS/FEMA training funds

FIAT Topics:

- The History of Intelligence Analysis
- The Purpose of Intelligence Analysis
- The Intelligence Cycle
- Analytical Thinking Skills
- Using Different Types of Analysis
- The importance of strategic analysis in deterring crime.

**Fusion Center**

URL: [http://www.dhs.gov/files/programs(gc_1156877184684.shtm](http://www.dhs.gov/files/programs(gc_1156877184684.shtm)

State and major urban fusion centers (fusion centers) serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners.

Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response,
public health, CIKR protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.

**Fusion Center Guidelines**


**Baseline Capabilities for State and Major Urban Area Fusion Centers**

September 2008 - A Supplement to the Fusion Center Guidelines


**Fusion Centers and Intelligence Sharing**


**Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template**


Assists fusion center personnel in developing a center privacy policy related to the information, intelligence, and suspicious activity report (SAR) information the center collects, receives, maintains, archives, accesses, and discloses to center personnel, governmental agencies, Information Sharing Environment (ISE) participants, and other participating criminal justice and public safety agencies, as well as to private contractors and the general public. Provisions contained in this template will help centers comply with requirements of the DHS Homeland Security Grant Program Guidance, the ISE Privacy Guidelines, and the Nationwide Suspicious Activity Reporting (SAR) Initiative.
Fusion Center Resources

URL:  

Fusion Center Technology Guide

URL:  http://it.ojp.gov/docdownloader.aspx?ddid=1283

Provides a methodology for fusion center directors and managers that can be used to facilitate technology planning and to provide a practical perspective on the value of technology as an enabler of the fusion center mission. Fusion center directors and managers can use the document to aid in the development and implementation of technology within their fusion centers to achieve their missions.

Future of American Intelligence

Editor: Peter Berkowitz
Pub Date:  October 28, 2005
URL:  http://www.hooverpress.org/productdetails.cfm?PC=1114

The urgent task of reforming U.S. intelligence The United States today faces new kinds of adversaries, armed with an array of sinister weapons and capable of communicating and coordinating actions around the globe with unprecedented ease. As The Future of American Intelligence demonstrates, this dangerous new world requires changes in how the United States collects and analyzes intelligence and translates it into policy. These essays from a diverse group of distinguished contributors deepen our understanding of the new national security threats posed by terrorism, by the proliferation of weapons of mass destruction, and by the spread of Islamic extremism. They examine the obstacles-intellectual, governmental, bureaucratic, military, and technological-to making U.S. intelligence more effective and offer thoughtful recommendations for reform. Approaching the problem from a variety of disciplinary perspectives, the authors stress how it is critical that the intelligence community revise its deeply entrenched assumptions and ideas about how to collect and analyze intelligence. They reveal how those assumptions led the United States to overlook the gravity of the threat posed by bin Laden and be dead wrong about weapons of mass destruction in Iraq-and how they generally stifle creative thinking and independent judgment within intelligence agencies. Their recommendations include suggestions for reforming the management style and the organizational structure of the intelligence services as well as establishing more effective procedures for taking advantage of both current and future technological advances. Peter Berkowitz teaches at George Mason University School of Law and
is a fellow at the Hoover Institution. Contributors: Reuel Mark Gerecht, Gordon Lederman, Kevin O'Connell, Gary Schmitt, Richard Schultz. Full-text PDF versions of each chapter are available on the web-site.

- Table of Contents
- Acknowledgments
- Contributors
- Introduction
- The Era of Armed Groups
- Truth to Power? Rethinking Intelligence Analysis
- Restructuring the Intelligence Community
- A New Clandestine Service: The Case for Creative Destruction
- The Role of Science and Technology in Transforming American Intelligence
- Index

---

**GeoChat**

URL: [http://instedd.org/technologies/geochat/](http://instedd.org/technologies/geochat/)

It is designed to enable self-organizing group communications by allowing users to link the field, headquarters, and the local community in a real-time, interactive conversation visualized on the surface of a map. GeoChat is a tool for group communications based on SMS, email, and Twitter.

People use GeoChat to simplify team communications, logistics and data reporting, and they can extend their own software applications using the open APIs. GeoChat is a flexible open source group communications technology that lets team members interact to maintain shared geospatial awareness of who is doing what where — over any device, on any platform, over any network. GeoChat allows you and your team to stay in touch one another in a variety of ways: over SMS, over email, and on the surface of a map in a web browser.

Whether you are sitting at a computer with a high-speed Internet connection, or on the go with your mobile phone, GeoChat lets you react to events on the ground with maximum agility, forming cross-organizational virtual teams on the fly, linking field to headquarters, and keeping everyone on your team connected, in sync, and aware of who is doing what, and where.
Geospatial Intelligence Handbook - TC 2-22.7 (18 FEB 2011) (FOUO)

URL:  https://armypubs.us.army.mil/doctrine/DR_pubs/dr_b/pdf/tc2_22x7.pdf?feedAHP=Y
(AKO Log-in Required)

TC 2-22.7 is the Army’s manual for geospatial intelligence (GEOINT) doctrine. It describes—

- GEOINT.
- Imagery.
- Imagery intelligence.
- Geospatial information and services.
- The implementation of GEOINT in the Army.
- GEOINT support to planning and operations.

This training circular provides GEOINT guidance for commanders, staffs, trainers, engineers, and military intelligence personnel at all echelons. It forms the foundation for GEOINT doctrine development. It also serves as a reference for personnel who are developing doctrine; tactics, techniques, and procedures; materiel and force structure; and institutional and unit training for intelligence operations.

Global Language Online Support System

URL:  http://gloss.dliflc.edu/

GLOSS online language lessons are developed for independent learners to provide them with the learning/teaching tools for improving their foreign language skills. Reading and listening lessons are based on authentic materials (articles, TV reports, radio broadcasts, etc.) and consist of 4 to 6 activities. The motivating tasks are accompanied with in-depth feedback that provide learners with thorough explanations and tutoring just like an attentive and experienced teacher would do. With more than 4,000 lessons, GLOSS is a valuable resource in maintaining and improving language ability of the learners.

Google Encrypted Search

URL:  https://encrypted.google.com/

With Google search over SSL, you can have an end-to-end encrypted search solution between your computer and Google. This secured channel helps protect your search terms and your
search results pages from being intercepted by a third party. This provides you with a more secure and private search experience.

To use search over SSL, visit https://encrypted.google.com each time you perform a search. Note that only Google web search is available over SSL, so other search products like Google Images and Google Maps are not currently available over SSL. When you're searching over SSL, these properties may not appear in the left panel.

Here's how searching over SSL is different from regular Google search:

- SSL encrypts the communication channel between Google and a searcher's computer. When search traffic is encrypted, it can't be read by third parties trying to access the connection between a searcher's computer and Google's servers. Note that the SSL protocol does have some limitations — more details are below.
- As another layer of privacy, SSL search turns off a browser's referrers. Web browsers typically turn off referrers when going from HTTPS to HTTP mode to provide extra privacy. By clicking on a search result that takes you to an HTTP site, you could disable any customizations that the website provides based on the referrer information.
- At this time, search over SSL is supported only on Google web search. We will continue to work to support other products like Images and Maps. All features that are not supported have been removed from the left panel and the row of links at the top. You'll continue to see integrated results like images and maps, and clicking those results will take you out of encrypted search mode.
- Your Google experience using SSL search might be slightly slower than you're used to because your computer needs to first establish a secure connection with Google.

Note that SSL search does not reduce the data that Google receives and logs when you search, or change the listing of these terms in your Web History.

How will SSL search affect content filtering services?

When searches are conducted using https://encrypted.google.com, those searches will bypass any content filters that are in place on your network.

**Google Fusion Tables**

URL: [http://tables.googlelabs.com](http://tables.googlelabs.com)

- Upload small or large data sets from spreadsheets or CSV files.
- Visualize your data on maps, timelines and charts.
- Pick who can access your data; hide parts of your data if needed.
- Merge data from multiple tables.
Discuss your data with others. Track changes and discussions.

Google Voice

URL: [http://www.google.com/voice](http://www.google.com/voice)

Google Voice is a telecommunications service by Google launched on March 11, 2009. The service provides a US phone number, chosen by the user from available numbers in selected area codes, free of charge to each user account. Inbound calls to this number are forwarded to other phone numbers of the subscriber. Outbound calls may be placed to domestic and international destinations by dialing the Google Voice number or from a web-based application. Inbound and outbound calls to US (including Alaska and Hawaii) and Canada are free of charge. International calls are billed according to a schedule posted on the Google Voice website.

Google Voice with a Google number

- Use one number to manage all your phones; your Google Voice number is tied to you, not to a particular device or location.
- Voicemail like email: Save voicemail messages for as long as you'd like, star important ones, and search through them
- Voicemail transcription: Voicemail messages will be automatically transcribed to text and sent to you via email and/or SMS.
- Customize your callers' experience (custom voicemail greetings, decide which of your phones ring based on who's calling, send some callers straight to voicemail, etc.)
- Define which phones ring, based on who's calling, and even ListenInTM on voicemail before answering the call. We use smart technology to route your calls. So, if you're already on a Google Voice call, we'll recognize it and use call waiting to reach you on the phone you're on.
- Works with mobile phones, desk phones, and work phones. There's nothing to download, upload, or install, and you don't have to make or take calls using a computer.
- International calling: Make low priced international calls from the web or from your phone.

Google Voice with your non-Google phone number: With this option you won't get some features (i.e. call forwarding, screening, and call recording), but you'll still get plenty of others, including:

- Voicemail like email: Save voicemail messages for as long as you'd like, star important ones, and search through them
- Voicemail transcription: Voicemail messages will be automatically transcribed to text and sent to you via email and/or SMS.
Custom voicemail greetings: Customize your voicemail greeting based on who is calling.
International calling: Make low priced international calls from the web or from your phone.

**Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces**


Provides guidance to agencies seeking to establish and operate gang task forces or gang intelligence units within their jurisdictions or to those agencies that participate in gang task forces. This document was developed by the Gang Intelligence Strategy Committee (GISC), under the U.S. Department of Justice’s Global Justice Information Sharing Initiative’s Intelligence Working Group. The GISC—composed of federal, state, local, and tribal law enforcement; justice; and corrections representatives—is tasked with improving gang related information sharing.

**Guide to Conducting Research in FBI Records (March 1, 2010)**


---

**Hawala and Alternative Remittance Systems**


The word “hawala” comes originally from the Arabic language and means transfer or remittance. Hawala provides a fast and cost-effective method for worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector. In some nations hawala is illegal, in others the activity is considered a part of the “gray” economy. It is therefore difficult to accurately measure the total volume of financial activity associated with the system, however, it is estimated that the figures are in the tens of billions of dollars, at a
minimum. Officials in Pakistan, for example, estimate that more than $7 billion flow into the nation through hawala channels each year. Other Alternative Remittance or Informal Value Transfer Systems include “hundi,” “fei ch ‘ien,” “chit system,” “poey kuan” and the black market peso exchange.

The very features which make hawala attractive to legitimate customers (mainly expatriates remitting money to relatives in their home country) ---efficiency, anonymity, and lack of a paper trail---also make the system attractive for the transfer of illicit funds. As noted in a recent report of the Asia Pacific Group (APG) on Money Laundering, the terrorist events of September 2001 have brought into focus the ease with which alternative remittance and underground banking systems may be utilized to conceal and transfer illicit funds. Not surprisingly, concerns in this area have led many nations to reexamine their regulatory policies and practices in regard to hawala and other alternative remittance systems.

The Hawala Alternative Remittance System and its Role in Money Laundering

URL:  http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/

Headstart2  - See: Defense Language Institute - Headstart-2

High-Intensity Drug Trafficking Areas

URL:  http://www.whitehousedrugpolicy.gov/hidta/index.html

The Anti-Drug Abuse Act of 1988 and the ONDCP Reauthorization Act of 1998 authorized the Director of The Office of National Drug Control Policy (ONDCP) to designate areas within the United States which exhibit serious drug trafficking problems and harmfully impact other areas of the country as High Intensity Drug Trafficking Areas (HIDTA). The HIDTA Program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Law enforcement organizations within HIDTAs assess drug trafficking problems and design specific initiatives to reduce or eliminate the production, manufacture, transportation, distribution and chronic use of illegal drugs and money laundering.
High Technology Crime Investigation Association

URL:  http://www.htcia.org/

The High Technology Crime Investigation Association (HTCIA) is designed to encourage, promote, aid and affect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

Homeland Security - See: Department of Homeland Security (DHS)

Homeland Security Information Network (HSIN)

URL:  http://www.dhs.gov/files/programs(gc_1156888108137.shtm

Member Log-in -- http://www.hsin.gov

HSIN is a comprehensive, nationally secure and trusted web-based platform able to facilitate Sensitive But Unclassified (SBU) information sharing and collaboration between federal, state, local, tribal, private sector, and international partners. The HSIN platform was created to interface with existing information sharing networks to support the diverse Communities of Interest (COI) engaged in preventing, protecting from, responding to, and recovering from all threats, hazards and incidents under the jurisdiction of the Department of Homeland Security.

A key by-product of HSIN is the ability to provide real-time, interactive connectivity between states and major urban areas and the National Operations Center (NOC). HSIN is focused on providing a collaborative environment that interoperates with existing mission area systems developed and managed by our federal, state and local partners. HSIN is focused on enhancing collaboration rather than duplicating the capabilities provided by our partners. As a result of its unique perspective, HSIN facilitates collaboration between mission areas such as Law Enforcement, Emergency Management, and Critical Sectors.

HSIN-Intelligence

URL:  https://hsin-intel.dhs.gov/

Homeland Security Points of Contact (by State)

URL:  http://www.dhs.gov/xgovt/editorial_0291.shtml
Homeland Security Risk Lexicon


The second edition of the Department of Homeland Security (DHS) Risk Lexicon, represents an update of the version published in September 2008. More than seventy terms and definitions were included in the first edition of the DHS Risk Lexicon. The 2010 edition includes fifty new terms and definitions in addition to revised definitions for twenty-three of the original terms.

House Permanent Select Committee on Intelligence (HPSCI)


  - Subcommittee on Oversight
  - Subcommittee on Technical and Tactical Intelligence
  - Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence

(Cross Reference: Senate Select Committee on Intelligence)

Human Intelligence Collector Operations (FM 2-22.3) September 2006


This manual provides doctrinal guidance, techniques, and procedures governing the employment of human intelligence (HUMINT) collection and analytical assets in support of the commander’s intelligence needs. It outlines:
• HUMINT operations.
• The HUMINT collector’s role within the intelligence operating system.
• The roles and responsibilities of the HUMINT collectors and the roles of those providing the command, control, and technical support of HUMINT collection operations.

HUMINT collection activities include three general categories: screening, interrogation, and debriefing. In some cases these may be distinguished by legal distinctions between source categories such as between interrogation and debriefing. In others, the distinction is in the purpose of the questioning. Regardless of the type of activity, or goal of the collection effort, HUMINT collection operations must be characterized by effective support, planning, and management.

HUMINT Training - Joint Center of Excellence (HT-JCOE)
Fort Huachuca, Arizona

URL: https://www.us.army.mil/suite/page/612679

Courses:

Advanced Source Operations Course (ASOC)

ASOC is an 89-training day course that certifies DOD personnel to conduct controlled intelligence operations under tactical and non-tactical conditions in multiple environments. Graduates will be subject-matter experts on controlled source operations capable of advising conventional force commanders on advanced military source operations methodology under permissive, semi-permissive and non-permissive conditions. Graduates will possess advanced military source operations skill sets capable of supporting tactical and operational commanders in the field.

Defense Strategic Debriefing Course (DSDC)

DSDC is a five-week course that provides an overview of techniques and methodologies for conducting strategic debriefings and preparing appropriate reports. Students will conduct real-world based training on the mechanics of debriefing, and develop interpersonal and source management skills. The course consists of scenario based exercises with heavy emphasis on overt collection and reporting. Students are also placed under stressful scenarios including no-win situations and reluctant sources to force resourceful and adaptive student responses and foster student creativity and flexibility.

Joint Analyst and Interrogator Collaboration Course (JAICC)
JAICC is a five-week intermediate course for Interrogators and HUMINT Analysts. The JAICC course pairs interrogators and HUMINT analysts into teams. Using both MOS' in a synergistic way, the JAICC teaches how more reliable and accurate information can be obtained in a shorter amount of time. The mission of JAICC is to produce highly capable human intelligence professional teams consisting of Interrogators and HUMINT Analysts. Upon completion of JAICC, these teams will be prepared to conduct medium and long term interrogations with target-centered analytical products responding to the time sensitive demands of the current operational environment. The objectives of these teams are to defeat enemy counter-interrogation techniques, breach cover stories, detect and counter deception, and to rapidly exploit intelligence information for dissemination to Department of Defense assets and other agencies of the U.S. Intelligence Community involved in the Global War on Terror.

Interrogators will use approved approaches and advanced deception detection strategies as well as advanced questioning methodologies in medium- and long-term interrogation environments. Analysts will assist HUMINT Collectors by providing real-time feedback, background research and analysis on source culture, tribal and religious affiliations, and geopolitical considerations in the target AOR, using the latest analytical tools not typically available to Interrogators.

**Joint HUMINT Analysis and Targeting Course (JHATC)**

JHATC is a two-week course that trains HUMINT collectors and analysts to work together in a synergistic manner to identify, develop, and vet lucrative sources.

**Joint HUMINT Officer Course (JHOC)**

JHOC is a four-week course that trains entry and mid-level HUMINT managers in the Defense HUMINT Enterprise (DHE). Graduates of this course are equipped to manage and maximize HUMINT collection in support of Combatant Commanders’ Priority Intelligence Requirements (PIR). JHOC provides thorough instruction on HUMINT policy law and procedure at the National, Joint, Service, Operational and Tactical levels. JHOC also trains its graduates to collaborate and coordinate HUMINT operations with other internal and external military and civilian intelligence partners. JHOC trains IT competencies using software and communications suites that are employed in real world HUMINT operations throughout the Defense HUMINT Enterprise.

**Joint Interrogation Certification Course (JICC)**

JICC is an eight-week course that provides the basic qualification skills to conduct Intelligence Interrogation collection operations; screening of Human Intelligence (HUMINT) sources and documents to establish priorities for exploitation; preparing and editing appropriate intelligence and administrative reports; utilizing CI/HUMINT reporting and communications equipment; using interpreters and managing interpreter/translator operations. Upon graduation, student will be a certified Department of Defense Interrogator.
Joint Interrogation Management Course (JIMC)

JIMC is a three-week course that trains mid-level HUMINT managers in the Defense HUMINT Enterprise (DHE). Graduates of this course are equipped to maximize HUMINT collection in support of Combatant Commanders’ Priority Intelligence Requirements through the management of interrogation operations. JIMC provides thorough instruction on Interrogation policy law, operations management, and procedure at the National, Joint, Service, Operational and tactical levels. JIMC also trains its graduates to collaborate and coordinate interrogation operations with other internal and external intelligence partners both military and civilian. JIMC is not a certification course. Graduates will sign a Memorandum of Understanding (MOU) prior to graduation attesting to the fact that they understand that the course does not certify them as DOD interrogators and that they are therefore not authorized to conduct interrogations. Copies of MOUs will be kept on file at HT-JCOE.

Joint Senior Interrogator Course (JSIC)

JSIC is a three-week course that trains senior interrogators to supervise DoD interrogation operations and improve interrogation skills based on lessons-learned from interrogations conducted in the current theater of operations. The JSIC provides instruction to senior-level interrogators on how to manage DoD Interrogation operations to include: cultural analysis; human behavioral analysis; screening and interrogation of sources of potential intelligence information; law of land warfare; automated systems functions; exploitation of open source material; intelligence information reports; and use of an interpreter. The JSIC is taught at a combined and joint level of instruction, providing senior interrogators from the U.S., Canada, the United Kingdom, and Australia the ability to learn not only from each other but also from coalition peers.

Joint Source Validation Course (JSVC)

JSVC is a two-day scenario and case-study led seminar developed by the HUMINT Training Joint Center of Excellence in coordination with national agencies. It is a collector-centric course that focuses on the proper application of Operational Tools and Operational Tests in support of sensitive HUMINT operations. The main effort of the course is to help the HUMINT Collector conduct the vetting process. As an overall objective, the proper application of these Operational Tools and Operational Tests will help to describe, evaluate, and use agents more accurately; make better use of limited resources by weeding out non-productive operations and those which simply cannot be resolved from a counterintelligence standpoint; build in accountability and emphasize the quality, not the quantity of operations.

Source Operations Course (SOC)

SOC is a 51-training day course that trains students to conduct Category 2 Military Source Operations to collect positive intelligence information against local terrorist, insurgent, criminal
organizations and personnel, and other hostile elements and activities that may pose a threat to friendly forces deployed to a theater of operations.

-------- I --------

ICE On-line Detainee Locator System

URL:  https://locator.ice.gov/odls/homePage.do

This Internet-based tool will assist family members, attorneys, and other interested people in locating individuals in ICE custody. By submitting accurate and basic data through the ODLS, individuals will be able to locate the detention facility where their relative or client is being held, as well as obtain contact information for the facility, visiting hours, and the phone number of the appropriate regional ICE office where additional information may be obtained.

Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety training video

URL:  http://www.ncirc.gov/privacylineofficer/

Assists local, state, and tribal law enforcement line officers in understanding their role in the protection of privacy, civil rights, and civil liberties as they perform their everyday duties. The short video provides an introductory overview of what privacy, civil rights, and civil liberties protections are; examples of these protections; and the important function line officers have in upholding these protections.

Individual's Guide for Understanding and Surviving Terrorism - USMC - MCRP 3-02E (September 2001)

Information Assurance Awareness (for Intelligence Community Personnel)

http://iase.disa.mil/eta/ic_iaa_v2/launchpage.htm

This web-based product presents information assurance (IA) for the Intelligence Community (IC) user with a focus on proper classification, marking, and handling of Sensitive Compartmented Information (SCI) within a SCI Facility (SCIF) environment. Precautions in secure SCI custody, transmission, and information sharing are reviewed. The IC user is further introduced to the principles of IA and IA-related laws and policies. The importance of critical infrastructure protection (CIP) and the differences between threats and vulnerabilities are explained in a style that reflects the constantly changing world of IA and its relationship to information technology. Through an interactive format, the user is presented with the dangers associated with the insider threat, social engineering, and peer-to-peer applications. The concept of malicious code, its impact, and the methods it uses to infect information systems are explored. The course identifies important guidelines that define the sensitivity levels of information, including personally identifiable information (PII), and your role as a user in protecting this information. Also explained are the threats associated with identity theft, spyware, and phishing. This course gives information on how you can protect yourself by providing security tips to practice in your daily routine at work and at home on your personal computer. (1.5 hrs)

Information Assurance Directorate - National Security Agency

URL:  https://www.iad.gov (Some areas of this web-site require DoD PKI/CAC)

Includes the following sites:

Committee on National Security Systems (CNSS)

The Committee on National Security Systems (CNSS) is a committee with representation from 21 U.S. Government Executive Branch Departments and Agencies. In addition to the 21 Members there are representatives serving as Observers from 11 additional organizations. The CNSS provides a forum for the discussion of policy issues; sets national policy; and promulgates direction, operational procedures, and guidance for the security of national security systems.

Information Assurance Events

The Information Assurance Directorate (IAD) Conferences and Exhibits Team is the designated focal point for oversight, coordination and administration of all IAD-sponsored or co-sponsored external conferences, symposia, and workshops. In addition, we serve as the technical and logistical point of contact for National Security Agency (NSA) and IAD internal and external exhibits.
Interagency OPSEC Support Staff (IOSS)

The Interagency OPSEC Support Staff (IOSS) was created to support the National OPSEC Program and help government organizations develop their own self-sufficient OPSEC programs in order to protect U.S. programs and activities. The IOSS provides tailored training, assists in program development, produces multimedia products and presents conferences for the defense, security, intelligence, research and development, acquisition and public safety communities.

Key Support Central Facility

The EKMS Central Facility is the center of the Electronic Key Management System (EKMS) responsible for the provision of electronic key and certificates. The EKMS Central Facility offers new key generation, electronic rekey and support services for an array of modern electronically rekeyable equipment servicing a world-wide customer base.

National Cryptographic Solutions Management Office (NCSMO)

The National Cryptographic Solutions Management Office (NCSMO) provides continuous guidance and oversight to multiple modernization projects and initiatives throughout the DoD services and agencies. Its mission is to provide a platform to expeditiously coordinate the secure exchange of Cryptographic Modernization (CryptoMod) management and technical information.

National Information Assurance Partnership (NIAP)

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors. This program is being implemented to help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

Secure Phone

The Secure Phone site is the source for Secure Wired and Wireless Technologies product information, to include warranties, procurement, training, and disposal. Its mission is to provide a platform to expeditiously coordinate the secure exchange of Secure Phone management and technical information.

Trusted Access Program Office (TAPO)

The Trusted Access Program Office (TAPO) has been chartered by the U. S. Government to find and maintain suppliers of trusted microelectronic parts. TAPO has successfully developed a reliable source of parts that gives the Intelligence Community needed access to state of the art...
commercial processes, fabrication tools and fabrication services. TAPO has made it possible for the Intelligence Community to design and obtain advanced mission critical systems via commercial, state of the art manufacturing processes. TAPO assures long term access to the latest and most capable commercial IC technologies in the world. TAPO resources are made available for government use only.

**Information Assurance Awareness (for Intelligence Community Personnel)**

URL:  [http://iase.disa.mil/eta/ic_iaa_v2/launchpage.htm](http://iase.disa.mil/eta/ic_iaa_v2/launchpage.htm) (Date 12/10)

With new material on the issues and risks of social networking and what to do when encountering classified or sensitive documents on the Internet, this web-based product presents information assurance (IA) for the Intelligence Community (IC) user, with a focus on proper classification, marking, and handling of Sensitive Compartmented Information (SCI) within a SCI Facility (SCIF) environment. Precautions in secure SCI custody, transmission, and information sharing are reviewed. The IC user reviews the principles of IA and the basics of critical infrastructure protection (CIP). Dangers associated with the insider threat, social engineering, and peer-to-peer applications are presented in a clear and understandable format. The concept of Malicious Code is introduced, including its impacts and the methods it uses to infect information systems. The course identifies important guidelines that define the sensitivity levels of information, including personally identifiable information (PII), and the IC user's role in protecting this information. Also explained are the threats associated with identity theft, spyware, and phishing. Security tips are provided for the user to practice in the daily work routine and at home. (1.5 hrs)

**Information Assurance Fundamentals Training (U.S. Army)**

URL:  [https://ia.signal.army.mil/IAF/default.asp](https://ia.signal.army.mil/IAF/default.asp)

This course provides individuals an understanding of the information systems security policies, roles, responsibilities, practices, procedures, and concepts necessary to perform the functions of an Information Assurance Security Officer (IASO). The lessons presented will aid the IASO in developing an effective security approach and in selecting cost-effective controls to meet the requirements of laws, directives, and regulations.

- Lesson 1 - Army Information Assurance Program (AIAP)
- Lesson 2 - Federal Laws, DoD Regulations and Policies
- Lesson 3 - Army Regulations and Policies
- Lesson 4 - Army Information Assurance Training Program
Information Assurance Support Environment

Defense Information Systems Agency (DISA)

URL: http://iase.disa.mil/

The Department of Defense information assurance portal. Provides a wide range of information assurance products, information and training in support of the military services and the combatant commands. Although some material is restricted to Department of Defense personnel, much of the information and training provided by the Information Assurance Support Environment is available to the general public.

Information Evaluation (Source Reliability and Content Validity)

Information used to develop intelligence comes from a variety of sources, with a wide degree of reliability and credibility. It is the job of the intelligence analyst to use these sources of information to build an accurate and up-to-date picture of the current situation and operational environment in order to allow users of produced intelligence products to make informed decisions.

In order to produce accurate intelligence products the information fed into the intelligence cycle must be evaluated for reliability and accuracy. In intelligence reporting information is evaluated and assigned an alphanumeric designation which reflects the reliability of the source of the
information based on past experience and the accuracy of the information provided as it relates to other information already known.

There are two standardized systems of information evaluation: the LEIU Criminal Intelligence File Guidelines and the NATO STANAG 2022 military guideline.

The LEIU Criminal Intelligence File Guidelines provide the following standard for source / information evaluation:

"Information to be retained in the criminal intelligence file should be evaluated and designated for reliability and content validity prior to filing. The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Circulating information which may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to the individual's right to privacy. To ensure uniformity with the intelligence community, it is strongly recommended that stored information be evaluated according to the criteria set forth below.

**Source Reliability:**

(A) Reliable - The reliability of the source is unquestioned or has been well tested in the past.

(B) Usually Reliable - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.

(C) Unreliable - The reliability of the source has been sporadic in the past.

(D) Unknown - The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

**Content Validity:**

(1) Confirmed - The information has been corroborated by an investigator or another independent, reliable source.

(2) Probable - The information is consistent with past accounts.

(3) Doubtful - The information is inconsistent with past accounts.

(4) Cannot Be Judged - The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

The military uses a similar system of evaluation based on the letters A-F and the numbers 1-6, as referenced in NATO STANAG 2022, and various other military publications.
Reliability of Source | Accuracy of Information
--- | ---
A – Completely Reliable | 1 – Confirmed By Other Source
B – Usually Reliable | 2 – Probably True
C – Fairly Reliable | 3 – Possibly True
D – Not Usually Reliable | 4 – Doubtful
E – Unreliable | 5 – Improbable
F – Reliability Cannot Be Judged | 6 – Truth Cannot Be Judged

(Re: Appendix B, FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations)

Because both the LEIU and the military system are each widely used it is important to differentiate between the two systems in intelligence reports. Failure to do so can result in confusion. For example is an evaluation of C3 a fairly reliable source providing possibly true information or an unreliable source providing doubtful information? To avoid this confusion, evaluation rating is best listed, for example, as C3 (LEIU) or C3 (MIL).

**Information Security Oversight Office (ISOO)**


The Information Security Oversight Office (ISOO) is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. ISOO is a component of the National Archives and Records Administration (NARA) and receives policy and program guidance from the National Security Council (NSC).

**Information Sharing Environment**


Improving information sharing constitutes a cornerstone of our national strategy to protect the American people and our institutions and to defeat terrorists and their support networks at home and abroad. The Implementation Plan for the Information Sharing Environment sets forth the following vision: "A trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States by the effective and efficient sharing of terrorism and homeland security information."
ISE Core Awareness Training


Organizational cultures across the ISE vary widely, and information sharing is not viewed across the board as a required behavior. To promote a shared awareness of the ISE and encourage such behavior, on July 16, 2008, the PM-ISE issued the ISE Core Awareness Training Course to Federal departments and agencies. The course is intended to give a common understanding of the ISE to all employees who support the counterterrorism mission. This training, coupled with continued efforts to include information sharing as a formal evaluation factor in personnel performance reports and agency incentive programs, is designed to help move the traditional "need to know" culture to one based on a "responsibility to provide."

Information Systems Security Association (ISSA)

URL:  http://www.issa.org/

Information Systems Security Association (ISSA) a not-for-profit, international professional organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

InfraGard

URL:  http://www.infragard.net/

Member log-in -- https://igc.infragard.org/

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and government agencies. The mission of the National InfraGard is to facilitate the sharing of information and analysis to improve the nation's ability to prevent, deter and investigate cyber-based crime and other criminal activity. InfraGard is a network of thousands of volunteers at the grassroots level who are committed to sharing information and enhancing the nation's ability to combat cyber-based crimes and other criminal activity.
enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories.

**In-Q-Tel**
P.O. Box 749  
Arlington, VA 22216  
Telephone: 703-248-3000  
Fax: 703-248-3001  
Email: info@iqt.org

URL: [http://www.iqt.org/](http://www.iqt.org/)


Throughout its lifetime, the CIA has operated at the cutting edge of science and technology. From the U-2 spy plane to the CORONA satellite, CIA's "wizards of Langley" earned a reputation for bold innovation and risk taking, working in advance of the private sector and other branches of government. Much of CIA's technology success was a result of identifying gaps and opportunities.

By the late 1990s, the pace of commercial IT innovation was outstripping the ability of government agencies—including the CIA—to access and incorporate. This commercial innovation was driven by private sector R&D investment which placed billions of dollars, and the nation's top talent, behind commercial technology development.

In 1998, CIA identified technology as a top strategic priority, and set out a radical plan to create a new venture that would help increase the Agency's access to private sector innovation. In-Q-Tel was chartered in February 1999 by a group of private citizens at the request of the Director of Central Intelligence and with the support of the U.S. Congress. IQT was tasked with building a bridge between the Agency and a new set of technology innovators.

**INSCOM** – See: Army Intelligence and Security Command (INSCOM)
INSCOM Intelligence Analyst Training Program

URL:  https://www.us.army.mil/suite/page/444525 (Requires AKO Log-in)

- What is Intelligence?
- INSCOM Overview
- Intelligence Community
- Boolean Logic for Search Engines
- Arabic Naming Conventions
- Analysts Notebook Applied
- Visual Analytics
- ArcGIS Converting Coordinates

- ArcGIS Data Types
- ArcGIS Projection, Datum, & Coordinate Systems
- ArcGIS Map Scale
- Critical Thinking
- CTAC Link Analysis
- CTAC Biases
- CTAC IPB

IntelCenter

URL:  http://www.intelcenter.com/

The IntelCenter focus is on studying terrorist groups and other threat actors and disseminating that information in a timely manner to those who can act on it. The IntelCenter looks at capabilities and intentions, warnings and indicators, operational characteristics and a wide variety of other points in order to better understand how to interdict terrorist operations and reduce the likelihood of future attacks.

The results of this work is then disseminated in a variety of Alert, Current Intelligence and Analytical Resource services. It also provides the foundation for our field books such as the "First Responder Chem-Bio Handbook." The IntelCenter's primary client base is comprised of military, law enforcement and intelligence agencies in the US and other allied countries around the world.
Intellink

URL:  https://www.intelink.gov/

Intelink is both an architectural framework and an integrated intelligence dissemination and collaboration service providing uniform methods for exchanging intelligence among intelligence providers and users. The Intelink service was patterned after the Internet model in which a variety of institutions have come together in the context of a global network to share information.

The Intelink intelligence network links information in the various classified databases of the US intelligence agencies (e.g. FBI, CIA, DEA, NSA, USSS, NRO) to facilitate communication and the sharing of documents and other resources.

Intelligence

“Intelligence is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.” (Joint Pub 2-0, Joint Intelligence, 22 June 2007)

"Intelligence sources can be people, documents, equipment, or technical sensors, and are grouped according to one of the seven major intelligence disciplines: geospatial intelligence (GEOINT); human intelligence (HUMINT); signals intelligence (SIGINT); measurement and signature intelligence (MASINT); open-source intelligence (OSINT); technical intelligence (TECHINT); and counterintelligence (CI)." (Joint Intelligence. JP 2-0. p.I-5, (22 June 2007)

GEOINT - Geospatial Intelligence - 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.(JP 1-02)

HUMINT - Human Intelligence - The intelligence derived from the intelligence collection discipline that uses human beings as both sources and collectors, and where the human being is the primary collection instrument. (Also called Human Resources Intelligence) (JP 1-02)

SIGINT - Signals Intelligence - A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. (JP 1-02)
MASINT - Measurement and Signature Intelligence - Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. (JP 1-02)

OSINT - Open-Source Intelligence - Information of potential intelligence value that is available to the general public. (JP 1-02)

TECHINT - Technical Intelligence - Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary’s technological advantages. (JP 1-02)

CI - Counterintelligence - Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Intelligence Advanced Research Projects Activity

URL: http://www.iarpa.gov/

The Intelligence Advanced Research Projects Activity (IARPA) invests in high-risk/high-payoff research programs that have the potential to provide our nation with an overwhelming intelligence advantage over future adversaries.

IARPA reports to the Office of the Director of National Intelligence's Director of Science and Technology (ODNI/DS&T)

IARPA by design does not have an operational mission, and its focus is on capabilities that the user community might want in the future, not on the requirements they have today

IARPA has three offices:

- Office of Smart Collection
- Office of Incisive Analysis
- Office of Safe & Secure Operations

There is clearly overlap across all three offices. Offices at IARPA should not be viewed as separate or independent entities. They have been established to span the space of the important
technical challenges the intelligence community will need to address in the future. It is expected that there will be significant collaboration among Program Managers within and across offices.

**Intelligence Analysis: Behavioral and Social Scientific Foundations**


**Intelligence Analyst Certified (IAC)**

American Board of Intelligence Analysts


**Phase I** - This course is designed for intelligence community analysts responsible for analyzing information and making decisions in intelligence related organization. The goal is to ensure Intelligence Analysts have a basic understanding of U.S. Intelligence Community from its inception to the present, in addition to the intelligence cycle and various forms of intelligence collection. A key component of the course is the legislation and executive orders creating the various members of the community, its members, and the roles they play in the Intelligence Community. Additionally, the role Congress plays in control and oversight of intelligence operations is beneficial to ensure the intelligence analyst understands expectations of U.S. laws and lawmaker overseers. Finally, the role of the Director of National Intelligence will be examined, coupled with understanding the ongoing restructuring of the intelligence community in the wake of 9/11.

**Phase II** - This course is designed for intelligence community analysts responsible for analyzing information and making decisions in intelligence related organization. The goal is to ensure a basic understanding of Intelligence Analysis is possessed by an individual seeking a certification in Basic Intelligence Analysis and Decision Making. This certification course examines the cultural and psychological biases which impact the objectivity of the intelligence process and decision-making with regard to their usefulness of intelligence products within today’s government, military, civil, and business organizations. Human information processing and problem solving will be discussed from a psychological perspective, as well as psychological factors influencing the information processing of the individual Analyst. Limitations of memory and attention, and effects of categorization and summarization of information on intelligence analysis will be determined. The students will review intelligence processes and inferences about cognitive sciences and decision-making processes. The course will identify ways of countering these psychological mechanisms, and students will acquire tools in order to improve the objectivity of intelligence analysis that influences the individual analyst during each stage of the intelligence cycle.
Phase III - This certification course is designed for intelligence community analysts responsible for analyzing information and making decisions in intelligence related organizations. The goal is to ensure an in-depth understanding of how critical thinking skills affect daily analysis of information. These skills are paramount and should be possessed by an individual seeking a certification in Critical Thinking and Intelligence Analysis. This certification course examines the definition of critical thinking, the standards of critical thinking, and skill-based definitions to further help an analyst understand the components of critical thinking. Using historical situations related to the intelligence community of past like the Soviet Missile Crisis in Cuba, this certification course will help an intelligence analyst understand how to employ critical thinking in analysis situations. Additionally, analysts will understand how to think critically, coupled with the cost and benefits of thinking critically and how critical thinking can transform current and future analytical analysis and decision making. Furthermore, the analyst will review key methodologies, learn how to assess evidence in a whole new light, and comprehend creating better inferences when employing critical thinking.

For more information, please contact the American Board of Intelligence Analysts at:

Email: cao@abchs.com
Telephone: 877-219-2519

Intelligence Analyst Course (US Army Correspondence Course Program)

Advanced Intelligence Analyst Course


This US Army Correspondence Course Program (ACCP) Course contains the sub-courses listed below:

- IT0478, Intelligence Support of Division Operations (8 credit hours)
- IT0480, Intelligence in Support of Internal Defense Operations (6 credit hours)
- IT0583, Strategic Intelligence (10 credit hours)
- IT0559, Perform and Supervise Duties and Functions in the Intelligence Center (8 credit hours)
- IT0560, The Collection Effort (8 credit hours)
- IT0425, Introduction to Battlefield Technical Intelligence (6 credit hours)
- IS3007, Electronic Warfare (6 credit hours)

Basic Intelligence Analyst Course (Course Revised 16 March 2009)
This US Army Correspondence Course Program (ACCP) Course consists of five (5) sub-courses:

- IT0426, Weather Support to Tactical Operations (4 credit hours)
- IT0462, Intelligence Preparation of the Battlefield (12 credit hours)
- IT0565, Preparation of the Intelligence Estimate (6 credit hours)
- IT0566, Prepare Analysis of the Battlefield Area (8 credit hours)
- IT0550, Introduction to the Intelligence Analyst (6 credit hours)

Course material is publically available, however formal enrollment is only available to U.S. Active and Reserve military officers, warrant officers, and enlisted personnel; Reserve Officers' Training Corps, National Guard Officer Candidate School, West Point cadets, and authorized federal civilian employees.

**Intelligence Analyst Training Program (IATP)**

The Counter Terrorism Division (CTD) of the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia, is home to the Intelligence Analyst Training Program (IATP). CTD is responsible for the training of intelligence analysts and intelligence associated personnel from Partner Organizations. The program is open to military, state, and local law enforcement intelligence personnel on a space available basis.

The 76 hour program provides a historical, legal, and conceptual basis for criminal/law enforcement intelligence. The beginning of the program establishes a firm historical, legal and ethical basis. IATP contains a practical exercise devoted to critical thinking concepts and the three components of analysis. IATP is designed around the intelligence process/cycle through the creation of requirements as the basis of an intelligence plan, devoted to the Planning and Direction phase, followed by the collection and documentation of information with the Collection Phase. IATP then transitions into the phases of processing and exploitation, analysis, dissemination and re-evaluation as the baseline process for transitioning information into intelligence. The program is structured around the Intelligence Cycle, identifying functions the analyst /research specialist is involved with during each phase. The IATP is conducted in a student centered learning environment, guided by subject matter experts in various fields.

The student is evaluated on the basic concepts of analysis, presentation skills, and writing abilities. The final practical exercise is devoted towards bringing together all teaching points, combining the fundamentals of analysis with a law enforcement problem area. This practical exercise culminates with the submission of both a report and presentation of a briefing of the student's findings to the class, instructors, and interested FLETC staff.
Type: Advanced

Length: The training program encompasses 9.5 days (76 hours).

- Curriculum
- Introduction to Law Enforcement Intelligence
- The Intelligence Cycle
- Intelligence Analysis: Core Competencies
- Introduction to Intelligence Analysis
- Legal Issues for Intelligence Analysts
- Intelligence Plans
- Digital Officer Safety & Operations Security (OPSEC)
- External Information Sources
- Electronic Sources of Information For Law Enforcement
- Analytical Methods & Techniques
- Report Writing for Analysts
- Introduction to Electronic Worksheets and Graphs
- Financial Aspects of Criminal Investigations
- Geographic Information Systems and Geographical Profiling
- Analytical Products and Presentations
- Practical Exercise Laboratory, Preparation and Presentation

POC for course information

Senior Instructor
Counterterrorism Division
1131 Chapel Crossing Rd.
Glynco GA 31524 Phone:
Telephone: 912-267-2347
Fax: 912-267-3144
E-mail: fletc-counterterrorismdivision@dhs.gov

**Intelligence & National Security Alliance (INSA)**

URL: [http://www.insaonline.org/](http://www.insaonline.org/)

INSA is the premier not-for-profit, nonpartisan, private sector professional organization providing a structure and interactive forum for thought leadership, the sharing of ideas, and networking within the intelligence and national security communities. INSA has over 100
corporate members, as well as several hundred individual members, who are industry leaders within the government, private sector, and academia.

**Intelligence Community**


The Intelligence Community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. These activities include:

- Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;
- Production and dissemination of intelligence;
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the US, international terrorist and international narcotics activities, and other hostile activities directed against the US by foreign powers, organizations, persons, and their agents;
- Special activities;
- Administrative and support activities within the US and abroad necessary for the performance of authorized activities; and
- Such other intelligence activities as the President may direct from time to time.
The 17 member agencies of the Intelligence Community are:

- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy
- Department of Homeland Security
- Department of State
- Department of the Treasury
The U.S. Intelligence Community is a federation of executive branch agencies and organizations
that work—both together and separately—to conduct intelligence activities necessary for the
conduct of foreign relations and the protection of the national security of the United States.
While the U.S. Intelligence Community is a large and complex organization, its primary mission
is clear cut: to collect and convey essential information needed by the President and other
members of the U.S. policymaking, law enforcement, and military communities for the
performance of their duties and responsibilities. This includes collecting and assessing
information concerning international terrorist and narcotic activities; other hostile activities by
foreign powers, organizations, persons, and their agents; and foreign intelligence activities
directed against the United States. The President also may direct the Intelligence Community to
undertake special activities, including covert action, as needed to support intelligence collection
activities and to protect against foreign threats to U.S. security interests.
The purpose of the following discussion is to provide an overall picture of the U.S. Intelligence Community today and how it functions. It is intended as a primer for readers who may be unfamiliar with the subject.


**Intelligence Cycle**

The intelligence cycle is the process of developing unrefined data into polished intelligence for the use of policymakers. The intelligence cycle consists of six steps, described below. The graphic below shows the circular nature of this process, although movement between the steps is fluid. Intelligence uncovered at one step may require going back to an earlier step before moving forward.

**Requirements** are identified information needs—what we must know to safeguard the nation. Intelligence requirements are established by the Director of National Intelligence according to guidance received from the president and the national and homeland security advisors. Requirements are developed based on critical information required to protect the United States from national security and criminal threats. The attorney general and the Director of the FBI participate in the formulation of national intelligence requirements.

**Planning and Direction** is management of the entire effort, from identifying the need for information to delivering an intelligence product to a consumer. It involves implementation plans to satisfy requirements levied on the FBI, as well as identifying specific collection requirements based on FBI needs. Planning and direction also is responsive to the end of the cycle, because
current and finished intelligence, which supports decision-making, generates new requirements. The executive assistant director for the National Security Branch leads intelligence planning and direction for the FBI.

**Collection** is the gathering of raw information based on requirements. Activities such as interviews, technical and physical surveillances, human source operation, searches, and liaison relationships result in the collection of intelligence.

**Processing and Exploitation** involves converting the vast amount of information collected into a form usable by analysts. This is done through a variety of methods including decryption, language translations, and data reduction. Processing includes the entering of raw data into databases where it can be exploited for use in the analysis process.

**Analysis and Production** is the conversion of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information’s reliability, validity, and relevance is evaluated and weighed. The information is logically integrated, put in context, and used to produce intelligence. This includes both "raw" and finished intelligence. Raw intelligence is often referred to as "the dots"—individual pieces of information disseminated individually. Finished intelligence reports "connect the dots" by putting information in context and drawing conclusions about its implications.

**Dissemination**—the last step—is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements. The FBI disseminates information in three standard formats: Intelligence Information Reports (IIRs), FBI Intelligence Bulletins, and FBI Intelligence Assessments. FBI intelligence products are provided daily to the attorney general, the president, and to customers throughout the FBI and in other agencies. These FBI intelligence customers make decisions—operational, strategic, and policy—based on the information. These decisions may lead to the levying of more requirements, thus continuing the FBI intelligence cycle.


**Intelligence Guide for First Responders**

Interagency Threat Assessment and Coordination Group (ITACG)

Intelligence Knowledge Network (IKN)

URL:  https://icon.army.mil/  (Requires AKO Login)

IKN is a Knowledge Management tool that enables Intelligence soldiers all over the world to communicate, collaborate and investigate. It hosts discussion forums, serves as a single point of entry to get to USAIC and other Intelligence Community websites, and hosts a variety of public and private web applications that support the Intelligence Community.

Intelligence Officer's Handbook - TC 2-50.5 (January 2010)

URL:  https://armypubs.us.army.mil/doctrine/DR_pubs/dr_b/pdf/tc2_50x5.pdf  (AKO Required)

Intelligence Oversight

URL:  http://atsdio.defense.gov/

The perceived need for a Department of Defense (DoD) Intelligence Oversight (IO) program came about as a result of certain activities conducted by DoD intelligence and counter-intelligence units against U.S. persons involved in the Civil Rights and anti-Vietnam War movements. During the 1960s and 1970s, the United States experienced significant civil demonstrations from protesters associated with these movements. Some of these demonstrations were believed to be beyond the ability of civilian authorities to control, and military forces were used to assist in the restoration of order. Units deploying for this purpose discovered they needed basic pre-deployment intelligence to perform their missions. The Army, designated as executive agent for providing aid to civilian authorities, requested assistance from the Federal Bureau of Investigation (FBI). When the FBI was unable to provide the information needed, the Army began collecting it. Over time, this collection mushroomed and led to abuse of the Constitutional rights of our citizens. Eventually, DoD intelligence personnel were using inappropriate clandestine and intrusive means to collect information on the legitimate political positions and expressions of U.S. persons, accumulating that information in a nationwide data bank, and sharing that information with law enforcement authorities. For example, during the 1960s and 1970s:
- Military counterintelligence special agents established, maintained, and disseminated files on civil rights activists and organizers. These were not legitimate DoD targets.
- Counterintelligence special agents penetrated organizations such as the "Resistors in the Army" and the "Friends of Resistors in the Army" and recruited members of these organizations as informers. These organizations posed no foreign threat.
- So called "dissidents", actually U.S. persons who were exercising their First Amendment rights, were placed under surveillance and their movements were observed and recorded. These U.S. persons were not legitimate DoD counterintelligence targets.
- Radio communications of civil rights and anti-war demonstrators were intercepted by military intelligence personnel. The interception of these communications was improper.
- Using media cover, military counterintelligence special agents infiltrated the 1968 Democratic National Convention in Chicago. There was no legitimate Defense investigative purpose for this action.
- Information collected by Defense elements was routinely transferred to civilian law enforcement authorities without evidence of criminal activity or relevance to the law enforcement missions of the receiving authorities. This activity was improper.

In the early and mid 1970s several Congressional committees, including the Church, Pike, and Ervin committees, conducted investigations and public hearings. After three and a half years of investigation, these committees determined that what had occurred was a classic example of what we would today call "mission creep." What had begun as a simple requirement to provide basic intelligence to commanders charged with assisting in the maintenance and restoration of order, had become a monumentally intrusive effort. This resulted in the monitoring of activities of innocent persons involved in the constitutionally protected expression of their views on civil rights or anti-war activities. The information collected on the persons targeted by Defense intelligence personnel was entered into a national data bank and made available to civilian law enforcement authorities. This produced a chilling effect on political expression by those who were legally working for political change in domestic and foreign policies. Senator Ervin concluded "the collection and computerization of information by government must be tempered with an appreciation of the basic rights of the individual, of his right to privacy, to express himself freely and associate with whom he chooses." As a result of these investigations, DoD imposed severe restrictions on future surveillance of U.S. persons, required that information already in DoD files be destroyed, and established a structure to regulate future DoD intelligence collection.

In 1976, President Ford issued an Executive Order placing significant controls on the conduct of all intelligence activities. Executive Order (EO) 11905, as the charter for the Intelligence Community, included provisions for an intelligence oversight mechanism. Consequently, the Secretary of Defense directed establishment of an Inspector General for Intelligence in the Office of the Secretary of Defense, responsible for the independent oversight of all DoD intelligence activities. EO 12036, signed by President Carter in 1978, and the current Executive Order, EO
12333, signed by President Reagan in 1981, continued the requirement for oversight to maintain the proper balance between the acquisition of essential information by the Intelligence Community, and the protection of individuals' constitutional and statutory rights.

In November 1982, following the establishment of the DoD Inspector General, the Deputy Secretary of Defense directed that the Inspector General for Intelligence be re-designated as the Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD (IO)). Today, the ATSD (IO) reports on Intelligence Oversight activities at least quarterly to the Secretary of Defense and, through him, to the Intelligence Oversight Board (IOB), a standing committee of the President's Foreign Intelligence Advisory Board (PFIAB).

The ATSD (IO) is responsible to the Secretary of Defense for the independent oversight of all intelligence, counterintelligence, and intelligence-related activities in the Department of Defense. The organization's charter can be found in DoD Directive 5148.11. The ATSD (IO) ensures that all activities performed by intelligence, counterintelligence, and intelligence related units are conducted in accordance with Federal law, Executive Orders, DoD directives, regulations and policies.

**Intelligence Support Activity (ISA)**

URL: [http://www.specwarnet.net/americas/isa.htm](http://www.specwarnet.net/americas/isa.htm)

The United States Army Intelligence Support Activity (USAISA), frequently shortened to Intelligence Support Activity or ISA, and nicknamed The Activity is a United States Army Special Operations unit originally subordinated to the US Army Intelligence and Security Command (INSCOM). It is tasked to collect actionable intelligence in advance of missions by other US special operations forces, especially Delta Force and DEVGRU in counter-terrorist operations.

Perhaps the least known, and most classified unit within the realm of US special operations is the Intelligence Support Activity, a small, highly trained and capable intelligence unit. The amount of accurate and up-to-date information about the ISA is very small, due to the extremely high secrecy surrounding the unit, but over the years, various books and reports have gleaned some information about the ISA.

The ISA's origins are in the Foreign Operating Group (FOG), whose origin in turn is in the 1979 overthrow of Nicaraguan dictator Anastasio Somoza. The rapidly deteriorating situation in the country prompted the United States to create a small Special Forces unit with the purpose of surveying the US embassy. Operators from the unit entered Nicaragua using false passports, and proceeded to photograph the embassy from every angle, record the types of locks on all doors,
inside and outside, record the number of exits and windows, and finally drew up the internal
layout of the building. The survey was successful, which led defense officials to create ad hoc
Special Forces units to survey US embassies in hotspots around the world. Ironically, the
embassy in Iran was on their itinerary, but, history intervened, and it was overrun by a mob who
took the larger part of the staff hostage.

When the first rescue attempt of the hostages in Iran failed, a second attempt, code-named Honey
Badger, immediately started. One problem that plagued the first attempt was the lack of valuable
intelligence. The CIA proved unable to provide the critical intelligence Delta Force needed, such
as the number of guards, the type of weapons they were using and what kinds of locks were on
the doors. The second rescue force was not going to be affected by the same problem, and the
FOG was established in July of 1980, under the control of Colonel Jerry King. In the summer of
1980, FOG agents were infiltrated into Teheran to report back on the hostages’ whereabouts,
movements of the Iranians, as well as to recruit local agents. Unfortunately, the hostages were
dispersed throughout the country, and the chance never came for a second attempt, but the seeds
were planted for the Intelligence Support Activity. (See URL for complete article.)

Intellipedia

Intellipedia is a wiki used by partners within the Intelligence, Defense, Homeland Security, Law
Enforcement, and Diplomatic Communities. It is one of the Office of the Director of National
Intelligence's (ODNI) Intelligence Community Enterprise Services (ICES) portfolio of Intelink
services. Three versions exist on the different networks: JWICS (Intellipedia-TS); SIPRNet
(Intellipedia-S); and DNI-U/Intellipedia-U. Contributors to Intellipedia are called
Intellipedians. Intellipedia-U allows users to easily integrate and interlink knowledge into
interagency, topical-based articles and collaborate on issues up to UNCLASSIFIED / SBU /
FOUO / LES or other "controlled unclassified information".

INTELST Info-Sharing Forum

URL: https://www.us.army.mil/suite/page/228144

URL: https://listserv.army.pentagon.mil/

The INTELST provides an information-sharing forum to discuss current and future intelligence
document, and to share and request ideas, and tactics, techniques and procedures (TTPs) between
intelligence professionals at all levels. Additionally, the INTELST now has a new website
(https://listserv.army.pentagon.mil/) with word searchable archives organized by discussion
subjects accessible via the website (You must be an INTELST member in order to access the website).

Discussions subjects on the INTELST have covered a wide range of topics, to include: Actionable Intelligence, Asymmetric warfare, AAR’s & Lessons Learned from OIF and OEF, Army and Joint Transformation and its impacts on intelligence requirements and structure, current and future MI force structures and requirements, the training of intelligence analysts, Effects Based Operations (EBO), Geospatial Intelligence (GEOINT), HUMINT and current intelligence force structures, UAVs, professional Recommended Reading Lists, FM 2-0 Intelligence series of field manuals issues, battlefield visualization, intelligence and the MDMP, Information Operations, open source intelligence (OSINT), Intelligence Preparation of the Battlefield (IPB), Operations Security (OPSEC), intelligence sharing with LEOs, targeting, and intelligence architectures and systems in general.

The INTELST has over 2,100 members all over the world, and at all levels of command and rank. The INTELST membership is composed of intelligence professionals from across the spectrum of the military and civilian intelligence worlds.

The INTELST (List server acronym for "Intel List") is an email address to which you send a message that is automatically distributed, after moderator approval and release, to everyone on the list. After you are signed up, you will receive a welcome message with instructions on how to use the INTELST, the INTELST website, and the INTELST Rules of Engagement. The INTELST uses the NIPRNET, so all content of the messages must remain unclassified. The INTELST is a closed list, and only those who are subscribed are authorized to post or receive notes sent to the list.

The INTELST can come to you in one of three versions: individual emails, a once-a-day digest with all the messages included, or a once-a-day index hyperlinked to the archives on the website. There can be anywhere from 3-5 emails up to as many as 30-50 emails per day, so a lot of busy folks either get the digest or index versions, or do not receive mail and check the archived messages on the website.

If you are interested in joining the INTELST send an email (your AKO/us.army.mil address is preferred) to INTELST.Forum@us.army.mil

**Interagency Language Roundtable**

URL: [http://www.govtilr.org/](http://www.govtilr.org/)

The Interagency Language Roundtable (ILR) is an unfunded Federal interagency organization established for the coordination and sharing of information about language-related activities at the Federal level.
It serves as the premier way for departments and agencies of the Federal government to keep abreast of the progress and implementation of techniques and technology for language learning, language use, language testing and other language-related activities.

**Interagency OPSEC Support Staff (IOSS)**

URL: [http://www.ioss.gov](http://www.ioss.gov)

In 1988, President Ronald Reagan signed National Security Decision Directive 298 (NSDD 298). This directive established the National Operations Security Program as a means to identify, control, and protect unclassified information and evidence associated with U.S. national security programs and activities. Adversaries or competitors working against the interests of the United States can exploit this information if it is not properly protected.

The NSDD 298 named the Director, National Security Agency, as the Executive Agent for interagency OPSEC training and included in his responsibilities the establishment and maintenance of the Interagency OPSEC Support Staff. By mandate, this organization shall include representatives from the Federal Bureau of Investigation, Central Intelligence Agency, Department of Energy, and Department of Defense, including the National Security Agency. Other government agencies are encouraged to provide personnel to this staff and participate in interagency OPSEC forums.

The primary responsibility of the Interagency OPSEC Support Staff (IOSS) is to act as a consultant to other U.S government departments or agencies by providing technical guidance and assistance that will result in self-sufficient OPSEC programs for the protection of the U.S. operations. Members of the IOSS staff assess OPSEC programs, assist in OPSEC program development, conduct surveys, and provide training.

The IOSS further supports the National OPSEC Program by providing multimedia products and presenting events that attract attendees from the security, intelligence, research and development, acquisition, and law enforcement communities. These events include the National OPSEC Conference and Exhibition, the National Threat Symposium, and regional training symposia.

**International Association for Intelligence Education (IAFIE)**

URL: [http://www.iafie.org/](http://www.iafie.org/)

The mission of the Association is to advance research, knowledge and professional development in intelligence education. IAFIE was formed in June 2004 as a result of a gathering of sixty plus intelligence studies trainers and educators at the Sixth Annual International Colloquium on
Intelligence at Mercyhurst College in Erie, Pennsylvania. This group, from various intelligence disciplines including national security, law enforcement and competitive intelligence, recognized the need for a professional association that would span their diverse disciplines and provide a catalyst and resources for their development and that of Intelligence Studies.

**International Association of Crime Analysts**

URL: [http://www.iaca.net/](http://www.iaca.net/)

The International Association of Crime Analysts was formed in 1990 to help crime analysts around the world improve their skills and make valuable contacts, to help law enforcement agencies make the best use of crime analysis, and to advocate for standards of performance and technique within the profession itself. IACA membership is around 1,500 members and climbing. Members include crime analysts, intelligence analysts, police officers of all ranks, educators, and students.

**International Association of Law Enforcement Intelligence Analysts**

PO Box 13857
Richmond, VA 23225

URL: [http://www.ialeia.org/](http://www.ialeia.org/)

IALEIA is the largest professional organization in the world representing law enforcement analysts. It is based in the United States, and is a non-profit 501-c-3 corporation. IALEIA is managed by an international Board of Directors made up of seventeen elected IALEIA members. Several board members are also supported by volunteer committees. IALEIA has a paid administrator, and an Executive Advisory Board appointed by the President. IALEIA supports chapters throughout the world, in accordance with a policy manual. IALEIA has a certification program for analysts, a code of ethics and bylaws providing structure for the organization.

**International Counter-Terrorism Officers Association (ICTOA)**

URL: [http://www.ictoa.org/](http://www.ictoa.org/)

The International Counter-Terrorism Officers Association (ICTOA) is a Non-Profit association founded by members of the New York City Police Department. The ICTOA is comprised of law enforcement personnel, firefighters, military, first responders, private/corporate security, and other related professionals.
International Security Research and Intelligence Agency (ISRIA)

URL:  http://www.isria.com/index.php

Founded in Paris in 2004, ISRIA is a consulting and information publishing service. The firm’s consulting arm focuses on information analysis, research and global intelligence. ISRIA.com provides daily open source intelligence, public domain and diplomatic materials on geopolitical, security and world politics issues. ISRIA analysts are based around the globe, including in the U.S.

International Spy Museum

URL:  http://www.spymuseum.org/

The International Spy Museum opened in Washington, DC on July 19, 2002. It is the only public museum in the United States solely dedicated to espionage and the only one in the world to provide a global perspective on an all-but-invisible profession that has shaped history and continues to have a significant impact on world events. The Museum features the largest collection of international espionage artifacts ever placed on public display. Many of these objects are being seen by the public for the first time. These artifacts illuminate the work of famous spies and pivotal espionage actions as well as help bring to life the strategies and techniques of the men and women behind some of the most secretive espionage missions in world history. The mission of the International Spy Museum is to educate the public about espionage in an engaging way and to provide a context that fosters understanding of its important role in and impact on current and historic events. The Museum focuses on human intelligence and reveals the role spies have played in world events throughout history. It is committed to the apolitical presentation of the history of espionage in order to provide visitors with nonbiased, accurate information.

Internet Crime Complaint Center

URL:  http://www.ic3.gov/

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA). IC3’s mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the
victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

**Internet Fraud Alert Program**

**URL:** [http://ifraudalert.org/](http://ifraudalert.org/)

Internet Fraud Alert is a collaborative project between public and private entities to help protect consumers from online fraud. Internet Fraud Alert is made possible through the support and participation of these and other organizations:

- National Cyber-Forensics and Training Alliance (NCFTA)
- Microsoft
- Accuity
- Citizens Bank
- American Bankers Association (ABA)
- Anti-Phishing Working Group (APWG)
- eBay/Paypal

**INTERPOL**

**URL:** [http://www.interpol.int/](http://www.interpol.int/)

INTERPOL is the world’s largest international police organization, with 188 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.

Each INTERPOL member country maintains a National Central Bureau staffed by national law enforcement officers. The NCB is the designated contact point for the General Secretariat, regional offices and other member countries requiring assistance with overseas investigations and the location and apprehension of fugitives.
Introduction to Cyber Investigations (DE-ICI)

Distance Education – Online -
Duration: 40 Hours / 5 Weeks
URL: http://www.dc3.mil/dcita/courseDescriptions/de-ici.php

This course presents the processes, techniques, specialized documentation, legal guidelines and requirements for conducting a basic cyber crime investigation through the use of lecture, practical exercises, scenarios and case studies. Please note: This course does not provide the depth needed to conduct an advanced cyber crime investigation (i.e., Intrusions).

Topics Covered:

Introduction to Cyber Investigations Technical Fundamentals

- IP Addresses
- Uniform Resource Locators
- Metadata and Logs
- E-Mail and Newsgroups
- Browser Evidence

Legal Fundamentals

- Authority to Search, Gather Records and Intercept Communications
- Prosecution of Cyber Crime

Special Aspects of Cyber Case Management

- On-Scene and Online Evidence Collection
- Cyber Forensic Laboratory Support Cyber Interviews
- Covert Online Investigations

Subjects of Cyber Investigations

- Motivations for Cyber Crime
- Military, Corporate and International Subject

ISRIA: See - International Security Research and Intelligence Agency (ISRIA)
JavaScript Browser Based Cryptography Tools

Fourmilabs Switzerland [http://www.fourmilab.ch/](http://www.fourmilab.ch/) is a web-site developed and maintained by John Walker, founder of Autodesk, Inc. and co-author of AutoCAD. While this web-site offers many interesting items, from the security viewpoint we are interested in the ‘Cryptography and Steganography’. The JavaScript Browser Based Cryptography Tools are easy to use, work on any computer that can handle JavaScript, and offer a good level of security for e-mail communication. [http://www.fourmilab.ch/javascrypt/](http://www.fourmilab.ch/javascrypt/) The encryption program is provided free of charge and has according to the web-site has been placed into the public domain.

"From the web-site: JavaScrypt runs entirely in your browser--nothing is sent to any Web site when you use it. You can, if you wish, download JavaScrypt to your own computer and use it when not connected to the Internet. JavaScrypt's encryption facilities use the Advanced Encryption Standard (AES) adopted by the United States as Federal Information Processing Standard 197. AES supports key lengths of 128, 192, and 256 bits; JavaScrypt uses 256 bit keys exclusively."

Joint Intelligence Course
(Doctrine Networked Education & Training)


Fundamentals and principles for the conduct of joint intelligence operations; overview of the joint intelligence process; and a review of intelligence organizations and their respective roles and responsibilities (1 hr 24 min)

Joint Intelligence

Joint Publication 2-0 (22 June 2007)

URL: [http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf)
Joint Intelligence Virtual University

(U) The Joint Intelligence Virtual University (JIVU) is the premier collaborative online training environment, designed especially to meet the needs of the Intelligence Community and to provide easy access to high-quality e-Learning products, tools, and services. Providing over 4000 courses, JIVU serves as an online learning platform for the Defense Intelligence Agency (DIA) and approximately 17 other IC Agencies, Commands and Services. JIVU utilizes the Plateau Learning Management System and the Central tool to deliver online learning content. It is accessible 24/7 on the Joint Worldwide Intelligence Communications System (JWICS) at http://jivu.dodiis.ic.gov, the Secret Internet Protocol Router Network (SIPRNet) at http://jivu.dse.dia.smil.mil, and StoneGhost at http://www.jivu.us.qlat (Link will only work when logged onto a native StoneGhost terminal).

Joint Knowledge On-Line (JKO)

URL:  http://jko.jfcom.mil/

JKO is the enterprise portal system providing convenient access to online joint training and information resources. JKO integrates with other DoD systems and uses the latest advanced distributed learning technologies to provide training courses and resources that better prepare warfighters for joint exercises and integrated operations.

Courses are available on any standard browser or operating system worldwide 24/7.

JKO also offers an Internet Public site. JKO-IP http://jko.cmil.org/ is the public access enterprise portal of the Joint Knowledge Development and Distribution Capability (JKDDC) Training Transformation initiative, managed by the JKDDC Joint Management Office (JMO) at the U. S. Joint Forces Command Joint Warfighting Center in Suffolk, Virginia.

JKO-P provides an online source for relevant, operationally focused joint training and knowledge services and products specifically tailored for access by the general public, multinational partners, and interagency/intergovernmental supporters.

To access JKO Communities of Interest (COI's) and on-line training courses, you need to register for an account to log-in to the JKO Members Portal.

Joint Language University

URL:  http://JLU.wbtrain.com
The Joint Language University (JLU) is a web based language learning support system. It comprises various projects and contributors from across the Federal Government including the NSA, DIA, US Navy, USSOCOM, and DLI. It is open to anyone within the Federal Government through self-registration using their '.mil' or '.gov' email address.

JLU includes quality foreign language learning and teaching resources. Quality assurance is accomplished by experts in the specific language and in pedagogy or second language acquisition, who are identified through relevant national teaching associations and programs at major universities. JLU also includes cultural and area familiarization materials from such programs as the National Cryptologic School's ICAS seminars, the Defense Language Institute’s Countries in Perspective and Area Familiarization Guides and the Navy's Center for Language, Regional Expertise, and Culture (CLREC).

The project goal is to support a wide range of languages, learner proficiency levels, and learning environments, and to provide access to these resources for language professionals across the Federal, DoD, and Intelligence language communities. The JLU is working to create a scalable, cost-effective system that can adapt to changing missions, circumstances, and teacher/learner needs. As the JLU continues to develop, new features, resources, and tools will be added as they become available.

The JLU has been created with the support of the US Government and is free for all members of the US Government. Registration is available only to users with a valid .mil or .gov email address and for select DoD and associated schools. Questions & comments: JLU_Admin@wbtrain.com

Joint Personnel Adjudication System (JPAS)


Joint Personnel Adjudication System (JPAS) is the Department of Defense (DOD) personnel security migration system for—

- The virtual consolidation of the DOD central adjudication facilities.
- Use by non-sensitive compartmented information (non-SCI) security program managers and special security officers.
- Special access program managers.
- DOD contractor security officers.

JPAS automates both core and central adjudication facility-unique functionality and provides “realtime” information about clearance, access, and investigative status to authorized DOD security personnel and other interfacing organizations, such as Defense Security Service,

Joint Personnel Recovery Agency

{Military & Government Information Entrance}

Includes products and links for:

- Blood Chits
- Evasion Charts
- Pointee-Talkees

JWICS - Joint Worldwide Intelligence Communications System

The Joint Worldwide Intelligence Communications System [JWICS] is a 24 hour a day network designed to meet the requirements for secure (TS/SCI) multi-media intelligence communications worldwide. JWICS replaces the DDN DSNET3 as the Sensitive Compartmented Information (SCI) component of the Defense Information System Network (DISN). It provides DODIIS users a SCI level high-speed multimedia network using high-capacity communications to handle data, voice, imagery, and graphics.

The system uses JDISS as its primary means of operator interface and display. In much the same way as ASAS, JWICS is an evolutionary system. The JWICS program initial or pilot phase established a hub and spoke circuit switched T1 backbone for point-to-point and multipoint video teleconferences (VTCS), broadcast of the Defense Intelligence Network (DIN), and variable bandwidth packet switched data communications. The Hybrid JWICS phase removed the DSNET3 PSNS, re-homed the lines to JWICS IP routers, and extended the JWICS to additional sites to form a mesh network. Some sites will have video and data capability on T1 lines, and some sites will have strictly data capability (64 kbps lines). The final phase--Goal JWICS--will replace Hybrid JWICS with a single commercially available technology that can accommodate data, voice, and video. This technology is expected to be asynchronous transfer mode (ATM). JWICS will ride the DISN as an overlay when the DISN acquires T3 lines.

The Defense Intelligence Agency (DIA) has directed that all Special Security Offices (SSOs) will install the JWICS.
Kryptos Sculpture


Kryptos is a sculpture by American artist Jim Sanborn located on the grounds of the Central Intelligence Agency (CIA) in Langley, Virginia. Since its dedication on November 3, 1990, there has been much speculation about the meaning of the encrypted messages it bears. Of the four sections, three have been solved, with the fourth remaining one of the most famous unsolved codes in the world.
Kurrently - A real-time search engine for Facebook and Twitter

URL: http://www.kurrently.com/

---------- L ----------

Language & Culture Training

See:

- Air Force Language, Region & Culture Program
- Center for Advanced Operational Culture Learning (CAOCL)
- Defense Language Institute Foreign Language Center
- Defense Language Institute - Headstart-2
- Español for Law Enforcement: An Interactive Training Tool
- Foreign Service Institute Language Courses
- Global Language Online Support System
- Interagency Language Roundtable
- Joint Language University
- Omniglot - Writing Systems & Languages of the World
- Rosetta Stone Language Program
- Tactical Language & Culture Training System
- TRADOC Culture Center
- Virtual Cultural Awareness Trainer (VCAT)

Language Translation

Babel Fish -- http://babelfish.altavista.com/

Google Language Translator -- http://www.google.com/language_tools?hl=en

Omniglot Writing Systems of the World -- http://www.omniglot.com/

Law Enforcement Analyst Certification Standards

Assists in instituting standards for the intelligence analysis process to ensure that intelligence products are accurate, timely, factual, and relevant, while also recommending implementation of policy and/or action(s). The certification standards incorporate the Law Enforcement Analytic Standards, developed by the International Association of Law Enforcement Intelligence Analysts (IALEIA) with support from the Global Intelligence Working Group (GIWG). This booklet contains 25 recommended analytic standards. The first 7 standards relate to analysts or those who fill the analytic function. These standards refer to education, training, professionalism, and certification. The remaining standards relate to analytical products and processes.

**Law Enforcement Analytic Standards**


Consists of 25 standards that explain the requirements of agencies to adopt the minimum standards for intelligence-led policing in order to support the development of sound, professional, and analytical products (intelligence). Included are educational standards and intelligence process standards, as well as testimony, data-source attribution, and feedback standards.


Describes changes (since the publication of the first edition) in the philosophy, national standards, and practice of law enforcement intelligence, while maintaining the core goal of being a primer on “all things intelligence” for the law enforcement community. The guide is intended to support policy in law enforcement agencies and seeks to objectively provide the best knowledge and practice of law enforcement intelligence at the time of publication. It is not intended to be an academic work, nor does it look at theoretical issues or arguments. It is not directed as a guide to the intelligence community except to explain the roles, responsibilities, and restrictions of the intelligence community’s state, local, and tribal law enforcement partners.

**Law Enforcement Intelligence Unit (LEIU)**

In the mid 1950's, local and state law enforcement agencies in the United States recognized that no single agency or organization was responsible for receiving, collating, maintaining, and disseminating information on persons involved in organized crime. These law enforcement agencies surmised correctly that organized crime would exploit advancing technologies in transportation and communications, become more mobile, and increase their spheres of influence and criminal activities. As a result, twenty-six (26) law enforcement agencies met in San Francisco, California on March 29, 1956 to discuss problems and possible solutions. The most important result of that meeting was the creation of the LEIU – The LAW ENFORCEMENT INTELLIGENCE UNIT and the development of an organizational purpose that survives to this day. The purpose of LEIU is to gather, record, and exchange confidential information not available through regular police channels, concerning organized crime and terrorism. LEIU is an association of state and local police departments, similar in many respects to numerous other professional associations serving doctors, attorneys, journalists, and educators. LEIU has no employees and no capability as an entity to conduct any investigation or law enforcement activity of any kind. Each member agency is bound by, and acts pursuant to local law and their own agency regulations.

Law Enforcement Online (LEO)

URL:  http://www.leo.gov

LEO is a 7 days a week, 24 hours a day online (real-time), controlled-access communications and information sharing data repository. It provides an Internet accessible focal point for electronic Sensitive But Unclassified (SBU) communication and information sharing for the international, federal, state, local, and tribal law enforcement agencies. LEO also supports antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities worldwide. Users anywhere in the world can communicate securely using LEO.

Lessons Learned Information Sharing Network

URL:  https://www.llis.dhs.gov

Lessons Learned Information Sharing (LLIS.gov) is the national network of Lessons Learned, Best Practices, innovative ideas, and preparedness information for homeland security and emergency response professionals. By facilitating the sharing of knowledge, LLIS.gov enhances the nation's ability to prepare for and respond to terrorism, natural disasters, and other incidents. LLIS.gov is not only a repository for information but also a network that enables homeland security and emergency response professionals from across the country to share their knowledge and expertise in a secure, online environment.
Library of Congress – Country Studies

URL: [http://memory.loc.gov/frd/cs/](http://memory.loc.gov/frd/cs/)

The Country Studies Series presents a description and analysis of the historical setting and the social, economic, political, and national security systems and institutions of countries throughout the world.

Lightweight Portable Security

URL: [http://spi.dod.mil/lipose.htm](http://spi.dod.mil/lipose.htm)

Lightweight Portable Security (LPS) creates a secure end node from trusted media on almost any Intel-based computer (PC or Mac). LPS boots a thin Linux operating system from a CD without mounting a local hard drive. Administrator privileges are not required; nothing is installed. SPI created the LPS family to address particular use cases.

LPS-Public is a safer, general-purpose solution for using web-based applications.

The accredited LPS-Remote Access is only for accessing your organization's private network.

LPS-Public allows general web browsing and connecting to remote networks. It includes a CAC-enabled Firefox browser, a PDF and text viewer, Java, and Encryption Wizard - Public. ([http://www.spi.dod.mil/ewizard_down.htm](http://www.spi.dod.mil/ewizard_down.htm))

LPS-Public turns an un-trusted system (such as a home computer) into a trusted network client.

No trace of work activity (or malware) can be written to the local computer. Simply plug in your USB CAC-reader to access CAC-restricted DoD websites.

To get started, download the LPS-Public ISO image and burn it to a CD.
Major Military Commands (MACOM)

Maltego

URL: http://www.paterva.com/web5/

Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format. Includes a freeware "community edition".

Maps, Satellite & Aerial Photos

- Global Land Cover Facility (University of Maryland) - http://glcf.umiacs.umd.edu/data/
- Google Earth - http://earth.google.com/
- Mapquest - http://www.mapquest.com/
- NASA World Wind - http://worldwind.arc.nasa.gov/
- Perry-Castañeda Library Map Collection U. of Texas at Austin - http://www.lib.utexas.edu/maps/
- Terrafly - http://www.terrafly.com/
- Terra Server USA - http://terraserver-usa.com/

Marine Corps Cryptologic Association

URL: http://www.mccaonline.org/index.html

Marine Corps Intelligence Activity

URL: https://www.intelink.gov/mcia/ (Requires Intelink Login)
The Marine Corps Intelligence Activity, located at Hochmuth Hall, provides tailored intelligence and services to the Marine Corps, other services, and the Intelligence Community based on expeditionary mission profiles in littoral areas. It supports the development of service doctrine, force structure, training and education, and acquisition.

**Marine Corps Intelligence Association (MCIA)**


The Marine Corps Intelligence Association, Inc. is a non-profit professional organization of regular, reserve, retired, and former Intelligence Marines. MCIA, Inc. promotes professionalism among the Marine Corps Intelligence Community through collective action by its membership and through its affiliation with other associations.

**Marine Corps Intelligence Detachment**

URL: [http://www.marines.mil/unit/hqmc/intelligence/Pages/defaultv2.aspx](http://www.marines.mil/unit/hqmc/intelligence/Pages/defaultv2.aspx)

The Intelligence Department is responsible for policy, plans, programming, budgets, and staff supervision of Intelligence and supporting activities within the United States Marine Corps. The Department supports the Commandant of the Marine Corps (CMC) in his role as a member of the Joint Chiefs of Staff (JCS), represents the service in Joint and Intelligence Community matters, and exercises supervision over the Marine Corps Intelligence Activity (MCIA). The Department has Service Staff responsibility for Geospatial Intelligence (GEOINT), Advanced Geospatial Intelligence (AGI), Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Counterintelligence (CI), and ensures there is a single synchronized strategy for the development of the Marine Corps Intelligence, Surveillance, and Reconnaissance (ISR) Enterprise.
Masters of the Intelligence Art (Fort Huachuca Museum)

Memorial Institute for the Prevention of Terrorism (MIPT)
URL:  http://www.mipt.org/

MIPT is a non-profit, nationally recognized think tank creating state-of-the-art knowledge bases and sharing information on terrorism.

Merchhurst College - Institute for Intelligence Studies
URL:  http://www.mciis.org/

MCIIS is a center of excellence promoting the study of intelligence in higher academic settings, while seeking to identify, promote, and employ best practices in the study and application of intelligence studies throughout its various disciplines (national security, law enforcement, business and academia).

Center for Intelligence, Research, Analysis, and Training
http://www.mciis.org/center_intelligence_research_analysis_and_training

The Center for Intelligence Research Analysis & Training (CIRAT) brings together the students and faculty of the Mercyhurst College Institute for Intelligence Studies (MCIIS) to perform high quality, low cost, open source research and analysis for private businesses and institutions and for governmental agencies through grants, partnerships and contracts.

Founded in 1995, CIRAT’s primary goal is to give MCIIS students exposure to actual intelligence problems and questions and the experience of applying what they have learned in the classroom to those problems and questions. CIRAT provides the flexibility of trained individuals or teams, led by experienced faculty and staff, who respond to unmet open source research and analytical needs in surge situations or longer-term requirements. These students are generalist analysts. They have been trained to conduct in-depth research on virtually any topic assigned to them and then to apply their analytical skills to the question or problem. From there, they present their results in a variety of formats customized to the need of the decision-maker. These range from massive spreadsheets to short written reports to highly visual or digital presentations.
Military Attaché Guide (December 2009)


The Military Attaché Guide outlines Department of the Army (DA) policy for foreign Military Attachés accredited to the United States (U.S.) Army and other representatives of foreign governments who wish to conduct official business with the U.S. Army. It is published as a service to the Foreign Military Attaché community.

Military Guide to Terrorism in the Twenty-First Century

http://www.fas.org/irp/threat/terrorism/

U.S. Army Training and Doctrine Command
TRADOC Intelligence Support Activity
15 August 2007

The handbook is a high level terrorism primer that includes an overview of the history of terrorism, descriptions of terrorist behaviors and motivations, a review of terrorist group organizations, and the threat posed to our forces, both in the United States and overseas. Additionally, it provides information on the various terrorist groups, the terrorist planning cycle, operations and tactics, firearms used by terrorists, improvised explosive devices, conventional munitions used by terrorists, and a discussion on weapons of mass destruction. The manual is designed to be used to help train and educate personnel on terrorism and assist units in recognizing the threat they face in planning for operations, both in the Continental United States and overseas.

A Military Guide to Terrorism in the Twenty-First Century

- chapter 1 - The Face of Terrorism Today
- chapter 2 - Terrorist Motivations and Behaviors
- chapter 3 - Terrorist Organizational Models
- chapter 4 - Terrorist Targeting of U.S. Military Forces
- chapter 5 - Terrorism of the Foreseeable Future
- appendix a - Terrorist Planning Cycle
- appendix b - Firearms
- appendix c - Conventional Military Munitions
o Supplement 2 — Critical Infrastructure Threats and Terrorism, 10 August 2006
o Supplement 3 — Suicide Bombing in the COE, 10 August 2006
o Supplement 4 — Terrorism and WMD in the Contemporary Operational Environment, 20 August 2007
o Supplement 5 — A Military Primer to Terrorism in the Contemporary Operational Environment, 10 August 2006
o Supplement 6 — Kidnapping and Terror in the Contemporary Operational Environment, 15 September 2008

Military Installations

URL:  http://www.militaryinstallations.dod.mil

View articles, photos, major unit listings and contacts for programs and services worldwide.

Military Intelligence Civilian Excepted Career Program (MICECP)


Department of Army
Commander, USAFSC
ATTN: IAFS-P-M (MICECP Recruitment)
375 Chamberlin Ave, Ste 5904
Fort Meade, MD 20755-5904
Telephone: 410-290-1749 / 1748
Email: micecp.division@us.army.mil

The MICECP is a centrally managed intelligence program in the excepted service. MICECP complies with the Defense Civilian Intelligence Personnel System's (DCIPS) regulations and guidance while at the same time providing personalized career management. MICECP personnel are carried on the Army Field Support Center (AFSC) Table of Distribution and Allowances (TDA) and all personnel and financial support are provided by the MICECP.

Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States

URL:  http://it.ojp.gov/documents/min_crim_intel_stand.pdf
Provides perspective and guidance for the development and delivery of law enforcement intelligence training. This document explains the recommended development of minimum training standards for all affected levels of law enforcement personnel, including core training objectives in six areas: General Law Enforcement Officer, Law Enforcement Executive, Intelligence Manager, Intelligence Officer/Collector, Intelligence Analyst, and Train-the-Trainer. The goals in developing the standards were to identify specific training topics and issues for each level of personnel involved in the intelligence process, to make specific recommendations for training objectives and the delivery of training, and to work with relevant agencies and groups to develop model curricula.

**Multijurisdictional Counterdrug Task Force Training**

URL:  [http://www.mctft.com/](http://www.mctft.com/)

The Multijurisdictional Counterdrug Task Force Training (MCTFT) program provides unique, tuition-free, courses covering all aspects of counterdrug law enforcement and training support for community anti-drug coalitions.

**CD-ROM Training**

- Analytical Investigative Tools
- Drugs in America: Lessons for Law Enforcement
- Explosives, Booby Traps and Bomb Threat Management
- Risk Management and Violence in Undercover Operations
- InFocus: A Clear Message About Drugs

**On-Line Training**

- Airport Narcotics Investigations
- Introduction to Clandestine Laboratory Investigations
- Clandestine Laboratory Recertification
- Command & Control Overview
- Introduction to Conspiracy Investigations
- Criminal Street Gangs Overview
- Criminal Street Gangs Overview - Spanish
- Drug Identification
- Ethical Issues and Decisions in Law Enforcement
- Explosives, Booby Traps & Bomb Threat Management
- Introduction to Highway & Rural Drug Investigations
- Introduction to Interview & Interrogation
• Introduction to Money Laundering
• Introduction to Patrol Drug Investigations
• Overdose America
• Police Intelligence
• Risk Management and Violence in Undercover Operations
• Surveillance Operations Overview

Multi-Service Tactics, Techniques, and Procedures for Survival, Evasion and Recovery
{FM 3-50.3; NTTP 3-50.3; AFTTP(I) 3-2.26} (20 March 2007)


----------- N -----------

Names and Naming Practices

This guide has been produced by the United Kingdom to aid with difficulties that are commonly encountered with names from around the globe. Interpol believes that member countries may find this guide useful when dealing with names from unfamiliar countries or regions.

ROCIC Law Enforcement Guide to International Names
URL: http://www.docstoc.com/docs/72433590/ROCIC-International-Names

National Center for Medical Intelligence (NCMI)
URL: https://www.intelink.gov/ncmi/

The National Center for Medical Intelligence (NCMI) at Fort Detrick, Maryland, USA — formerly the Armed Forces Medical Intelligence Center (AFMIC) — is an agency within the Defense Intelligence Agency (DIA) of the United States Department of Defense (DoD; its mission is to track and assess the full range of global health issues for the DoD, specifically
monitoring and analyzing health events that could negatively impact the health of U.S. military and civilian populations.

**National Counterproliferation Center**


National Counterproliferation Center (NCPC), which resides within the ODNI, is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD). NCPC conducts strategic counterproliferation planning for the IC to support policy efforts to prevent, halt, or mitigate the proliferation of WMDs, their delivery systems, and related materials and technologies. This includes both states of concern and, in partnership with the National Counterterrorism Center, non-state actors. NCPC achieves this by drawing on the expertise of counterproliferation professionals in the IC, the U.S. Government, industry, and academia. These relationships foster an atmosphere of collaboration and intelligence sharing in order to protect the U.S.’s interests at home and abroad.

**National Counter-Terrorism Center**


The National Counterterrorism Center (NCTC) was established by Presidential Executive Order 13354 in August 2004, and codified by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). NCTC integrates foreign and domestic analysis from across the Intelligence Community (IC) and produces a wide-range of detailed assessments designed to support senior policymakers and other members of the policy, intelligence, law enforcement, defense, homeland security, and foreign affairs communities. By law, NCTC serves as the USG’s central and shared knowledge bank on known and suspected terrorists and international terror groups. NCTC also provides USG agencies with the terrorism intelligence analysis and other information they need to fulfill their missions. 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.
National Criminal Intelligence Resource Center (NCIRC)

URL:  http://www.ncirc.gov/

The National Criminal Intelligence Resource Center (NCIRC) is sponsored by the Bureau of Justice Assistance (BJA) for the purpose of providing a secure web-site developed to serve as a "one-stop shop" for local, state, tribal, and federal law enforcement to keep up with the latest developments in the field of criminal intelligence. The NCIRC web-site contains information regarding law enforcement intelligence operations and practices. It provides criminal justice professionals with a centralized resource information bank to access a multitude of criminal intelligence resources in a secure environment.

National Criminal Intelligence Sharing Plan (NCISP)

URL:  http://it.ojp.gov/documents/NCISP_Plan.pdf

**Also available online as an overview CD (http://it.ojp.gov/documents/ncisp/)

** Executive Summary (http://it.ojp.gov/documents/NCISP_executive_summary.pdf)

Provides a blueprint to help agencies establish criminal intelligence sharing policies, procedures, standards, technologies, and training. Implementation of the NCISP will provide law enforcement agencies with the ability to gather, analyze, protect, and share information and intelligence to identify, investigate, prevent, deter, and defeat the perpetrators of criminal and terrorist activities, both domestically and internationally.

National Cryptologic Museum

URL:  http://www.nsa.gov/about/cryptologic_heritage/museum/

The National Cryptologic Museum is the National Security Agency's principal gateway to the public. It shares the Nation's, as well as NSA's, cryptologic legacy and place in world history. Located adjacent to NSA Headquarters, Ft. George G. Meade, Maryland, the Museum houses a collection of thousands of artifacts that collectively serve to sustain the history of the cryptologic profession. Here visitors can catch a glimpse of some of the most dramatic moments in the history of American cryptology: the people who devoted their lives to cryptology and national defense, the machines and devices they developed, the techniques they used, and the places where they worked. For the visitor, some events in American and world history will take on a
new meaning. For the cryptologic professional, it is an opportunity to absorb the heritage of the profession.

National Defense Industrial Association (NDIA)

URL:  http://www.ndia.org/

The National Defense Industrial Association (NDIA) is America’s leading Defense Industry association promoting national security. NDIA is proud to provide a legal and ethical forum for the exchange of information between Industry and Government on National Security issues. Our members foster the development of the most innovative and superior equipment, training and support for our warfighters and first responders through our divisions, local chapters, affiliated associations and events.

National Defense Intelligence College

URL:  http://www.ndic.edu/

The National Defense Intelligence College is a dynamic learning community with a professionally diverse student body of over 700, representing a balanced mixture of experience in federal agencies and all branches of the US Armed Services. All students must be employed in the federal government and hold Top Secret security clearances. The College's degrees, the Master of Science of Strategic Intelligence, and the Bachelor of Science in Intelligence are authorized by Congress.

The College was chartered by Department of Defense in 1962, and has since served as a leading institution for intelligence education and research. In December 2006, Department of Defense Instruction 3305.01 renamed the College and broadened its mission. The new Charter reflects the deep value attached to the College by the US national security community and the trust given to the College to educate future intelligence leaders in the Armed Services, the US Combatant Commands, and the Departments and agencies of the intelligence and homeland security communities.

The College’s Bachelor of Science in Intelligence and Master of Science of Strategic Intelligence are both authorized in law by Congress. Among the nation’s federally chartered colleges and universities, the College has the unique distinction of annually awarding both graduate and undergraduate degrees in Intelligence.

The College is a member of the Consortium of Universities of the Washington Metropolitan Area.
National Do Not Call Registry

URL: http://www.donotcall.gov

The Federal Bureau of Investigation (2011) warned:

Mass-marketing fraud encompasses many deceptive and misleading schemes conducted through mass-communications techniques (e.g., telemarketing, the Internet, mass-mailings, e-mail) that are intended to defraud individuals, businesses, and other organizations of money, property, services, valuable assets, or information. Mass-marketing fraud perpetrators tend to be mobile and adaptable, frequently change solicitation methods, and target vulnerable populations, causing estimated losses in the tens of billions of dollars.

The Federal Trade Commission has long recognized the potential for fraud associated with telemarketing calls, and as the nation’s consumer protection agency established the National Do Not Call Registry to give individuals a choice about whether to receive telemarketing calls at home.

Once you register your telephone number with the National Do Not Call Registry most telemarketers should not call your number. Legitimate businesses conducting telemarketing screen their call lists against the National Do Not Call Registry. If you receive a telemarketing call after you have registered your number with the National Do Not Call Registry, that telemarketing call is almost certainly some type of deceptive and misleading scheme.

To register your telephone numbers with the National Do Not Call List visit their web-site http://www.donotcall.gov/ and follow the simply registration instructions.

National Drug Intelligence Center (NDIC)

URL: http://www.usdoj.gov/ndic/

The National Drug Intelligence Center (NDIC) was established by the Department of Defense Appropriations Act, 1993 (Public Law 102-396) signed into law on October 6, 1992. Placed under the direction and control of the Attorney General, NDIC was established to "coordinate and consolidate drug intelligence from all national security and law enforcement agencies, and produce information regarding the structure, membership, finances, communications, and activities of drug trafficking organizations."

Email: NDIC.Contacts@usdoj.gov
National Drug Intelligence Center
319 Washington Street, 5th Floor
Johnstown, PA 15901-1622
Telephone: 814-532-4601
Fax: 814-532-4690

National Drug Intelligence Center
U.S. Department of Justice
Robert F. Kennedy Building, Room 3341
950 Pennsylvania Avenue, NW
Washington, DC 20530-2000
Telephone: 202-532-4040

**National Geospatial-Intelligence Agency**

URL: [https://www1.nga.mil/Pages/Default.aspx](https://www1.nga.mil/Pages/Default.aspx)

The National Geospatial-Intelligence Agency is the nation’s premier source of geospatial intelligence. As a Department of Defense combat support agency and a member of the U.S. Intelligence Community, NGA provides imagery, geospatial and targeting analysis, along with image sciences and modeling for U.S. national defense, disaster relief and safety of navigation. NGA seeks to know the Earth, show the way, and understand the world.

**National Ground Intelligence Center**

Commander
National Ground Intelligence Center
Building 4465
2055 Boulders Road
Charlottesville, VA 22911-8318
Telephone: 434-980-7000

The National Ground Intelligence Center is the Defense Department’s primary producer of ground forces intelligence. NGIC produces scientific and technical intelligence and military capabilities analysis on foreign ground forces required by warfighting commanders, the force modernization and research and development communities, Defense Department and national policymakers.

NGIC’s general military intelligence mission focuses on foreign ground forces from the operational through small-unit level, maintaining detailed knowledge of current foreign ground
force capabilities as well as a focus of five, 10 and 20 years in the future. It includes irregular and conventional warfare analysis examining foreign ground forces from a perspective that includes battlefield operating systems, doctrine, tactics, techniques and procedures, training, maintenance, logistics and order of battle.

**National HIDTA Assistance Center**

URL: [http://www.nhac.org/](http://www.nhac.org/)

The National HIDTA Assistance Center offers two CD-ROM based courses:

**Introduction to HIDTA Analytical Techniques**

This no cost informational distance learning CD-ROM was created through a collaborative effort between the NHAC Training and Multimedia Units. It was designed to provide the Analyst with introductory information into the intelligence cycle, the basic graphical techniques used in the analytical process, and various resources available to the HIDTA Analyst in the course of doing business.

Topics covered in the CD include:

- Document Exploitation
- Intelligence Cycle
- Analytical Techniques
- Validity and Reliability Scales
- Title III
- Criminal Intelligence Process
- Uses of DNR/Pen Register
- Intelligence Products Generation
- USC Title 18
- Statistical Comparison Formula
- Intelligence Education & Training
- Threat Analysis Elements
- Post Seizure Analysis Reports
- Briefing Techniques

**So What’s Next? Analysis & Critical Thinking**

This no cost informational distance learning CD-ROM entitled "So What’s Next? Analysis & Critical Thinking" was created to provide you with introductory information regarding
conceptual blockbusting, problem solving, analysis, reasoning skills, creative thinking and a mixture of games and puzzles to practice and sharpen your thinking skills.

Both CD-ROM programs are open to Federal, State and Local Law Enforcement Personnel, Criminal Intelligence Analysts, Crime Analysts, Investigators, Investigative Assistants, Counterdrug Operations Supervisors at all levels and military personnel – both active and reserve components – assigned to support counterdrug activities in a HIDTA.

**National Insurance Crime Bureau**

URL: [https://claimsearch.iso.com](https://claimsearch.iso.com)

Law enforcement, criminal justice, and regulatory agency personnel may obtain online access to ISO’s ClaimSearch, the insurance industry’s “All Claim Database”, which includes property and casualty claims data along with vehicle related information through the National Insurance Crime Bureau (NICB).

“Qualified” law enforcement agencies will be able to see all information the ISO ClaimSearch database contains pertaining to vehicles, casualty claims, and property claims, including individuals’ names, addresses and the following numeric identifiers:

- Driver License Number
- Vehicle Identification Number (VIN)
- Social Security Number
- Tax Identification Number
- Telephone Number
- Vehicle License Plate Number
- Policy/Claim Number
- Law Enforcement Agency Case Number


**National Intelligence Council**

URL: [http://www.dni.gov/nic/NIC_home.html](http://www.dni.gov/nic/NIC_home.html)
The National Intelligence Council (NIC) is an all-source ODNI analytic component and is the IC’s center for mid-term and long-term strategic thinking. Since its formation in 1979, the NIC has served as a unique bridge between the intelligence and policy communities, a source of deep substantive expertise on intelligence matters, and as a facilitator of IC collaboration. Some of the NIC’s core functions are to:

- Produce National Intelligence Estimates (NIEs)—the IC’s most authoritative written assessments on national security issues, as well as a broad range of other products.
- Reach out to nongovernmental experts in academia and the private sector to broaden the IC’s perspective.
- Articulate substantive intelligence priorities and procedures to guide intelligence collection and analysis.

**National Intelligence Strategy of the United States of America (August 2009)**


**National Media Exploitation Center**

The National Media Exploitation Center (NMEC) ensures the rapid collection, processing, exploitation, dissemination, and sharing of all acquired and seized media across the intelligence, counterintelligence, military, and law enforcement communities. These tasks include the collection, receipt, cataloging, initial processing, and transmission of information; forensic analysis and translation; and reporting, storage, dissemination, and sharing. NMEC is a DNI Center, and DIA is its Executive Agent.

**National Military Intelligence Association (NMIA)**

URL: [http://www.nmia.org/](http://www.nmia.org/)
One of the first of the professional US-based intelligence associations to focus on public education and the dissemination of unclassified knowledge about the profession or "craft" of intelligence.

NMIA was founded in 1974 at the US Army Intelligence Center & School at Fort Huachuca, AZ as an Army intelligence professional organization. LTG Vernon A. (Dick) Walters, Deputy Director of Central Intelligence, was the Association's first president. Several chapters were organized and the NMIA Digest, forerunner of the American Intelligence Journal, began to be published quarterly. In 1976, membership was opened to former and retired officers, and NCOs as well as civilians, the first Executive Director was hired, and an office was opened in Washington, DC. During that year, NMIA became a truly joint organization, and by the end of the year there were 25 chapters.

During the 1980's, NMIA broadened its vision to support all military intelligence services and the several DOD intelligence agencies. In 1984, the association was re-chartered in Virginia as a 501(c)(6), not-for-profit professional development organization. In 1986, Col (ret.) Roy Jonkers became President, LTG (ret.) Jim Williams became Chairman of the Board and they hired Zhi Hamby-Nye as Director of Administration. This trio began a number of initiatives including an expanded awards program and a series of symposia on critical topics of interest to the intelligence community. Corporate membership and support increased substantially. In the mid 1990's, Zhi Hamby launched the ZGram, a daily on-line compendium of unclassified reports from around the world. In 2004 it was joined by the CABLE Gram, an on-line publication dealing with homeland security issues.

With the dawn of the 21st century NMIA continues to serve the military intelligence community. Following the retirement of Zhi Hamby-Nye in 2004, responsibility for administration and corporate liaison came under direction of Mrs. Debra Davis who initiated an expanded outreach for corporate members and who helped institute expanded use of the Internet to facilitate communications with members. NMIA is ready for new initiatives to improve our service to all who serve or have served the defense intelligence and national security communities and to increase public understanding of the role and importance of intelligence to the nation.

**National Nuclear Security Administration**

URL: [http://nnsa.energy.gov/index.htm](http://nnsa.energy.gov/index.htm)

1000 Independence Ave. SW
Washington, DC 20585
Telephone: 1-202-586-5000
Fax: 1-202-586-4403
NNSA was established by Congress in 2000 as a separately organized agency within the U.S. Department of Energy. NNSA is responsible for the management and security of the nation’s nuclear weapons, nuclear nonproliferation, and naval reactor programs. It also responds to nuclear and radiological emergencies in the United States and abroad. Additionally, NNSA federal agents provide safe and secure transportation of nuclear weapons and components and special nuclear materials along with other missions supporting the national security.

**National Reconnaissance Office (NRO)**

URL: [http://www.nro.mil/](http://www.nro.mil/)

The NRO designs, builds and operates the nation's reconnaissance satellites. NRO products, provided to an expanding list of customers like the Central Intelligence Agency (CIA) and the Department of Defense (DoD), can warn of potential trouble spots around the world, help plan military operations, and monitor the environment. A DoD agency, the NRO is staffed by DoD and CIA personnel. It is funded through the National Reconnaissance Program, part of the National Foreign Intelligence Program.

**National Sex Offender Public Registry**

URL: [http://www.nsopr.gov/](http://www.nsopr.gov/)

The Dru Sjodin National Sex Offender Public Registry is provided as a public service by the U.S. Department of Justice. Using this Web site, interested members of the public have access to and may search participating state Web site public information regarding the presence or location of offenders, who, in most cases, have been convicted of sexually-violent offenses against adults and children and certain sexual contact and other crimes against victims who are minors. The public can use this Web site to educate themselves about the possible presence of such offenders in their local communities.

**National Strategy Information Center (NSIC)**

URL: [http://www.strategycenter.org/](http://www.strategycenter.org/)

The National Strategy Information Center (NSIC) identifies, researches, pilots, and promotes innovative strategies to enhance security and the quality of life in democratic societies. Founded
as a nonpartisan, nonprofit, nongovernmental organization, NSIC has been at the forefront of education about challenges to democratic institutions for nearly 50 years.

NSIC seeks to achieve a multiplier effect by developing programs that can become independent and self-sustaining. NSIC’s collaboration with educators, government officials, and civil society leaders in the United States and abroad translates its research findings into meaningful contributions to policy and programs.

National Technical Investigators’ Association

URL:  http://www.natia.org

NATIA is composed of over 2,500 law enforcement, intelligence officers, and support staff, who provide the technical operations, surveillance activities, and scientific support for hundreds of federal, state, and local agencies across the United States, Canada and the United Kingdom.

National Terrorism Preparedness Institute (NTPI)

URL:  http://terrorism.spcollege.edu/

National Terrorism Preparedness Institute (NTPI) opened in May 1998 as a result of the Nunn-Lugar-Domenici Act, commonly known as the Weapons of Mass Destruction Act. Significantly, NTPI is one of the few pre-9/11 institutions of its kind. NTPI provides extensive support to our Nation’s War on Terror. This support includes monthly nationwide, satellite television broadcasts on important training topics for emergency managers and responders; traditional classroom instruction; training support packages that include student and instructor guides, video, CD, DVD, and VHS products; mobile training teams; and web- and computer-based training products.

National Virtual Translation Center

URL:  http://www.nvtc.gov/

The National Virtual Translation Center (NVTC) was established in 2003 to provide timely and accurate translations of foreign intelligence for all elements of the IC. Its mission includes acting as a clearinghouse for facilitating interagency use of translators; partnering with elements of the
U.S. Government, academia, and private industry to identify translator resources and engage their services; building a nationwide team of highly qualified, motivated linguists and translators, connected virtually to the program office in Washington, D.C.; and applying state-of-the-art technology to maximize translator efficiency. NVTC is a DNI Center, and the Federal Bureau of Investigation (FBI) is its Executive Agent.

**National White Collar Crime Center (NW3C)**

URL: [http://www.nw3c.org/](http://www.nw3c.org/)

Member Log-in -- [https://members.nw3c.org/login.cfm](https://members.nw3c.org/login.cfm)

The mission of NW3C is to provide a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high-tech crimes and to support and partner with other appropriate entities in addressing homeland security initiatives, as they relate to economic and high-tech crimes.

NW3C is a congressionally-funded, non-profit corporation whose membership primarily comprises law enforcement agencies, state regulatory bodies with criminal investigative authority, and state and local prosecution offices.

While NW3C has no investigative authority itself, its job is to help law enforcement agencies better understand and utilize tools to combat economic and high-tech crime.

**Naval Criminal Investigative Service**

URL: [http://www.ncis.navy.mil/](http://www.ncis.navy.mil/)

716 Sicard Street SE, Suite 2000
Washington Navy Yard DC 20388-5380
NCIS Hotline 1-877-579-3648

NCIS evolved out of the Department of the Navy's (DON's) need for investigative autonomy into a full-fledged federal law enforcement agency with both law enforcement and counterintelligence responsibilities. NCIS investigative standards and evidence collection methods support prosecution in domestic and international criminal courts.
Naval Intelligence Professionals

URL:  http://navintpro.net/

The goal of the Naval Intelligence Professionals (NIP) is to further the knowledge of the art of maritime intelligence, and to provide a vehicle whereby present and former Naval Intelligence Professionals may be kept informed of developments in the Naval Intelligence community and of the activities and whereabouts of past shipmates.

Founded in 1985, NIP is a nonprofit organization incorporated to enhance awareness of the mission and vital functions of the Naval Intelligence community, as well as to foster camaraderie among Naval Intelligence Professionals.

It is an association of active duty, retired and reserve officers, enlisted personnel, and civilians who serve or have served within the Naval Intelligence community, as well as those in certain other categories who qualify as a nonvoting Subscriber.

Navy and Marine Corps Intelligence Training Center (NMITC)

URL:  https://www.netc.navy.mil/centers/cennavintel/nmitc/


The NMITC courses are:

**NMITC - Introduction to Intelligence** - This course is designed for Marines whose work depends on understanding the role of intelligence, intelligence development, the objectives of intelligence, and intelligence functions.

**NMITC - Intelligence Cycle** - This course will enhance your knowledge of intelligence operations by addressing the intelligence cycle’s purpose, six phases, and application process.

**NMITC - FMF Intelligence Structure** - This course is designed for Marine personnel whose work depends on being able to determine the proper Marine Corps intelligence organization that will provide the required intelligence to support the Marine Air-Ground Task Force (MAGTF) mission.
NMITC - Intelligence Disciplines - This course explains the five intelligence disciplines.

NMITC - Intelligence Preparation of the Battlespace - This course introduces the IPB process as well as the four steps that compose the process.

NMITC - Intelligence Writing - This course is designed for Marine personnel whose work depends on being able to draft an intelligence analytical paper.

NMITC - Marking Classified Documents - This course is designed for Marine personnel whose work depends on being able to choose the proper classification markings for classified material.

NMITC - Threat Analysis - This course introduces the Order of Battle (OOB) and the fundamentals of Analysis of Enemy Capabilities.

NMITC - Targeting - This course is designed for Marine personnel whose work depends on being able to give intelligence support to the targeting cycle, when given appropriate reference(s), material(s), and equipment.

Navy Intelligence Professionals (NIP)

URL: http://www.navintpro.org/

Naval Intelligence Professionals (NIP) is a nonprofit organization incorporated to enhance awareness of the mission and vital functions of the Naval Intelligence community, as well as to foster camaraderie among Naval Intelligence Professionals, founded in 1985.

It is an association of active duty, retired and reserve officers, enlisted personnel, and civilians who serve or have served within the Naval Intelligence community, as well as those in certain other categories who qualify as a nonvoting Subscriber. The goal of the Naval Intelligence Professionals is to further the knowledge of the art of maritime intelligence, and to provide a vehicle whereby present and former Naval Intelligence Professionals may be kept informed of developments in the Naval Intelligence community and of the activities and whereabouts of past shipmates.
Near Repeat Calculator

URL:  http://www.temple.edu/cj/misc/nr/

This software originates with the relatively recent discovery of the near repeat phenomenon in burglary patterns, a discovery that has highlighted the communicability of crime events that affect the risk level at nearby locations. The near repeat phenomenon states that if a location is the target of a crime (such as burglary), the homes within a relatively short distance have an increased chance of being burgled for a limited number of weeks (Townsley et al, 2003; Bowers and Johnson, 2004; Johnson and Bowers, 2004a, 2004b). This communicability of risk to nearby locations for a short amount of time raises the possibility that other crime types may also suffer from a near repeat spatio-temporal pattern of behavior.

The analytical method employed builds on a space-time clustering methods first pioneered by Knox (1964) to study the epidemiology of childhood leukemia. The Knox test seeks to determine whether there are more event-pairs observed that occur with a closer proximity in space and time than would be expected on the basis of a random distribution. To do this, each shooting for a particular dataset is compared with every other and the spatial and temporal distance between them recorded. The result is a matrix of space-time distances.

To establish a null hypothesis measure against which to test the shooting patterns, we employ a Monte Carlo simulation process. By computing multiple simulations of the expected values, it is possible to generate an expected distribution under a null hypothesis – using the actual study data. This provides a unique way to examine what would occur if there were no near repeat patterns.

Newspapers (On-line)

URL:  http://www.onlinenewspapers.com/

NIPRNet - Unclassified but Sensitive Internet Protocol (IP) Router Network

The Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNet) is a global long-haul IP based network to support unclassified IP data communications services for combat support applications to the Department of Defense (DoD), Joint Chiefs of Staff (JS), Military Departments (MILDEPS), and Combatant Commands (COCOM). Provide seamless interoperability IP services to customers with access data rates ranging from 56KB to 1.0GB via direct connections to a NIPRNet router, remote dial-up services (56KB), services to the Tactical community via ITSDN/STEP sites, and access to the Internet. NIPRNet Contact 703-882-0158
NodeXL: Network Overview, Discovery and Exploration in Excel


URL:  http://nodexl.codeplex.com/

NodeXL is a powerful, open-source, and easy-to-use interactive network visualization and analysis tool that leverages the widely available MS Excel application as the platform for representing generic graph data, performing advanced network analysis and visual exploration of networks. The tool supports multiple social network data providers that import graph data (nodes and edge lists) into the Excel spreadsheet.

An introductory video to NodeXL is here: http://www.youtube.com/watch?v=0M3T65Iw3Ac

NW3C – See: National White Collar Crime Center

Office of Secure Transportation

URL:  http://nnsa.energy.gov/aboutus/ourprograms/defenseprograms/securetransportation

OST Recruitment - https://fmt.kcp.com/OSTfederalagent/

Office of the Coordinator for Counterterrorism

U.S. Department of State
Office of the Director of National Intelligence

URL: http://www.dni.gov/

The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC), overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. Working together with the Principal Deputy DNI (PDDNI) and with the assistance of Mission Managers and four Deputy Directors, the Office of the DNI's goal is to effectively integrate foreign, military and domestic intelligence in defense of the homeland and of United States interests abroad.

Office of the National Counterintelligence Executive

URL: http://www.ncix.gov/

The Office of the National Counterintelligence Executive (ONCIX) is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. The ONCIX develops, coordinates, and produces:

- Annual foreign intelligence threat assessments and other analytic CI products.
- An annual national CI strategy for the US Government.
- Priorities for CI collection, investigations, and operations.
- CI program budgets and evaluations that reflect strategic priorities.
- In-depth espionage damage assessments.
- CI awareness, outreach, and training standards policies.

**Office of Naval Intelligence**


**Omniglot - Writing Systems & Languages of the World**

URL:  [http://www.omniglot.com/](http://www.omniglot.com/)

**One-Time Pad**

One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. It is the only known method to perform mathematically unbreakable encryption. Used by Special Operations teams and resistance groups in WW2, popular with intelligence agencies and their spies during the Cold War and beyond, protecting diplomatic and military communications around the world for many decades, the one-time pad gained a reputation as a simple yet solid encryption system with an absolute security which is unmatched by today's modern crypto algorithms. Whatever technological progress may come in the future, one-time pad encryption is, and will remain, the only system to provide real long-term message security.

- One-Time Pad Generator -- [http://www.fourmilab.ch/ontime/otpjs.html](http://www.fourmilab.ch/ontime/otpjs.html)
Open Source Center

URL:  http://www.opensource.gov

OpenSource.gov provides timely and tailored translations, reporting and analysis on foreign policy and national security issues from the Open Source Center and its partners. Featured are reports and translations from thousands of publications, television and radio stations, and Internet sources around the world. Also among the site's holdings are a foreign video archive and fee-based commercial databases for which OSC has negotiated licenses. OSC's reach extends from hard-to-find local publications and video to some of the most renowned thinkers on national security issues inside and outside the US Government. Accounts are available to US Government employees and contractors.

Open Source Intelligence Training

https://www.intelink.gov/sites/dhs-ose/training/default.aspx  (Requires Intelink Access)

- Module 1 - The Value and Definition of Open Source
- Module 2 - Assessing Reliability of Sources
- Module 3 - Search Engines
- Module 4 - The Deep Web
- Module 5 - The Use of RSS
- Module 6 - Social Bookmarking
- Module 7 - Introduction to Anonymization
- Module 8 - Intellink
- Module 9 - OpenSource.gov
- Module 10 - Non-Internet Open Source
- Module 11 - Blogosphere
- Module 12 - Virtual Worlds
- Module 13 - Research Planning

Operational Environment

A composite of the conditions, circumstances, and influences environment which affect the employment of military forces and bear on the decisions of the unit commander. Some examples are: a. permissive environment—operational environment in which host country military and law enforcement agencies have control and the intent and capability to assist operations that a unit intends to conduct. b. uncertain environment—operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct,
do not have totally effective control of the territory and population in the intended area of operations. c. hostile environment—operational environment in which hostile forces have control and the intent and capability to effectively oppose or react to the operations a unit intends to conduct. (JP 1-02)

**Operations Security (OPSEC)**

[Diagram of OPSEC process]

OPSEC (Operations Security) is a process used to deny a competitor or adversary information concerning your intentions and capabilities by identifying, controlling and protecting indicators associated with your planning processes or operations.

OPSEC is comprised of 5 steps:

- Identify Sensitive/Critical Information.
- Assess Threat.
- Analyze Vulnerabilities.
- Analyze Risk.
- Apply Countermeasures.

**Identify Sensitive/Critical Information**
Sensitive/critical information is unclassified information that a competitor or adversary could obtain from openly available sources. This information provides crucial information or clues to your company’s activities, possessions, strategies and future.

**Assess Threat**

The goal of threat assessment is to determine the real extent of a threat. A threat requires both intent and capability. If one or the other is not present, there is no threat.

\[ \text{Threat} = \text{intent} + \text{capability} \]

**Analyze Vulnerabilities**

A vulnerability is an opportunity or weakness in securing information. Indicators are any observable pattern or activity changes that when looked at by themselves or in conjunction with something else, allows your competitor to obtain a sensitive piece of information. To analyze vulnerabilities, ask yourself: Are there things that give away data directly? Are there certain signs that could lead to deducing the data?

**Analyze Risk**

Risk is the likelihood of an undesirable event occurring and the consequences of that event. Risk analysis is the process of determining the potential for a threat’s success to acquire, exploit and capitalize on critical information.

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact} \]

**Apply Countermeasures**

Countermeasures are anything that effectively negates a threat’s ability to exploit vulnerabilities.

There are typically five types of countermeasures:

- Changes in procedure
- Controlling dissemination
- Cover and deception
- Speed of execution
- Awareness training

**OPSEC Professionals Society (OPS)**

URL: [http://opsecsociety.org/](http://opsecsociety.org/)
The mission of the Operations Security Professionals Society is to advance the interests of the United States and its allies by: Promoting, within federal, state and municipal government agencies, academe, and private industry, as vital to national security interests, the development and nurturing of an Operations Security mindset and the practice of risk management based upon Operations Security principles; Serving as a means of educating and informing the American people with regard to the role of Operations Security in maintaining a strong national defense.

**ORA**


ORA is a dynamic meta-network assessment and analysis tool developed by CASOS at Carnegie Mellon. It contains hundreds of social network, dynamic network metrics, trail metrics, procedures for grouping nodes, identifying local patterns, comparing and contrasting networks, groups, and individuals from a dynamic meta-network perspective. ORA has been used to examine how networks change through space and time, contains procedures for moving back and forth between trail data (e.g. who was where when) and network data (who is connected to whom, who is connected to where ...), and has a variety of geo-spatial network metrics, and change detection techniques. ORA can handle multi-mode, multi-plex, multi-level networks. It can identify key players, groups and vulnerabilities, model network changes over time, and perform COA analysis. It has been tested with large networks (106 nodes per 5 entity classes). Distance based, algorithmic, and statistical procedures for comparing and contrasting networks are part of this toolkit.

**OSAC** - See: Overseas Security Advisory Council

**Overseas Security Advisory Council (OSAC)**

URL: [http://www.osac.gov/](http://www.osac.gov/)

The Overseas Security Advisory Council (OSAC) is a Federal Advisory Committee with a U.S. Government Charter to promote security cooperation between American business and private sector interests worldwide and the U.S. Department of State. OSAC currently encompasses the 34-member core Council, an Executive Office, over 100 Country Councils, and more than 3,500 constituent member organizations and 372 associates.

The objectives of the Council as outlined in the Charter are:
To establish continuing liaison and to provide for operational security cooperation between State Department security functions and the Private Sector.

To provide for regular and timely interchange of information between the Private Sector and the State Department concerning developments in the overseas security environment.

To recommend methods and provide material for coordinating security planning and implementation of security programs.

To recommend methods to protect the competitiveness of American businesses operating worldwide.

Overview of the United States Intelligence Community for the 111th Congress

URL: http://www.dni.gov/overview.pdf

--------- P ---------

PACER – See: Public Access to Court Electronic Records (PACER)

Personnel Recovery (PR) 101 Series

Personnel Recovery (PR) 101 series consists of three courses (A-C) totaling 12 hours of individual instruction. The intended audience consists of all Soldiers (active, reserve, and National Guard) and Department of the Army (DA) civilians and contractors. Army PR 101A is the annual recurring PR training requirement and Army PR 101B and 101C will together replace SERE 100/100.1 as the Army’s Level A SERE trainers and meet current and projected theater entry requirements.

- Army PR 101B, PR in a Non-Adversarial Environment.
- Army PR 101C, PR in an Adversarial Environment.

Available from through on CD/DVD from Defense Imagery at http://defenseimagery.mil
Personnel Recovery Course (DOCNET)

URL:  http://www.dtic.mil/doctrine/docnet/courses/operations/csar.htm

Primary objectives of the DOD's personnel recovery system; roles and responsibilities related to personnel recovery; personnel recovery planning processes, procedures, and products; five personnel recovery tasks (2 hrs)  This course is available to military (.mil) domain users only.

Personnel Recovery (Fundamentals) on JKO J3OP-US018

URL:  http://jko.jfcom.mil/ (See course catalog)

Fundamentals of Personnel Recovery provides an overview of the DOD implementation of joint personnel recovery doctrine. The course familiarizes the student with all aspects of personnel recovery, from the governing directives, instructions, and joint doctrinal concepts to the importance of integrating evasion and recovery into existing operational plans to support military operations across the spectrum of conflict. It is not a tactical level course; the intent is for exposure to the personnel recovery arena from the strategic- and operational- levels of war. (5 hrs.)

Physical Security

Certified Physical Security Officer
URL:  http://hits.astcorp.com/security/cpso.html

Enhancing Information Assurance through Physical Security
URL:  http://iase.disa.mil/eta/enhanc-ia-phys-sec/

Physical Security - FM 3-19.30 (U.S. Army)
URL:  http://www.wbdg.org/ccb/ARMYCOE/FIELDMAN/fm31930.pdf

Physical Security Criteria for Federal Facilities
URL:  http://training.fema.gov/EMIWeb/IS/is892.asp

Physical Security Professional - ASIS Certification
URL:  http://www.asisonline.org/certification/psp/pspabout.xml

Physical Security for SIPRNet (DoD PKI Cert req'd)
URL:  https://powhatan.iiie.disa.mil/eta/phys-sec/index.html

Physical Security Training Program (PSTP)

Federal Law Enforcement Training Center
Police Intelligence Course

URL:  http://www.mctft.com/edrug_training/view_course.aspx?courseNumber=MCD0159

This course will provide law enforcement, intelligence personnel, and analysts with information necessary to understand the intelligence cycle - Direction, Collection, Processing, and Dissemination - and the techniques used to organize and analyze data. In addition to this, training will also include Federal laws applicable to the gathering of intelligence and its use.

In this course, the student will learn about:

- Reviewing the legal direction and authority of intelligence gathering
- Collecting intelligence information
- Reporting and processing the raw information
- Analyzing gathered intelligence
- Disseminating the analyzed product
- Threat Assessment
- The potential nexus between illegal activities and criminal acts
- The way in which Police Intelligence Operations filters through the other law enforcement functions in both tactical and non-tactical environments
- The intelligence cycle
- Rules, regulation, and laws that provide the basis of intelligence operations
- The importance of the direction and planning in the intelligence operations
- Issues to consider when planning intelligence operations
- The types of intelligence resources
• The general types of intelligence information
• The purpose for intelligence collection
• Importance of reporting and processing within the intelligence cycle
• Types of reporting
• The types of data entry points
• The need for prioritizing reports
• Collecting telephone data
• Deciphering telephone records
• Intelligence Education & Training
• Analyzing telephone records
• Charting the analysis of calls
• Developing an understanding of the use and applicability of a DNR/pen register
• The role of dissemination and integration in the intelligence cycle
• Types of intelligence classification
• Reasons why some materials receive classified status
• Limitations to dissemination of intelligence products
• Types of distribution systems

Target Audience: Active military, active law enforcement, and criminal justice professionals

Course Duration: 16 hours

**Police Intelligence Operations** - FM 3-19.50 - 29 July 2010


**Posse Comitatus Act**

The Posse Comitatus Act (PCA) was passed by Congress in 1878 following the election of Rutherford B. Hayes as President and the end of Reconstruction. The Act was an effort to prevent troops from performing in a law enforcement capacity except when authorized by the Constitution or an Act of Congress.

The PCA applies to all Title 10 military personnel in four of the five components of the Armed Forces—the Army, Navy, Air Force, and Marine Corps (and their respective Title 10 Reserves).
The PCA never applies to the fifth component of the Armed Forces, the Coast Guard, even when placed under Department of Defense (DoD) command.

The PCA does not apply to the other two components of the seven Uniformed Services—the Commissioned Corps of the Public Health Service, and the Commissioned Corps of the National Oceanic and Atmospheric Administration (NOAA)—even though both have the same rank structure and wear the same uniform as the Navy.

The PCA prohibits federal, state, and local leaders from using federal forces for direct civil law enforcement. Prohibited activities include searches, seizures, arrests, apprehensions, conducting security patrols, crowd and traffic control, and any other similar activities on behalf of civilian law enforcement authorities. Prohibiting direct military involvement in law enforcement is in keeping with long-standing United States law and policy limiting the military’s role in domestic affairs.

**Military Support for Civilian Law Enforcement Agencies, 10 USC 371-381, DoDD 5525.5**

In 1981 Congress passed the Military Support to Civilian Law Enforcement Agencies statute, Title 10 USC, Sections 371-379, which codified several Federal District Court decisions that found the PCA is not an absolute prohibition on DoD involvement with civilian law enforcement agencies. DoD personnel may provide support to civil law enforcement agencies as long as the support is “passive” and “indirect,” military personnel do not subsume the role of a law enforcement official, and military personnel do not subject civilians to compulsory military authority.

**§ 371 Information collected during the normal course of training or operations concerning violation of a federal or state law:**

The Chairman of the Joint Chiefs of Staff (CJCS) Standing DSCA Execution Order (EXORD), dated 14 August 2009, states, “Information collected on U.S. Persons by military personnel in a Title 10 USC status during [a DSCA] mission that indicates the existence of a threat to life or property or the violation of law will be turned over to civilian law enforcement official IAW [in accordance with] DoDD 5200.27, ‘Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense,’ and [Enclosure 2 to] DoDD 5525.5, DoD Cooperation with Civilian Law Enforcement Officials.


One of the exceptions mentioned in DoDD 5525.5 is the "Military Purpose Doctrine." Although this exception on its face does not have a direct Constitutional or Act of Congress basis, federal courts have validated the exception by recognizing that it is embedded in DoDD 5525.5 and that this directive was required by Congress in Section 375 of the Military Support to Civil Law Enforcement Act of 1981.
As long as the DoD unit is performing a legitimate military or foreign affairs function, then any law enforcement benefit to civil law enforcement authorities will be considered “incidental” and would not be a violation of the PCA.

For example, in 1959 the Girl Scouts asked the Army to provide generators and communications equipment to support their Girl Scout Round-Up outside of Colorado Springs, Colorado. The Army agreed, but also wanted to send a platoon of Military Police (MPs) to protect this military equipment by conducting patrols inside and along the perimeter of the Round-Up. Would these security patrols be a violation of the PCA? No, because the primary purpose for the MPs and the patrols would be to protect military property, a legitimate military purpose. Consequently, any benefit to the local civil law enforcement authorities, such as the patrols serving as a deterrent to any criminal activity, would be —incidental and thus permissible.

The following activities are NOT restricted under Posse Comitatus:

- Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities. This provision must be used with caution, and does not include actions taken for the primary purpose of aiding civilian law enforcement officials or otherwise serving as a subterfuge to avoid the restrictions of the Posse Comitatus Act.
- Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ)
- Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regardless of whether there is a related civil or criminal proceeding.
- Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation or facility.
- Protection of classified military information or equipment.
- Protection of DoD personnel, DoD equipment, and official guests of the Department of Defense.
- Such other actions that are undertaken primarily for a military or foreign affair's purpose.
- Protection of Federal property and functions authorizes Federal action, including the use of military forces, to protect Federal property and Federal Government functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection.

Pre-OCONUS Travel File (PRO-File)

URL: [https://medinah.sed.monmouth.army.mil/PRO-File/](https://medinah.sed.monmouth.army.mil/PRO-File/) (Requires AKO Log-in)
Before any soldier deploys or goes on TDY Outside the Continental United States (OCONUS), they must complete a Pre-OCONUS travel File (PRO-File).

What is PRO-File?

All of the Geographic Combatant Commands require personnel to complete a Personnel Recovery Mission Software (PRMS) digital ISOPREP prior to entering their respective geographic areas of responsibility. However; most Army personnel do not have classified system access on a regular basis prior to deployment.

HQDA developed the PRO-File program to enables Soldiers, DA Civilians, and DA Contractors to meet these theater entry requirements. PRO-File is the Army's interface with PRMS. Although a PRO-File survey is not an ISOPREP, it is the only authorized alternative for use on unclassified networks.

All Soldiers, DA Civilians, and DA Contractors are required to complete a PRO-File survey prior to departing CONUS for official duty. Army personnel departing for the USPACOM AOR, for official or unofficial travel, must complete this requirement as well.

Army forces assigned to USSOCOM or USASOC organizations are exempt from this requirement and will continue to follow USSOCOM guidance for completion of ISOPREPS. Civil Affairs and Psychological Operations forces operating under the control of a conventional force commander are not exempt from this requirement. Official PRO-File implementation guidance can be found in All Army Activities Message (ALARACT) 156/2007.

Pretty Good Privacy (PGP)


Pretty Good Privacy or PGP is an encryption program developed by Phil Zimmermann and published in 1991. It was one of the first public-key encryption programs available to the general public, and has today become the "unofficial standard" for encryption of e-mail and personal communication on the Internet.

PGP uses public key encryption. It has one key (a public key) for encryption and a second key (a private key) for decryption. With PGP installed on your computer you can encrypt a message to any person whose public key you possess. However, the only way to then decrypt that message is to possess the associated private key. Thus when using PGP you give your public key to everyone, add it to key servers, and maybe even publish it on the Internet, but you keep your private key secret and secure, thereby ensuring that while anyone can encrypt a message and send it to you, only you can decrypt and read that message.
People who use PGP on a regular basis will often publish their PGP public key to a "key server". A key server is simply a site where you can search for a person's public key and post your own public key for others to use. PGP key servers are run by several groups and organizations, but some of the major key servers can be found on-line at:

- MIT PGP Public Key Server - http://pgp.mit.edu/
- PGP Corporation Public Key Server - http://keyserver.pgp.com/
- DFN-CERT Public Key Server (Germany) - http://wwwkeys.pgp.net/
- University of Mainz (Germany) Public Key Server - http://pgp.uni-mainz.de/

If you use PGP you could visit anyone of these PGP key servers and locate the author's PGP public key. This would give you a way to securely contact the author of this book without first having met him or otherwise exchanged any type of encryption key. If you included a copy of your own PGP public key in your e-mail, or if your PGP public key was posted to the key server you could receive an encrypted reply to your e-mail... a reply that only you could read.

PGP is available for most operating platforms and systems, and is available as freeware from the PGP International site at: http://www.pgpi.org/. Gnu Privacy Guard (GnuPG) is a PGP compatible free implementation of the OpenPGP standard. GnuPG is available on-line at: http://www.gnupg.org/

**Problem Analysis Module**

URL:  http://www.popcenter.org/learning/pam/

Problem Analysis Module (PAM) gives you a framework for analyzing any persistent crime and public safety problem. PAM will ask you to input information concerning every aspect of the problem and then suggest the kinds of responses you could try.

PAM was developed to assist police problem solving through the asking of specific questions. The questions come from research into a set of powerful theories within the field of Environmental Criminology – particularly Routine Activity Theory, Situational Crime Prevention, and Crime Pattern Theory.

**Protected Critical Infrastructure Information (PCII) Program**

URL:  http://www.dhs.gov/pcii
The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security and other federal, state and local analysts use PCII to:

- Analyze and secure critical infrastructure and protected systems,
- Identify vulnerabilities and develop risk assessments, and
- Enhance recovery preparedness measures.


---

**Protective Design Center - US Army Corps of Engineers**

URL: [https://pdc.usace.army.mil/](https://pdc.usace.army.mil/)

The PDC provides a number of engineering services related to force protection and protective design. The Corps of Engineers works on a cost-reimbursable basis. When the PDC provides services for customers, the customer covers all expenses, including the cost of labor and any costs for travel, if travel is involved.

**Psychological Operations**

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals. The purpose of Psychological Operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives. (JP 1-02)

**Psychology of Intelligence Analysis**

Richards J. Heuer, Jr.
Center for the Study of Intelligence
Central Intelligence Agency 1999
Table of Contents
Author's Preface
Foreword by Douglas MacEachin
Introduction by Jack Davis

PART I--OUR MENTAL MACHINERY
Chapter 1: Thinking About Thinking
Chapter 2: Perception: Why Can't We See What Is There to Be Seen?
Chapter 3: Memory: How Do We Remember What We Know?

PART II--TOOLS FOR THINKING
Chapter 4: Strategies for Analytical Judgment: Transcending the Limits of Incomplete Information
Chapter 5: Do You Really Need More Information?
Chapter 6: Keeping an Open Mind
Chapter 7: Structuring Analytical Problems
Chapter 8: Analysis of Competing Hypotheses

PART III--COGNITIVE BIASES
Chapter 9: What Are Cognitive Biases?
Chapter 10: Biases in Evaluation of Evidence
Chapter 11: Biases in Perception of Cause and Effect
Chapter 12: Biases in Estimating Probabilities
Chapter 13: Hindsight Biases in Evaluation of Intelligence Reporting

PART IV--CONCLUSIONS
Chapter 14: Improving Intelligence Analysis

Public Access to Court Electronic Records (PACER)

URL: http://www.pacer.gov/

Public Access to Court Electronic Records (PACER) is an electronic public access service that allows users to obtain case and docket information from federal appellate, district and bankruptcy courts, and the PACER Case Locator via the Internet. PACER is provided by the
federal Judiciary in keeping with its commitment to providing public access to court information via a centralized service.

--- Q ---

**QR Codes**

A QR Code is a matrix code (or two-dimensional bar code) created by Japanese corporation Denso-Wave in 1994. The "QR" is derived from "Quick Response", as the creator intended the code to allow its contents to be decoded at high speed.

The QR code is that carry meaningful information in the vertical direction as well as the horizontal, hence the two-dimensional term. By carrying information in both directions, QR code can carry up to several hundred times the amount of data carried by ordinary bar codes.

QR Codes storing addresses and URLs may appear in magazines, on signs, buses, business cards, or just about any object that users might need information about. Users with a camera phone equipped with the correct reader app can scan the image of the QR Code causing the phone's browser to launch and redirect to the programmed URL.

The use of the QR Code is free of any license. The QR Code is clearly defined and published as ISO standard. Denso Wave owns the patent rights on QR Code, but has chosen not to exercise them.

**QR Code data capacity**

- Numeric only Max. 7,089 characters
- Alphanumeric Max. 4,296 characters
- Binary (8 bits) Max. 2,953 bytes

--- R ---
Random Numbers

URL: http://www.random.org/

RANDOM.ORG offers true random numbers to anyone on the Internet. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. People use RANDOM.ORG for holding draws, lotteries and sweepstakes, to drive games and gambling sites, for scientific applications and for art and music. The service has been operating since 1998 and was built and is being maintained by Mads Haahr who is a Lecturer in the School of Computer Science and Statistics at Trinity College, Dublin in Ireland.

Ranger Handbook - SH 21-76 (July 2006)


Regional and State Online Resource for Emergency Management

URL: http://rasor.jsrts.org/

The capability displays conventional maps, digital satellite imagery or both, and it can create custom map overlays. The maps can be configured to display icons for key places.

Regional Information Sharing System (RISS)

URL: http://www.riss.net/

RISS is a national program of regionally oriented services designed to enhance the ability of local, state, federal, and tribal criminal justice agencies to:

- Identify, target, and remove criminal conspiracies and activities spanning multijurisdictional, multistate, and sometimes international boundaries.
- Facilitate rapid exchange and sharing of information among the agencies pertaining to known suspected criminals or criminal activity.
- Enhance coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be inter-jurisdictional in nature.
RISS supports a proactive, preventive approach and offers services, tools, and resources to aid law enforcement and criminal justice entities to identify, disrupt, and prevent terrorist and criminal activities.

The RISS Program operates in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. RISS is the collective effort of six regional centers. While the RISS centers operate independently and are tailored to support the unique needs of the region served, they also operate as a collective body to address national criminal justice issues.

Report Intelligence Information

301-348-1050 (IMI) - REPORT INFORMATION OF POTENTIAL INTELLIGENCE VALUE (INTERACTIVE MULTIMEDIA INSTRUCTION) - 1 JAN 2007


301-371-1000 (IMI) - REPORT INTELLIGENCE INFORMATION (INTERACTIVE MULTIMEDIA INSTRUCTION) - 1 JAN 2007


URL:  http://www.gpoaccess.gov/wmd/

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction was established in 2004 and charged with examining the capabilities and challenges of the American intelligence community concerning the capabilities, intentions, and activities of foreign powers relating to the design, development, manufacture, acquisition, possession, proliferation, transfer, testing, potential or threatened use, or use of weapons of mass destruction, related means of delivery, and other related threats of the 21st Century.

The Full Report (3.3 MB, 618 pages) has been made available in its entirety, as a single PDF file. The report is also available as a collection of smaller PDFs arranged in a browse table based on the Final Report's summary of contents.

**Request for Intelligence Information (RII)**

RIIs are usually generated by a subordinate command, but may be sent laterally or down as taskings, to obtain intelligence or information collection support for needs that exceed organic capabilities. Requests received that exceed organic requirements are always consolidated and forwarded to the next higher echelon as RII. When prepared, the RII must indicate the degree of urgency and the type of request being made. When received, the requests are assigned priorities depending on the criticality and the timeline specified by the requester.

**Resource Tool for Security Professionals**

URL:  https://enrol.dss.mil/courseware/resource_tool/

**Rewards for Justice**

URL:  http://www.rewardsforjustice.net/

The Rewards for Justice Program, administered by the U.S. Department of State's Diplomatic Security Service, is one of the most valuable U.S. Government assets in the fight against international terrorism. Under this program, the Secretary of State may offer rewards for information that prevents, frustrates, or favorably resolves acts of international terrorism against
U.S. persons or property worldwide, including by dismantling an organization in whole or significant part. Rewards also may be paid for information leading to the arrest or conviction in any country of any individual attempting, committing, conspiring to commit, or aiding and abetting in the commission of such acts or to the identification or location of an individual who holds a key leadership position in a terrorist organization.

**RFFlow Crime Analysis Charts**

URL:  [http://www.rff.com/sampleriminal_analysis.htm](http://www.rff.com/sampleriminal_analysis.htm)

It is often easier to modify an existing chart than to draw a new one. If you haven't done so already, download the free trial version of RFFlow. Once it is installed, you can open the samples on this page directly in RFFlow by double-clicking the links to the right of each picture. From there you can zoom in, edit, and print the sample chart.

**Risk Terrain Modeling Manual**

URL: [http://www.rutgersefps.org/rtm/](http://www.rutgersefps.org/rtm/)

Risk Terrain Modeling (RTM) is an approach to risk assessment that standardizes risk factors to common geographic units over a continuous surface. Separate map layers representing the presence, absence, or intensity of each risk factor at every place throughout a terrain is created in a Geographic Information System (GIS), and then all risk map layers are combined to produce a composite “risk terrain” map with attribute values that account for all risk factors at every location throughout the geography. RTM aids in strategic decision-making and tactical action by showing where conditions are ripe for events to occur in the future.

This manual is offered as a primer on risk in the criminal event and demonstrates effective ways to apply RTM to crime analysis and policing operations. It begins with a review of the RTM approach to spatial risk assessment and presents a short overview of the theoretical underpinnings of criminological theory that have addressed the social and environmental factors that contribute to crime patterns, hotspots, and risk terrains. The second part details the technical steps for analysts to take in using ArcGIS software to develop risk terrain maps. The third and final part presents ideas of how RTM works in strategic and tactical decision-making, particularly within the context of the ACTION model for risk-based intelligence-led policing.

With this manual, analysts can produce risk terrain maps that give actionable meaning to the relationships that exist between place-based indicators and crime outcomes. Planners can use this approach to develop strategic models to forecast where crime problems are likely to emerge and to engage in steps that might reduce risks of crime occurring in the future.
Rosetta Stone Language Program

URL:  http://usarmy.rosettastone.com/

All Active Army, Army National Guard, Army Reserve, DA Civilians, USMA or ROTC contracted cadets should go to usarmy.skillport.com to access Army e-Learning where you'll have online access to Rosetta Stone® courses in thirty one languages. The Rosetta Stone breakthrough Dynamic Immersion method teaches you to understand spoken and written language and quickly develops your speaking and writing skills.

ROT13

ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple substitution cipher used in online forums as a means of hiding spoilers, punchlines, puzzle solutions, and offensive materials from the casual glance. ROT13 has been described as the "Usenet equivalent of a magazine printing the answer to a quiz upside down". ROT13 is an example of the Caesar cipher, developed in ancient Rome.

In the Basic Latin alphabet, ROT13 is its own inverse; that is, to undo ROT13, the same algorithm is applied, so the same action can be used for encoding and decoding. The algorithm provides no cryptographic security, and is often cited as a canonical example of weak encryption. ROT13 has inspired a variety of letter and word games on-line, and is frequently mentioned in newsgroup conversations.
ROT47

ROT47 is a derivative of ROT13 which, in addition to scrambling the basic letters, also alternates numbers and the most common symbols. Instead of using the sequence A-Z as the alphabet, ROT47 uses a larger set of characters from the common character encoding known as ASCII. ASCII maps letters, digits, punctuation and other special characters to numbers in the range 0-127. ROT47 uses just 94 of these characters (it excludes 'space' for instance), from '!' (the exclamation mark, ASCII code 33) to '~' (the tilde, ASCII code 126), rotating them by an offset of 47 positions. The method also takes into consideration change in case. For example, the character A is mapped to p, while a is mapped to 2. A second application of ROT47 would restore the ciphered text to the original. The use of a larger alphabet is intended to produce a more thorough obfuscation than that of ROT13.

--------- S ---------

S2 Safety & Intelligence Institute
Distance Learning Programs

URL:  http://www.s2institute.com/index.php

The S2 Institute offers several distance learning programs. Examples of the courses offered include:

Anti-Terrorism Officer Program - The distance learning version of the S2 Anti-Terrorism Officer (ATO) Program is designed to prepare frontline security and police officers for deployment in environments where terrorism is a critical threat. This program provides an exploration of contemporary terrorist methods and basic anti-terrorism skills and knowledge that all officers should possess.

Bomb Security for Executive Protection - The S2 Bomb Security for Executive Protection distance learning course provides students with essential skills for protecting individual principals against assassination by the use of explosives. In this 12-hour advanced-level course, anti-terrorism expert Craig Gundry explores IED technology, explosive assassination methods used by professional adversaries, and measures for preventing, detecting, and mitigating explosive attacks.

Covert Surveillance for Private Investigators - In the S2 Covert Surveillance for Private Investigators course, veteran private investigator Ron Azarello and S2 Staff Instructor Craig Gundry survey the strategies, tactics, and technology available for use in conducting surveillance
operations in private investigations. Although the core of this course is focused on surveillance technique and technology, considerable attention is also devoted to important parallel topics such as legal issues, teamwork, report writing, and more.

**Defense Against Anti-Vehicle Explosive Attacks** - Attacks against vehicles in transit by the use of explosives have emerged in recent years as some of the most popular methods of assassination by terrorists and professional adversaries. In this two hour distance learning program, bomb security expert Craig Gundry examines the spectrum of explosive related threats to vehicles in transit and provides effective strategies for countering these risks.

**Human Intelligence for Law Enforcement** - The S2 Human Intelligence for Law Enforcement distance learning program is designed to provide new and experienced homeland security and law enforcement intelligence professionals with a deeper understanding of the HSINT intelligence process and successful strategies for solving domestic counterterrorism problems through effective use of human intelligence. The instructor, a former CIA Senior Field Operations Officer, draws on his previous experience in dismantling Al-Qaeda operations overseas to present students with practical strategies for planning and executing domestic HUMINT operations in addition to valuable advice about working in collaboration with the US Intelligence Community.

**WMD & The Intelligence Function** - In today's threat environment, law enforcement and national-level intelligence professionals are increasingly called on to gather and assess information about chemical and biological terrorism or suspected weapons programs. In this 13-hour distance learning course, former UN Weapons Inspector Harvey J. McGeorge demystifies the complex world of chemical and biological WMD and provides effective strategies for identifying, collecting, and analyzing CBW information.

**SARDOT (Search and Rescue Dot)**

The SARDOT is a geographic location known only to friendly forces that allows Isolated Persons (IP) to pass their location over an unsecured radio net without compromising their location. SARDOT locations and reporting procedures will be extracted from special instructions (SPINS) by the staff and will be included in ISG. The SARDOT is updated and disseminated daily (like challenge and password). The PR SPINS lists SARDOT locations; coordinate format; map datum; and GPS programming procedures, including bearing and distance formats. IP determine their bearing and distance to a SARDOT to determine and report their location.

SARDOT: The Search and Rescue Dot (SARDOT) is a coordinate point (or points) that are programmed into your navigation system to allow immediate reference when making a rescue call. Unlike the BULLSEYE, the SARDOT is used only for SAR related purposes. This point should be in a standardized waypoint location in the navigation system so all crewmembers can
access it without having to reprogram it each time. Do not name the Waypoint! Enter a code name if desired.

Your position is to be reported as a radial and distance from the SARDOT. A typical call would be, “Rescue, Rescue, Rescue, Call sign, bearing (magnetic degrees) at distance (nautical miles) from SARDOT (name).” Ensure navigation system is configured to read your bearing in magnetic north and your distance in nautical miles. If possible, GPS coordinate format should be on MGRS/DATUM WGS 84 to minimize spheroid deviation and error offset between the downed crewmember system and the rescue team navigation systems.

Do not use SARDOT references to encrypt enemy locations. Give enemy locations in the clear.

Do not utilize 243.0 or 121.5 if possible, as this frequency will likely also be monitored by all other enemy aircraft/units as well.

SARNEG: The Search and Rescue Numerical Encryption Grid

SARNEG: The Search and Rescue Numerical Encryption Grid (SARNEG) is a word system that allows encryption/decryption of position coordinates during plain-voice (non-secure) transmissions. SARNEG words will always consist of ten (10) non-repeating letters.

To Encrypt a Grid Coordinate:

When secure communication is not available, the SARNEG codeword may be used for encrypt/decrypt numerical information. The ten (10) letter SARNEG allows the user to overlay digits 0 – 9, left to right underneath each letter. Ensure that you start with zero (0), not one (1).

Example: The SARNEG codeword for Tuesday is “SLOT RACING”. Simply substitute the letters of the codeword in place of the numbers of the grid coordinate. If a person’s hole up location is at YJ 123 789, he would encrypt his location as “Lima, Oscar, Tango, India, November, Golf.” Normally the grid zone designator is not included.

Although the primary purpose of the SARNEG is to communicate position coordinates, it can also be used to authenticate a message.

To Authenticate a Message:
The challenger selects two (2) letters from the SARNEG code word of the day, one letter on either side of the desired response. The correct response is the letter that is bracketed by the two challenge letters. Example: The SARNEG codeword for Tuesday is “SLOTRACING”. The challenger wants “Tango Alpha” authenticated. The correct reply would be “Romeo”. Downed crewmembers should authenticate rescue forces just as the rescue forces will authenticate the person(s) to be rescued.

**Satellite Reconnaissance Advanced Notice (SATRAN) Program**

USSPACECOM is tasked by the Joint Strategic Capabilities Plan (JSCP) to provide timely notification of potential space-based reconnaissance of US forces worldwide by a foreign nation. This program is known as SATRAN and is a proven, reliable Operations Security (OPSEC) support tool that informs customers of expected foreign intelligence satellite overflights.

SATRAN reporting is site-specific and provides sufficient warning to allow recipients time to respond to a potential threat by employing cover, concealment or cessation of activity until the threat is passed.

Under JCS guidance, the Defense Intelligence Agency (DIA) is the manager for SATRAN. Operational execution of the program has been delegated to the USSPACECOM Combined Intelligence Center (CIC) at Peterson AFB, Colorado.

The Naval Space Operations Center (NAVSPOC), a component of Naval Space Command, is delegated the responsibility of providing satellite reconnaissance OPSEC support to US Navy and Marine Corps assets only.

Likewise, the US Army White Sands Missile Range (WSMR) produces satellite overflight times for users of the White Sands Ranges only.

**Security Fundamentals Professional Certification**


The Security Fundamentals Professional Certification (SFPC) serves as a valid and reliable indicator of a security practitioner's understanding of facts, concepts, and principles the DoD security community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to and protect DoD assets.

**Security Fundamentals Professional Certification Candidate Handbook**


---

**Senate Select Committee on Intelligence**

URL: [http://intelligence.senate.gov/](http://intelligence.senate.gov/)

The Committee was created by the Senate in 1976 to “oversee and make continuing studies of the intelligence activities and programs of the United States Government,” to “submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs,” and to “provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States.”

The Committee has 15 Senators: eight from the majority party and seven from the minority. The one-seat majority is dictated by Senate resolution and, unlike most other committees, does not change in proportion with the overall Senate ratio of majority to minority membership. The Committee structure is intended to reflect the nonpartisan nature of intelligence and encourage the Committee to work in a bipartisan manner. By resolution, the 15 SSCI members include two members (one per side) from the Appropriations, Armed Services, Foreign Relations, and Judiciary Committees in order to ensure appropriate coordination with those Committees. The Senate Majority and Minority Leaders and the Chairman and Ranking Member of the Armed Services Committee serve as ex officio SSCI members.

(Cross Reference: House Permanent Select Committee on Intelligence (HPSCI))

---

**Sensitive Homeland Security Information (SHSI)**

Any information created or received by an agency or any local, county, state, or tribal government that the loss, misuse, unauthorized disclosure, modification of, or the unauthorized access to could reasonably be expected to impair significantly the capabilities and/or efforts of agencies and/or local, county, state, and tribal personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism.

SHSI does not include any information that is:

- Classified as national security information pursuant to Executive Order 12958, as amended, or any successor order.
- Designated by Executive Order 12951, any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011), to require protection against unauthorized disclosure.
- Protected Critical Infrastructure Information (PCII) as defined in 6 Code of Federal Regulations (CFR) § 29.2.
- Sensitive Security Information (SSI) as defined in 49 CFR Part 1520.

**SENTRY**


The National Drug Intelligence Center (NDIC) SENTRY is an Internet-based system designed to collect and disseminate synthetic drug-related data in order to identify new trends at an early stage, evaluate their likely importance, and track their development.

SENTRY focuses on synthetic drugs that are primarily produced via a chemical process, such as LSD (lysergic acid diethylamide), MDMA (3,4-methylenedioxyamphetamine, also known as ecstasy), and methamphetamine. To be truly effective as an early warning system, however, the system also monitors prescription drugs, over-the-counter medications, botanical substances and extracts, and chemicals and products involved in the manufacturing of synthetic drugs.

SENTRY is accessible at www.sentry.usdoj.gov or via the NDIC Internet site. From the SENTRY web site, authorized users can submit information on a new or unusual synthetic drug-related activity via an electronic submission form, link to partner agencies and our listserv, search and receive NDIC products, and view previously reported submissions using the geographic information system capabilities.

**SERE 100.1 Level A - Code of Conduct Training Course**

URL: [http://jko.jfcom.mil/](http://jko.jfcom.mil/) (See course catalog - Course: J3T A-US022)

The purpose of this course is to provide DoD personnel the fundamental knowledge necessary to uphold the spirit and intent of the Code of Conduct and address the challenges of isolation, captivity, and recovery. It provides the essential Personnel Recovery and Survival, Evasion, Resistance and Escape (SERE) knowledge necessary for personnel to execute their responsibilities when isolated. The new SERE 100.1 blends the latest immersive gaming technology and scenario-driven activities with instructional video and other multimedia that focuses the student to develop SERE knowledge and skills, and at times, places them under realistic duress. This course also has personal interviews with former Vietnam, Desert Storm, and Operation Iraqi Freedom Prisoners of War (POW), which assist putting the course in a “yes, it can happen to me” perspective. Students will be guided through the correct tactics, techniques,
and procedures for outdoor survival and evasion, captivity resistance, captivity resolution through escape, and personnel recovery (PR). Ultimately, this course prepares the military member to return with honor, regardless of the circumstances of isolation.

**SERE Student Handbook (Navy & Marines)**


**Silobreaker**

URL:  [http://www.silobreaker.com/](http://www.silobreaker.com/)

Silobreaker is a search service for news and current affairs that aims to provide more relevant results to the end user than what traditional search and aggregation engines have been offering so far. Instead of returning just lists of articles matching a search query, Silobreaker finds people, companies, topics, places and keywords; understands how they relate to each other in the news flow, and puts them in context for the user through graphical results in its intuitive user interface.

The site pulls content on global issues, science, technology and business from thousands of news sources, blogs, multimedia, and other forms of news media from around the world. With the engine’s focus on finding and connecting related data in the information flow, Silobreaker’s user tools and visualizations are ideal for bringing meaning to content from either today’s Web or the evolving Semantic Web, or both.

**SIPRNet - Secret IP Router Network**

The Secret IP Router Network (SIPRNet) is DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56 kbps to 155Mbps. Remote dial-up services are available up to 115.2kbps. SIPRNet contact 703-882-2770

**Small Wars Journal**

URL:  [http://smallwarsjournal.com/](http://smallwarsjournal.com/)
Small Wars Manual - USMC, 1940

Smart Traveler Enrollment Program (STEP)
See: Travel Registration (US Department of State)

Social Engineering

Social Engineering Fundamentals, Part I: Hacker Tactics
URL:  http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Social Engineering Fundamentals, Part II: Combat Strategies
URL:  http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies

Solitaire Encryption Algorithm
URL:  http://www.schneier.com/solitaire.html

In Neal Stephenson's novel Cryptonomicon, the character Enoch Root describes a cryptosystem code-named "Pontifex" to another character named Randy Waterhouse, and later reveals that the steps of the algorithm are intended to be carried out using a deck of playing cards. These two characters go on to exchange several encrypted messages using this system. The system is called "Solitaire" (in the novel, "Pontifex" is a code name intended to temporarily conceal the fact that it employs a deck of cards) and [Bruce Schneier] designed it to allow field agents to communicate securely without having to rely on electronics or having to carry incriminating tools. An agent might be in a situation where he just does not have access to a computer, or may be prosecuted if he has tools for secret communication. But a deck of cards...what harm is that?

Solitaire gets its security from the inherent randomness in a shuffled deck of cards. By manipulating this deck, a communicant can create a string of "random" letters that he then combines with his message. Of course Solitaire can be simulated on a computer, but it is designed to be implemented by hand.
Solitaire may be low-tech, but its security is intended to be high-tech. I designed Solitaire to be secure even against the most well-funded military adversaries with the biggest computers and the smartest cryptanalysts. Of course, there is no guarantee that someone won't find a clever attack against Solitaire (watch this space for updates), but the algorithm is certainly better than any other pencil-and-paper cipher I've ever seen.

**Special Forces Handbook for the Fingerprint Identification System**
**TC 31-20-2 (Sept. 2008)**

URL:  [https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/tc31_20_2.pdf](https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/tc31_20_2.pdf) (AKO Required)

**Special Forces Personnel Recovery - FM 3-05.231 (June 2003)**

[https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/fm3_05x231.pdf](https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/fm3_05x231.pdf)

**Special Forces Special Reconnaissance Tactics, Techniques, and Procedures - ATTP 3-18.04 (FM 3-05.204) (JAN 2011)**

URL:  [https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/attp3_18x04.pdf?feedAHP=Y](https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/attp3_18x04.pdf?feedAHP=Y)

Special Reconnaissance (SR) are those “reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. These actions provide an additive capability for commanders and supplement other conventional reconnaissance and surveillance actions.” SR is one of the seven SF core tasks. SR operations can support the execution of any SF core task (such as, unconventional warfare, foreign internal defense, or direct action [DA]) and the operational or strategic objective of a geographic combatant commander. The conduct of SR by SF Soldiers supports the operational concepts found in both Joint and Army doctrine.

**Special Operations Forces Intelligence – FM 3-05.102 (July 2001)**

Special Operations Team - Alpha (SOT-A)

- Four-man team
- Provides Intelligence and Electronic Warfare support to Operational Detachments – Alpha
- Electronic Reconnaissance
- Electronic Surveillance
- Electronic Protection
- SIGINT Targeting
- Early Warning and Force Protection
- Conducts intelligence training with allied forces
- Can conduct unilateral or bilateral missions

SOT-A teams are normally deployed with an SF team to provide electronic warfare (EW) to the SF team commander during the operation. This may require SOT-A's to:

- Deploy independently and then infiltrate to join a deployed SF team.
- Deploy with the SF team.
- Deploy independently from the SF team.

When a SOT-A is deployed with an SF team, they provide security and support. A SOT-A has the capability to support an SF team with limited interrogation, translation, interpretation, and communications support. In addition to providing EW support to the SF team commander, the SOT-A transmits collected information for decryption, processing, analysis, and dissemination to the appropriate user.

The SOT-A teams are capable of operating in all environments and across the operational continuum in support of special operation elements. Their small size and ability to task organize in a variety of combat configurations supports SF commanders’ intelligence requirements.
**Squidmat** (courses of action evaluation program)

URL: http://faculty.tamu-commerce.edu/jmstauffer/Squidmat/

The program compares two or more courses of action based on two or more evaluation criteria. The user arranges the evaluation criteria in descending order of importance and tells the program how much more important each criterion is than the next lower criterion. These importance ratings are used to calculate weights for each criterion. SquidMat takes user-supplied values for each course-of-action/criterion combination and converts them to Z scores. Using the criterion weights, the program calculates weighted sums for each course of action. The course of action with the highest weighted sum is considered to be the best. SquidMat is designed as a replacement decision matrix program for the CAS3 program DECMAT.

**Stable Shadow Program**


The purpose of the Stable Shadow Program is to identify qualified government civilians, contractors, and former military personnel to hire and deploy as DA civilians, In Lieu of (ILO) military personnel, to resource critical MI shortages in CENTCOM's area of responsibility (AOR). The implementation of this program began FY06. The program is managed by DA G2.

**State and Local Antiterrorism Training (SLATT)**

URL: https://www.slatt.org/

The State and Local Anti-Terrorism Training (SLATT) Program is funded by the United States Department of Justice, Bureau of Justice Assistance. The Program provides specialized training for law enforcement personnel in combating terrorism and extremist criminal activity. In order to ensure that SLATT training always delivers the most up-to-date information, terrorism-related topics are constantly researched and reviewed, and timely information is offered regarding pre-incident preparation, investigation, prevention, and interdiction training.

The SLATT Program has been proactively involved in anti-terrorism research and training since 1996. It is entirely separate and fulfills a different need from First Responder and other related Weapons of Mass Destruction/Nuclear, Biological, and Chemical response training provided to emergency service personnel. SLATT focuses on the prevention of terrorism in the United States by providing the tools necessary for state and local law enforcement officers to understand, detect, deter, and investigate acts of terrorism in the United States by both international and domestic, or homegrown terrorists.
**Statistical Abstract of the United States**

URL: [http://www.census.gov/compendia/statab/](http://www.census.gov/compendia/statab/)

The Statistical Abstract of the United States, published since 1878, is the authoritative and comprehensive summary of statistics on the social, political, and economic organization of the United States.

Use the Abstract as a convenient volume for statistical reference and as a guide to sources of more information both in print and on the Web.

Sources of data include the Census Bureau, Bureau of Labor Statistics, Bureau of Economic Analysis, and many other Federal agencies and private organizations.

**Strategic and Competitive Intelligence Professionals (SCIP)**

URL: [http://www.scip.org/](http://www.scip.org/)

The Strategic and Competitive Intelligence Professionals (SCIP), formerly the Society of Competitive Intelligence Professionals, is a global nonprofit membership organization for everyone involved in creating and managing business knowledge. Our mission is to enhance the success of our members through leadership, education, advocacy, and networking. Specifically, SCIP provides education and networking opportunities for business professionals working in the rapidly growing field of competitive intelligence (the legal and ethical collection and analysis of information regarding the capabilities, vulnerabilities, and intentions of business competitors). Many SCIP members have backgrounds in market research, strategic analysis, or science and technology. Established in 1986, today SCIP has chapters around the world, with individual members in nations around the globe. In addition, SCIP has alliance partnerships with independent affiliate organizations in many countries.

**Strategic Studies Institute United States Army War College**

URL: [http://www.strategicstudiesinstitute.army.mil/](http://www.strategicstudiesinstitute.army.mil/)

The Strategic Studies Institute of the U.S. Army War College publishes national security and strategic research and analysis which serves to influence policy debate and bridge the gap between Military and Academia.
Stratfor: Global Intelligence

URL:  http://www.stratfor.com/

A private intelligence company which provides open-source information, current-awareness and analysis. Areas of focus are three Intelligence Centers: Global, CIS & Eastern Europe, and Asia; Hotspots (areas of current world conflict); Global Intelligence Update (GIU), a weekly and quarterly summary of events arranged around a specific theme; and quarterly and annual forecasts of economic and political events worldwide.

---

Studies in Intelligence

(Unclassified Extracts from Classified Studies)

URL:  https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html

---

Tactical Intelligence and Related Activities (TIARA)

TIARA encompasses those programs/activities outside the NFIP and JMIP that: 1) respond to operational commanders’ tasking for time sensitive information on foreign entities; 2) respond to national intelligence community tasking of systems whose primary mission is support to operating forces; 3) train personnel for intelligence duties; 4) provide an intelligence reserve; or 5) are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data. TIARA programs / activities are funded as part of normal Service budget development, and as a result are often embedded in larger force structure or weapon system budget lines.
Tactical Language & Culture Training System

URL:  http://support.tacticallanguage.com/

Alelo TLT, LLC  
12910 Culver Blvd. Suite J  
Los Angeles, CA 90066  
Telephone: 310-945-5985 (Support Hotline)  
Fax: 310-574-7599

The courses are free of charge to download by members of the US military.

If you have a .mil email address, register on this website to download your copies of the Tactical Iraqi, Tactical Pashto, Tactical Dari and Tactical French Language & Culture Training Systems software, manuals, and trainer materials.

Technical Support Working Group

URL:  http://www.tswg.gov/

Technical Surveillance Countermeasures (TSCM)

Includes techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidics, and acoustic means, as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information.

TSCM CI Special Agents are trained in sophisticated electronic and sensing equipment to identify technical collection activities carried out by adversary intelligence entities. The use of TSCM is critical to ensuring that sensitive and/or restricted areas are clear of any adversary intelligence-placed active or passive electronic sensing, or eavesdropping or collection devices. These areas include SCIF, secure working and planning areas, and C2 facilities.

References:

DoD S-5240.05-M-1, "The Conduct of Technical Surveillance Countermeasures (U)," Volume I, April 30, 2007
DoD 5240.05-M-2, "The Conduct of Technical Surveillance Countermeasures (U)", Volume II, November 13, 2007

Terms and Definitions of Interest for DOD Counterintelligence Professionals


Terrorism Awareness for Marines

URL:  https://www.marinenet.usmc.mil/marinenet/

This interactive course presents an overview of the motives and objectives of terrorists. Learners will gain an understanding of the organization, training, and operations of terrorist groups. They will also study the methods of surveillance employed by terrorists and learn measures of counter-surveillance and personal protection. Other topics covered include: residential and workplace security, protective travel measures, and hostage survival. 8-hours

Terrorist Identities Datamart Environment (TIDE)

A consolidated repository of information on international terrorist identities that is the authoritative database supporting the Terrorist Screening Center and the U.S. Government’s watch listing system.

Terrorist Screening Center (TSC)

1-866-872-5678 / 1-866-872-9001

E-mail: tsc@tsc.gov

The Terrorist Screening Center (TSC) maintains the U.S. government’s consolidated Terrorist Watchlist—a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity.
By supporting the ability of front line screening agencies to positively identify known or suspected terrorists trying to obtain visas, enter the country, board aircraft, or engage in other activity, the consolidated Terrorist Watchlist is one of the most effective counterterrorism tools for the U.S. government.

TSC is leading significant improvements in counterterrorism information sharing among federal, state, local, and international agencies by distributing information about encounters with known or suspected terrorists reported to its 24/7 call center.

**Top Secret America**
A Washington Post Investigation

URL:  [http://projects.washingtonpost.com/top-secret-america/](http://projects.washingtonpost.com/top-secret-america/)

"Top Secret America" is a project nearly two years in the making that describes the huge national security buildup in the United States after the Sept. 11, 2001, attacks.

The articles in this series and an online database at topsecretamerica.com depict the scope and complexity of the government's national security program through interactive maps and other graphics. Every data point on the Web site is substantiated by at least two public records.

**TOR - The Onion Router**

URL:  [http://www.torproject.org/](http://www.torproject.org/)

Tor is an encryption tool that can help you protect the confidentiality of your communications. Tor is a free, relatively easy to use tool primarily designed to protect your anonymity online. But it also has the side benefit of encrypting your communications for some of their journey across the Internet.

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.

**Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis (CIA, March 2009)**
This primer highlights structured analytic techniques—some widely used in the private sector and academia, some unique to the intelligence profession. It is not a comprehensive overview of how intelligence officers conduct analysis. Rather, the primer highlights how structured analytic techniques can help one challenge judgments, identify mental mindsets, stimulate creativity, and manage uncertainty. In short, incorporating regular use of techniques such as these can enable one to structure thinking for wrestling with difficult questions.

TRADOC Culture Center

URL: https://ikn.army.mil/apps/tccv2/

The TRADOC Culture Center provides relevant, mission-focused, accredited cross-cultural education and training in order to instill and empower Soldiers and Department of the Army Civilians with cross-cultural competencies and synthesize the Army’s cultural policy, training and standards.

Travel Registration (US Department of State)

URL: https://travelregistration.state.gov/ibrui/

Travel registration is a free service provided by the U.S. Government to U.S. citizens who are traveling to, or living in, a foreign country. Registration allows you to record information about your upcoming trip abroad that the Department of State can use to assist you in case of an emergency. Americans residing abroad can also get routine information from the nearest U.S. embassy or consulate.

Treason 101: By the Numbers

Espionage by the Numbers A Statistical Data Base
by: Lynn F. Fischer, DSS/Security Research Center
The Defense Security Service's (DSS) Security Research Center (SRC) maintains an unclassified espionage case database in order to gain a better understanding of the crime of espionage. The SRC database includes information on all Americans arrested and convicted of espionage against the U.S. since World War II. It contains information on over 100 variables for 148 cases from 1945 to through 1998.

**TRIPwire | Technical Resource for Incident Prevention**

URL:  [https://www.tripwire.dhs.gov/](https://www.tripwire.dhs.gov/)

TRIPwire is a comprehensive resource for information on terrorist design, manufacture, and employment of improvised explosive devices (IEDs). This secure information portal presents detailed IED research alongside operational terrorist source material to offer a unique perspective on global terrorism efforts from the terrorists themselves.

TRIPwire is sponsored by the Department of Homeland Security's Office for Bombing Prevention (DHS/OBP). TRIPwire is an online network designed to provide the state and local bombing prevention community with information on terrorist tactics, techniques, and procedures (TTPs) in order to better identify prevention opportunities involving improvised explosive devices (IEDs). TRIPwire aims to serve the bombing prevention community as a "one-stop resource" by offering a consolidated and expert-validated resource of near real-time information on improvised explosives and explosive devices (IEDs), relevant news, and threat alerts. It also facilitates information sharing and networking by offering collaboration tools such as community forums and secure e-mail.

**TrueCrypt - Free open-source disk encryption software**

URL:  [http://www.truecrypt.org](http://www.truecrypt.org)

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).
Files can be copied to and from a mounted TrueCrypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations). Files are automatically being decrypted on the fly (in memory/RAM) while they are being read or copied from an encrypted TrueCrypt volume. Similarly, files that are being written or copied to the TrueCrypt volume are automatically being encrypted on the fly (right before they are written to the disk) in RAM. Note that this does not mean that the whole file that is to be encrypted/decrypted must be stored in RAM before it can be encrypted/decrypted. There are no extra memory (RAM) requirements for TrueCrypt. For an illustration of how this is accomplished, see the following paragraph.

Let's suppose that there is an .avi video file stored on a TrueCrypt volume (therefore, the video file is entirely encrypted). The user provides the correct password (and/or keyfile) and mounts (opens) the TrueCrypt volume. When the user double clicks the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the TrueCrypt-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, TrueCrypt is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the TrueCrypt-encrypted volume to RAM (memory) and the process repeats. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.

Note that TrueCrypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and files stored in it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), files stored in the volume are inaccessible (and encrypted). To make them accessible again, you have to mount the volume (and provide the correct password and/or keyfile).

A beginner's tutorial to TrueCrypt is available here: http://www.truecrypt.org/docs/tutorial

**TSCM** – See: Technical Surveillance Countermeasures (TSCM)
Unconventional Warfare


Underground Facilities Analysis Center

The Underground Facilities Analysis Center (UFAC) uses national intelligence and non-intelligence resources to find, characterize, and assess underground facilities (UGFs) used by adversarial state and non-state actors. UFAC coordinates IC efforts to detect, analyze, collect, and report on UGF programs in support of U.S. policymakers, warfighters, and the defense acquisition community. The UFAC Director reports jointly to the Secretary of Defense and the DNI through DIA. UFAC is composed of elements from DIA, Defense Threat Reduction Agency (DTRA), NGA, and NSA.

Unified Facilities Criteria (UFC)

URL:  http://www.wbdg.org/ccb/browse_cat.php?o=29&c=4

Unified Facilities Criteria (UFC) documents provide planning, design, construction, sustainment, restoration, and modernization criteria, and apply to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with USD(AT&L) Memorandum dated 29 May 2002. UFC are distributed only in electronic media and are effective upon issuance.

The United States Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC) and the Office of the Air Force Civil Engineer are responsible for administration of the UFC system. Points of contact and procedures for the development and maintenance UFC documents are prescribed in the latest edition of MIL-STD-3007.

Uniform Crime Reports

URL:  http://www.fbi.gov/ucr/ucr.htm
The Uniform Crime Reporting (UCR) Program was conceived in 1929 by the International Association of Chiefs of Police to meet a need for reliable, uniform crime statistics for the nation. In 1930, the FBI was tasked with collecting, publishing, and archiving those statistics. Today, several annual statistical publications, such as the comprehensive Crime in the United States, are produced from data provided by nearly 17,000 law enforcement agencies across the United States. Other annual publications, such as Hate Crime Statistics and Law Enforcement Officers Killed and Assaulted address specialized facets of crime such as hate crime or the murder and assaults of law enforcement officers respectively.

**United States National Central Bureau (USNCB) - INTERPOL**

URL: [http://www.usdoj.gov/usncb/](http://www.usdoj.gov/usncb/)

The Interpol-United States National Central Bureau (USNCB) serves as the United States' representative to INTERPOL, the International Criminal Police Organization. Each of the 186 INTERPOL member countries establishes a National Central Bureau (NCB) to serve as the central point of contact for its law enforcement authorities to communicate with their counterparts in other INTERPOL member countries. Each NCB works with the police authorities in its country to transmit, respond to, and execute requests for assistance in criminal investigations and police matters to and from other countries’ NCBs via the INTERPOL communications network.

The USNCB is the central point of contact for all INTERPOL matters in the United States, and coordinates and transmits requests for investigative and humanitarian assistance between foreign police authorities and U.S. law enforcement authorities at all levels, from the small town police department to the large federal agencies. On a daily basis, the USNCB transmits thousands of messages about wanted fugitives, kidnapped children, terrorism, illegal drug trafficking, and other criminal activities to assist police investigations around the world.

The USNCB is a component of the U.S. Department of Justice, and is co-managed by the Departments of Justice and Homeland Security pursuant to a memorandum of understanding between the Departments.

The USNCB is comprised of permanent employees of the Department of Justice and staff detailed from other agencies. Agents, including the USNCB Director and Deputy Director, are detailed to the USNCB from federal and state law enforcement agencies for specified terms. Agents at USNCB are assigned to work in divisions dedicated to specific investigative areas.

Please note that the USNCB can only assist law enforcement authorities conducting their official duties. The USNCB is not permitted to assist private individuals or entities. Private individuals
seeking assistance in criminal matters should contact their local police department or other appropriate law enforcement officials.

University of Military Intelligence


The University of Military Intelligence (UMI) is not a brick and mortar university but we want you to think of us as your online training resource for Military Intelligence. At UMI, we provide web-based training and reference material for Military Intelligence professionals around the globe. Although, targeted towards the Intelligence community, UMI provides a variety of materials that are both relevant and useful to all military professionals. UMI consists of three major areas, our public section and UMI’s two password-protected areas, the UMI Secured Training Network and Self-Paced Training.

University of Military Intelligence courses include:

- Cryptologic Linguist Reclassification - Phase 1 (IMI Hours: 44)
- Dari Familiarization (IMI Hours: 15)
- Defense Strategic Debriefing Course (IMI Hours: 42)
- Detainee Operations (IMI Hours: 38)
- Every Soldier a Sensor - Leader Course (IMI Hours: 22)
- Garrison S2 Coordinating Staff Course (IMI Hours: 33)
- Imagery Analyst - Basic (IMI Hours: 42)
- Imagery Analyst - Intermediate (IMI Hours: 35)
- Imagery Analyst - Intermediate (IMI Hours: 35)
- Information Security - Security Training for Non-MI Garrison S2 Officers (IMI Hours: 8)
- Intel Analyst Military Decision-Making Process (IMI Hours: 6)
- Intelligence in Combating Terrorism - Anti-Terrorism (IMI Hours: 50)
- Intelligence in Combating Terrorism - Terrorist Threat Assessment (IMI Hours: 8)
- Intelligence Oversight (IMI Hours: 1.5)
- Intelligence Support to Garrison Operations (IMI Hours: 33)
- Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization (IMI Hours: 77)
• Iraqi Language Training (IMI Hours: 40)
• MI Anthropology - Afghanistan (IMI Hours: 22)
• MI Anthropology - Iraq (IMI Hours: 22)
• Pashto Familiarization Course (IMI Hours: 15)
• Pashto Headstart Course (IMI Hours: 100)
• Stability Operations & Support Operations (SOSO) (IMI Hours: 24)
• Tactical Questioning (IMI Hours: 16)

U.S. Army War College Guide to National Security Policy and Strategy
(2d Edition) - Edited by Dr. J. Boone Bartholomees Jr.

Download -
http://www.strategicstudiesinstitute.army.mil/Pubs/display.cfm?pubID=708

This edition of the U. S. Army War College Guide to National Security Policy and Strategy reflects to some extent recent changes in the structure of the core curriculum at the War College. The college broke its traditional core course, “War, National Policy and Strategy,” into two courses: “Theory of War and Strategy” and “National Security Policy and Strategy.” The result for this book is the expansion of the block on strategic theory and the introduction of a block on specific strategic issues. Because little time has past since the publication of the most recent version of this book, this edition is largely an expansion of its predecessor rather than a major rewriting. Several chapters are new and others have undergone significant rewrites or updates, but about two-thirds of the book remains unchanged. Although this is not primarily a textbook, it does reflect both the method and manner we use to teach strategy formulation to America’s future senior leaders. The book is also not a comprehensive or exhaustive treatment of either strategy or the policymaking process. The Guide is organized in broad groups of chapters addressing general subject areas. We begin with a look at some specific issues about the general security environment—largely international. The section on strategic thought and formulation includes chapters on broad issues of strategy formulation as well as some basic strategic theory. The third section is about the elements of national power. A section on the national security policymaking process in the United States precedes the final section that deals with selected strategic issues
For several years now, a number of mathematical, scientific, acquisition, and analysis disciplines have been converging as components of a larger discipline—geospatial intelligence. Geospatial intelligence has become the cornerstone of our national and homeland security through its place at the functional center of many diverse intelligence methods. Now, the private sector is experiencing a similar convergence of geospatial intelligence disciplines. From this, USGIF was formed, becoming the first and only foundation where members can work together—toward a mutual goal of improving our Nation’s homeland security through the benefits of their work. USGIF is the only organization of its kind aimed at bringing together the many disciplines involved in the geospatial intelligence sector to exchange ideas, share best practices, and promote the education and importance of a national geospatial intelligence agenda.
USMC Annual Security Awareness Training

URL:  http://www.usmc-mccs.org/employ/training/annualsecurity/launchPage.htm

This course will take approximately 3 hours to complete.

- Basic Information & Personnel Security
- Anti-Terrorism & Force Protection
- Counter-Espionage Awareness

Utilization of Internet Tools and Resources for Open Source Intelligence (OSINT)

Utilization of Internet Tools and Resources for Open Source Intelligence

URL:  http://www.onstrat.com/osint/

---------- V ----------

VBIED - Vehicle Born Improvised Explosive Device (VBIED)

Vehicle borne IEDs come in all shapes, colors, and sizes. From a simple passenger car, to a large delivery or sewage truck. There have even been instances of what appeared to be generators, donkey drawn carts, and ambulances used to attempt attacks. VBIEDs have increasingly used larger amounts of explosives, and the explosive charge has ranged anywhere from 100lbs to well over 1000 pounds. And has included things such as mortar rounds, rocket motors, rocket warheads, PE4 explosives, and artillery rounds. A growing technique is to have multiple vehicles
involved. The lead vehicle is used as a decoy or barrier buster, once it has been stopped or neutralized and the coalition forces start moving to inspect or detain – the main VBIED comes crashing though and into the crowd and detonates. Thus increasing their casualty ratio.

**VineLink**

URL:  https://www.vinelink.com/vinelink/initMap.do

VINELink is the online version of VINE (Victim Information and Notification Everyday), the National Victim Notification Network. This service allows crime victims to obtain timely and reliable information about criminal cases and the custody status of offenders 24 hours a day. Victims and other concerned citizens can also register to be notified by phone, email or TTY device when an offender's custody status changes. Users can also register through their participating state or county toll-free number.

**Virtual Cultural Awareness Trainer (VCAT)**

URL:  https://www.us.army.mil(suite/page/648483  (requires AKO / JKO)

Demo Video -  https://www.us.army.mil(suite/doc/25571264&inline=true

**VCAT Horn of Africa** - Provides cultural awareness training for the Horn of Africa region. Countries covered in the course include: Comoros, Djibouti, Eritrea, Ethiopia, Kenya, Madagascar, Mauritius, Seychelles, Somolia, Sudan, Tanzania, Uganda, and Yemen. Missions covered are civil affairs, security cooperation, and humanitarian relief.

**VCAT Northern Africa** - Provides cultural awareness training for the countries, regions, and languages that comprise the area known as Northern Africa. Countries covered in the course include: Algeria, Egypt, Libya, Morocco, Mauritania, and Tunisia. Missions covered are civil affairs, humanitarian assistance, and security cooperation.

**VCAT Afghanistan** - The final release will provide culture and language training for the regions of Kabul, Kandahar, and Jalalabad. Mission areas will include meetings and engagements and squad and platoon patrols and will cover initial meetings, local grievances, coordinating humanitarian assistance (HA)/commander's emergency response program (CERP) projects, conducting training with ANSF, and checkpoint manning / house searches.

------- W -------
Weather, Light & Time Data

National Climate Data Center
http://www.ncdc.noaa.gov oa/ncdc.html

NOAA Regional Climate Centers
http://www.ncdc.noaa.gov oa/climate/regionalclimatecenters.html

US Naval Observatory - Light Data

US Naval Observatory - Time References

The U. S. Naval Observatory is charged with maintaining the DoD reference for Precise Time and Time Interval (PTTI).

Web-Based Time Synchronization
http://www.usno.navy.mil/USNO/time/display-clocks

Telephone Time

USNO provides voice announcements of the time:
Time Voice Announcer, Washington, DC:
202-762-1401
202-762-1069
DSN 762-1401
DSN 762-1069

Time Voice Announcer, Colorado Springs, CO:
719-567-6742
DSN 560-6742

(Time may be delayed on long distances calls.)

Web Lens

URL: http://www.weblens.org/invisible.html
The terms invisible web, hidden web, and deep web all refer to the same thing: a massive storehouse of online data that the search engines don't capture. That's because terabytes of information are buried in databases and other research resources. Searchable and accessible online but often ignored by conventional search engines, these resources exist by the thousands. Known in research circles as the invisible, deep, or hidden Web, this buried content is an estimated 500 times larger than the surface Web, which is estimated at over four billion pages. This mass of information represents a potent research resource, no matter what your discipline or interest. Below are some tools to help you mine it. Students and serious researchers may also find our collections of web directories and scholarly and academic research tools and strategies useful.

**Why Law Enforcement Agencies Need an Analytical Function**

URL: [http://www.it.ojp.gov/documents/analysts_9_steps.pdf](http://www.it.ojp.gov/documents/analysts_9_steps.pdf)

Analysis is an integral part of every major investigation an agency opens. Often, small pieces of information that may appear insignificant can be a major part of a larger picture. The analytical function organizes these critical pieces of data and creates valuable and meaningful products to assist law enforcement in solving cases and prosecuting criminals. Personnel responsible for producing intelligence are professionals, civilian or sworn, whose training includes law enforcement analytical techniques and criminal analysis.

**WISER - Wireless Information System for Emergency Responders**


WISER is a system designed to assist first responders in hazardous material incidents. WISER provides a wide range of information on hazardous substances, including substance identification support, physical characteristics, human health information, and containment and suppression advice.

**World-Check**


World-Check risk intelligence reduces customer exposure to potential threats posed by the organizations and people they do business with. More than 5 400 institutions, including over 49 of the world's top 50 banks and 200 enforcement and regulatory agencies, rely on the World-
Check database of known heightened-risk individuals and businesses to efficiently screen their customers, associates, transactions and employees for potential risk.

World-Check’s research department methodically profiles individuals and entities deemed worthy of enhanced scrutiny, as well as occurrences of fraud, corruption, terrorism, money laundering, narcotics trafficking and many other types of financial crime. This highly structured database is regularly updated by our international research team and is derived from thousands of reliable public sources.

It also covers Politically Exposed Persons (PEPs), their family members and potentially high-risk associates worldwide, thus making World-Check risk intelligence the ideal solution for Politically Exposed Foreign Person (PEFP) and PEP screening.

World-Check’s proprietary database and tools are continually used in financial compliance, Anti Money Laundering (AML), Know Your Customer (KYC), Politically Exposed Person (PEP) screening, Enhanced Due Diligence (EDD), fraud prevention, government intelligence and enforcement, and other identity authentication, background screening and risk-prevention practices.

**World Health Organization - Country Profiles**

URL: [http://www.who.int/countries/en/](http://www.who.int/countries/en/)

**World News Connection**

URL: [http://wnc.fedworld.gov/](http://wnc.fedworld.gov/)

World News Connection® (WNC) is an online news service that offers an extensive array of translated and English-language news and information. Particularly effective in its coverage of local media sources, WNC provides you with the power to identify what really is happening in a specific country or region. Compiled from thousands of non-U.S. media sources, the information in WNC covers significant socioeconomic, political, scientific, technical, and environmental issues and events.

The material in WNC is provided to the National Technical Information Service (NTIS) by the Open Source Center (OSC), a U.S. government agency. For over 60 years, analysts from OSC's domestic and overseas bureaus have monitored timely and pertinent open-source materials, including gray literature. Uniquely, WNC allows you to take advantage of the intelligence gathering experience of OSC.
The information is obtained from full text and summaries of newspaper articles, Websites, conference proceedings, television and radio broadcasts, periodicals, and non-classified technical reports. New information is entered into WNC hourly every day. Generally, this information is available within 24-72 hours from the time of original publication or broadcast.

Regional categories covered include:

- Africa (Central, East, North, Southern, West)
- Americas (Caribbean, Central, North, South, Antarctica)
- Asia (East, South, Southeast)
- Eurasia (Caucasus, Central, Russia)
- Europe (Balkans, Central, North, South)
- Middle East
- Oceania

WNC is a valuable research tool for anyone who needs to monitor non-U.S. media sources.

Yahoo Countries

URL:  http://dir.yahoo.com/Regional/countries/
Zfone

URL:  http://zfoneproject.com/

Zfone™ is a new secure VoIP phone software product which lets you make encrypted phone calls over the Internet. Its principal designer is Phil Zimmermann, the creator of PGP, the most widely used email encryption software in the world.

Zfone uses a new protocol called ZRTP, which is better than the other approaches to secure VoIP, because it achieves security without reliance on a PKI, key certification, trust models, certificate authorities, or key management complexity that bedevils the email encryption world. It also does not rely on SIP signaling for the key management, and in fact does not rely on any servers at all. It performs its key agreements and key management in a purely peer-to-peer manner over the RTP media stream. It interoperates with any standard SIP phone, but naturally only encrypts the call if you are calling another ZRTP client. This new protocol has been submitted to the IETF as a proposal for a public standard, to enable interoperability of SIP endpoints from different vendors. Zfone is available as a universal "plugin" for a wide variety of existing VoIP clients, effectively converting them into secure phones. It's also available as an SDK to allow VoIP product vendors to integrate encryption into their products.

Zfone:

- Doesn't depend on signaling protocols, PKI, or any servers at all. Key negotiations are purely peer-to-peer through the media stream
- Interoperates with any SIP/RTP phone, auto-detects if encryption is supported by other endpoint
- Available as a "plugin" for existing soft VoIP clients, effectively converting them into secure phones
- Available as an SDK for developers to integrate into their VoIP applications
- Submitted to IETF as a proposal for a public standard, and source code is published

A public beta release of the Zfone software is available for download for Windows, Mac OS X, or Linux.
Contact Information

Michael Chesbro, CPO, CSS, CCIA, CFC, CAS, CHS-III, SSI, IAC
Criminal Intelligence Specialist / Certified Crime & Intelligence Analyst
DES OPSEC Officer / DES Security Manager / DES COMSEC Officer
Joint Base Lewis-McChord Fusion Center - Directorate of Emergency Services
Joint Base Lewis-McChord, Washington 98433
Tel: 253-966-7303 / DSN: 347-7303
Fax: 253-966-7318
AKO: michael.chesbro@us.army.mil
LEO: michael.chesbro@leo.gov