Surveillance Technologies

Introduction

Section

1

1 - Introduction and Overview

Surveillance Technologies

1

Introduction & Overview

1. Introduction

1.a. Scope and Focus

This book fills a significant gap in the literature related to surveillance. There are currently thousands of books about spies and international espionage, dozens of catalogs that list price information about ‘spy’ devices (though without any real explanation of their uses), and many recent books about loss of privacy from increasing levels of surveillance. There are also a few books on spy technologies as they relate to espionage and military use. However, until now, no book has adequately covered *surveillance devices* in a broader context so that readers can understand the origins and current practices of the technologies as they are used in a wide range of fields.

A page dotted with Base Censor and U.S. Censor Office stamps, in 1943, is an example of how written, radio, and wire communications are surveilled, probed, recorded, regulated, and subjected to constant scrutiny during times of political turbulence. [U.S. Army Signal Corp historic photo by McQuarrie, released.]

This volume discusses surveillance devices that are used in intelligence and military operations, but it differs from other books in that it provides a broader view of surveillance technologies that encompasses other applications including search and rescue, scientific enquiry, domestic applications, corporate security, skip tracing, and personal communications.

Specific Focus of this Volume

This book focuses primarily on the technologies of surveillance and secondarily on the ways in which they are used. It also provides a rich set of pointers to information on related organizations and more advanced publications in the field. It doesn't emphasize spies or intrigue or specific strategies for use because there are already many volumes covering these topics. Surveillance is a subset of the larger process of intelligence-gathering, and thus a key tool in intelligence operations, but it is also an equally important tool of wildlife conservation, weather forecasting, and corporate and domestic security.

This volume does not cover the design and engineering of surveillance devices (there are no circuit board or installation diagrams). It doesn't discuss technologies that may be used to extract information directly from human beings through coercion or torture. It also does not cover surveillance of nuclear radiation leaks except in a very general way. It does provide a wealth of information on the prevalent technologies that aid humans in hearing, seeing, smelling, and otherwise detecting and recording trends and activities, people, places, wildlife, and natural disasters.

While this book takes a broad view of surveillance devices, it has been necessary, in most cases, to use American examples and illustrations. The author would have preferred a more international viewpoint, but there are compelling and practical reasons for using U.S.-based examples. The first is that surveillance is a huge topic and it would be impossible in one volume to cover international activities and organizations with any kind of depth. Another is that the United States, as a global superpower, has put a high priority on the development and use of surveillance technologies and thus, they are widely available and widely used in the U.S. A further justification is that the price of surveillance devices in America has become so low that even teenagers are buying high-tech surveillance gadgets to secure their forts and treehouses.

Price and Availability

Surveillance devices are falling in price. They are showing up in mail order catalogs mixed in with ads for computer monitors and lawn furniture. A week's wages is now sufficient to set up a simple surveillance or security system whereas five years ago, the same setup would have cost several thousand dollars. These examples illustrate this trend:

- Board-level pinhole cameras can be purchased in bulk for under $25 each for high-resolution grayscale models. Outdoor color wireless bullet cameras are now under $200.
- Video/audio transmitters can be located for less than $33 each and a $120 VCR can be used to record the signal.
- Two-way radios with a two-mile range are now as low as $40.
- Basic computer systems are less than $800 and fully functioning older models are available for less than $40.
- A high-speed connection to the Internet (which was $500 in 1997) now costs only slightly more than a telephone dialup connection, about $29 to $39/month.

Consumer Devices

The design and manufacture of ‘spy’ devices are no longer limited to specialized markets. Surveillance technologies are consumer items and a general reference is needed to put the technology in perspective and provide information that isn’t yet available all in one place through existing sources. This is the first introductory text designed to meet this need. It could have been much longer, but I was constrained, as all authors are, by time and space. In spite of these constraints, this is currently the most comprehensive coverage of the subject from this broad perspective that is presently available.

Technology access isn’t limited to the U.S. Electronic devices are readily available in Europe, Japan, and Canada and some European countries offer free Internet access, but few countries in the world have as many inexpensive computer and electronics products as the United States and this is true of surveillance devices as well.

Political Openness

The sheer volume of *open source* information that is available in America due to enforcement of democratic freedoms and specific acts such as the Freedom of Information Act is substantial. To balance the American bias in this book, I have tried to select examples that generically illustrate a class of technologies and I trust that you, as reader, can extrapolate other possible uses from the information given.

You may be a layperson wanting to better understand this important topic, or you may be a student of political science, business, sociology, or forensics. You may be a beginning professional, involved in industrial surveillance, law enforcement, private detection, national security, archaeology, search and rescue, news-gathering, or corporate security. Whatever your status, this volume provides a broad overview and fundamental basis for understanding the types of devices that are used in surveillance activities. While it focuses chiefly on *devices*, there is also sufficient information to provide a sense of the *role* of these devices within the larger field of surveillance and the broad context of the gathering of *intelligence*.

1.b. Format

Understanding Surveillance Technologies is designed to be modular. The chapters have been organized so that they don’t have to be read in any particular order. Cross-references are provided to alert you to closely related information in other chapters. The only recommendation is that you read this introductory chapter first, in its entirety (you can probably scan-read the history section the first time around). It gives preliminary information relevant to all the chapters and will familiarize you with the general format of the rest of the book.

Individual chapters are also reasonably modular; some sections can be read out of order, depending on your interests and technical background. To make it easier to use as a reference, each chapter follows the same format, consisting of:

1. An *introduction* to the chapter providing the scope and focus.
2. *General types and variations*, sometimes including just a little bit of introductory physics.
3. The *context* in which the technologies are most commonly used.
4. A *historical basis* for the evolution of the various technologies (which is sometimes quite extensive) to provide a foundation for understanding where the technologies came from, how they were initially used, and how they evolved. Some of the histories include interesting anecdotes.

5. A *general description* of aspects not covered in the previous sections.
6. *Examples* of technologies used in practical applications and some *commercial sources* of some example devices.
7. Some of the *problems and limitations* inherent in a particular class of technologies.
8. Some of the *legislative restrictions, trends, and concerns* related to the use of the technologies. Keep in mind that use of surveillance technologies for some purposes is highly illegal, with severe penalties.
9. *Implications of use* of the technology to introduce some of the philosophical and ethical aspects of surveillance.

Extensive resource information for further study is grouped toward the end of each chapter. There's enough to provide a decade's worth of reading, but I have tried to pick the best references out of the thousands extant. They are numbered and organized as follows:

10. **Resources**

    10.a. **Organizations** - some of the prominent agencies related to the topic.

    10.b. **Print** - bibliographies of books, articles, and journals to aid the reader in locating intermediate and advanced print resources.

    10.c. **Conferences** - some of the more significant conferences and workshops, with an emphasis on top industry conferences that occur annually.

    10.d. **Online Sites** - selections of some of the more worthwhile sites on the Web.

    10.e. **Media Resources** - a handful media resources, including films, museums, and television broadcasts.

11. **Glossary** - a short list of words and abbreviations related to each subject area.

The author hopes that the modular format will maximize your enjoyment of this book, allowing you to choose topics at will. It also makes it useful as a reference book, after an initial reading, as similar items can be found in the same location in each chapter. The modular format necessitates some redundancy, but pays off with a great deal of flexibility. Training instructors using this as a textbook will appreciate this feature as well.

1.c. The Impact of Surveillance Technologies

Important Trends

While this text doesn't deal in depth with surveillance sociology or politics, it does provide enough sidenotes to illustrate some of the major trends. There are important changes occurring in the industry that are relevant to anyone planning to use or study surveillance technologies.

Surveillance is changing the way we view ourselves and our neighbors. It is even changing the ways in which we interact with one another and protect ourselves. In the last decade there have been some significant turnovers in the technologies that are used in surveillance. Just as word processors superseded typewriters, surveillance devices are superseding many traditional manual techniques of security and information-gathering. Motion sensors are being substituted for landmines, video cameras are being substituted for security personnel, DNA profiles are being substituted for traditional blood typing in parental custody lawsuits, and nanny monitors are being substituted for frequent trips to the nursery.

Mines to Motion Detectors. Beginning in 1961, the U.S. Naval Station at Guantanamo Bay, Cuba, installed approximately 50,000 antitank and antipersonnel landmines in the buffer zone separating Communist Cuba and the Bay. Following a 1996 Presidential Order, these were excavated, transported to a demolition site (left) and prepared for destruction (right). To ensure the continued security of the base, surveillance motion and sound detectors are being substituted. [U.S. DoD 1997 news photos by R. L. Heppner, U.S. Navy, released.]

Shift In Access

The capability to unobtrusively observe other people's business is power. With that power comes responsibility, whether or not it is mandated by law. Until the mid-1990s, the power of surveillance was mainly in the hands of local and federal government agents and, to a lesser extent, private detectives. This is no longer true. It is now possible to purchase an aerial picture of your neighbor's back yard for less than $20 that is sufficiently detailed for you to distinguish between a large dog house and a small hot tub. You can purchase an equally detailed picture of government buildings in foreign nations, a refugee tanker, a controversial logging site, or the production yard of your chief business competitor on the other side of town.

This civilian access has already resulted in some surprising revelations. Citizens have become, in a sense, an extension of the government surveillance system. Nuclear installations in other countries, for example, are now closely scrutinized by private individuals who are locating and disseminating information that previously was known and handled only by small government departments with limited budgets. It will be interesting to see where this trend will lead and whether citizen involvement will help or hinder national security objectives.

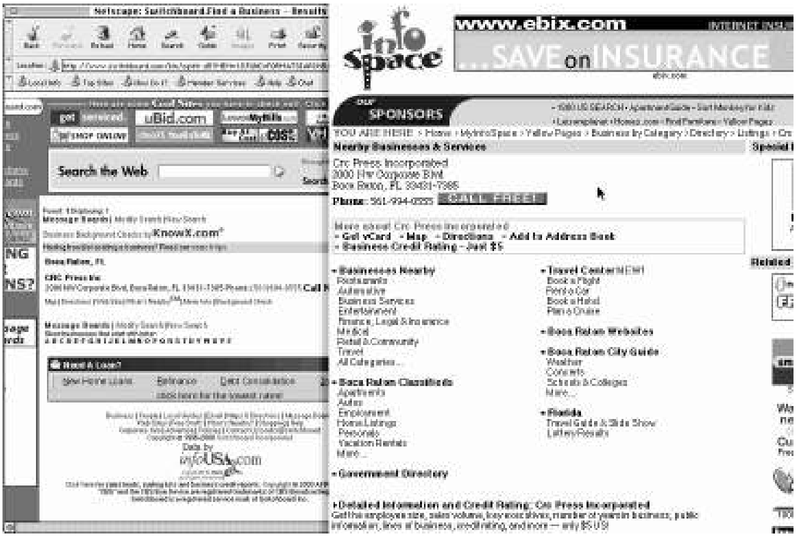
Web access is dramatically influencing surveillance. Intimate information is available as never before. You can log onto the Internet and use reverse phone directories, public records databases, and genealogical databases containing a remarkable amount of personal information. Marketing professionals are mining this data with a little more enthusiasm than most people would like, judging by the tidal wave of junk email and postal mail resulting from their efforts. These open-source databases and search engines are discussed in more detail throughout this text.

Legislative Considerations

Technology changes faster than laws can be drafted to protect the vulnerable. Currently, private citizens don't need any special permission to purchase or own most types of video or photographic surveillance images. They can download them off the Internet. Satellites and network distribution channels have put access to information in the hands of ordinary people in most of the democratic developed nations. More than half the populace now has access to the Net.

While military personnel are still the only ones who can get the highest resolution imagery, sometimes accessible in realtime, the gap between the information available to civilians and those in traditional positions of power (e.g., national defense) has narrowed dramatically. At the same time, this shift of access puts a great deal of power and responsibility in the hands of an underinformed public which, in free societies, is bound to result in some unethical and unscrupulous behavior on the part of a percentage of individuals willing or eager to take advantage of others. Lobbyists and lawmakers need to sit up and take notice of the possible negative consequences of broad distribution of personal and private information and of 24-hour surveillance of every member of the populace.

Responsibility and Social Evolution



Nearby Businesses & Services

Crc Press Incorporated
2000 Nw Corporate Blvd
Boca Raton, FL 33431-7385
Phone: 561-994-0555

More about Crc Press Incorporated
- Get vCard - Map - Directions - Add to Address Book
- Business Credit Rating - Just $5

- Businesses Nearby
- Travel Center
- Boca Raton Websites
- Boca Raton City Guide
- Boca Raton Classifieds
- Florida
- Government Directory

Detailed Information and Credit Rating: Crc Press Incorporated
Get the employee size, sales volume, key executives, number of years in business, public information, lines of business, credit rating, and more — only $5 US!

Switchboard (left) and InfoSpace (right) are just two of the many sources on the Web that now provide addresses and phone numbers of almost every directory listing in America (some cover Canada and the U.K. as well). Most of these Web-based businesses include value-added pay services. For example, in this search for CRC Press, InfoSpace also offered to provide detailed business and credit information on CRC including employee size, sales volume, key executives, number of years in business, public information, and lines of business for a flat rate fee of $5. Most Web-based directories allow you to view a map of the area and even to look up the names and numbers of people in neighboring houses. Such broad access to information from a distance was almost unknown five years ago and the ease of acquisition is changing the way private detectives are promoting and managing their investigations. [Classic Concepts Web capture, April 2000.]

Researching this book has given me concerns that we may be moving into a not-too-distant future in which newborn infants are implanted with radio tracking devices, without their knowledge or consent, to ‘ensure their safety’ from wandering or kidnapping. These actions may be well-intentioned initially but may subsequently be used to curtail freedom of choice and movement during their teenage years and beyond.

Free citizens reading this book today wouldn't accept that form of repression for a moment, but one or two generations of children who have never experienced our concept of freedom may not understand what they have lost until they reach adulthood, when it may be too late to change their surrounding social structure. A child who has been branded at birth doesn't understand the concept of a brand until at least adolescence and cannot undo it. Similarly, a child who has been implanted with a radio tracking beacon at birth won't understand the full ramifications of the device until he or she begins to try to become independent. It is important for us to understand surveillance technologies so we can safeguard future freedoms as well as those we currently enjoy. (If you don't believe these scenarios could happen, read the Radio Surveillance chapter on tracking devices and Visual Surveillance for software developments that allow a video camera to select and recognize individual faces in a crowd.)

To resolve the issues related to privacy and security, we must either evolve as a society to take more personal responsibility to respect the rights of others, or we must give up a significant portion of our freedoms and more stringently regulate access to and use of the new forms of personal and business information that are becoming available. Either way, society must change and adapt, because it may only be five years before satellites and unpiloted air vehicles can recognize and track not just backyard hot tubs, but individual people on the move, without their knowledge or consent. It might only be a decade before your every action can be recorded in realtime by satellites and intelligent software. We shouldn't allow a fascination with the technology or entrepreneurial greed cloud our judgment in such important matters.

2. Types and Variations

2.a. Basic Terms and Concepts

Each chapter in this book has a set of basic terms and concepts related to the topic of the chapter. Some generalized surveillance concepts/terms are listed here (additional terms are in the glossaries at the end of each chapter):

information In the context of surveillance, information consists of *knowledge, data, objects, events, or facts* which are sought or observed. It is the raw material from which intelligence is derived.

intelligence This is information which has been *processed and assessed within a given context.* Thus, the number of barrels of oil shipped by a nation in a year is *information* whereas the number of barrels of oil shipped by a nation in a year compared to other nations or compared to the previous year is *intelligence* if it can be used as an economic or political lever in comparative social contexts. It often is not known in advance what information may later become part of a body of intelligence. Prior to their fatal accident, the hotel videotaped sequence of Princess Diana and Dodi al Fayed leaving the hotel was information, whereas after the accident, it formed part of an extensive investigation, especially of the driver, contributing to a body of intelligence.

surveillance Surveillance is the *keeping of watch* over someone or something. Technological surveillance is the use of technological techniques or devices to aid in detecting attributes, activities, people, trends, or events.

covert Masked, concealed, or hidden. Covert activities are those which involve disguises, hidden equipment, camouflage, and shrouded activities intended to have a low probability of detection.

clandestine Secret, surreptitious, stealthy, sneaky, furtive. Thus, a detective hiding behind a curtain in a window using binoculars to view someone from a distance is engaging in *covert* behavior, whereas a detective standing in plain sight in normal attire but secretly monitoring someone's activities is behaving in a *clandestine* manner. Similarly, a corporate agent wiretapping a competitor is engaged in covert surveillance while a corporate representative chatting at lunch with a competitor without revealing his or her agenda is engaged in clandestine surveillance (this is further explained in Section 2.c., following).

occult Hidden, concealed, secret, not easily understood. Originally a generic term, this has gradually come to be associated with ghosts and psychics and has lost most of its practical use as surveillance jargon. However, it still has some relevance with regard to reports of 'supernatural' events. It is included here because classified military exercises or tests are sometimes interpreted by uninformed onlookers as occult or*paranormal* events.

reconnaissance Reconnaissance is a preliminary or exploratory survey to gain information. Job-hunters often do reconnaissance on potential employers and vice versa. Law enforcement agents conduct crime scene reconnaissance in preparation for a full investigation. Military intelligence agents conduct reconnaissance of hostile territory before sending in troops.

2.b. Disclaimer and Regulatory Restrictions

Most surveillance technologies are, in themselves, neutral technologies: not inherently helpful or harmful. Their implementation, however, is rarely neutral. Surveillance technologies are put into place for many reasons, including distrust, fear, curiosity, sexual gratification, profit, exploitation, sales pressure, and sometimes just because they are 'techie toys.' Once installed, the temptation to use them in unauthorized or inappropriate ways is substantial. The temptation to subtly alter the original mandate for their use may be even greater and can be equally as harmful.

This text is intended to be educational and thus presents a broad view of surveillance devices and their implementation. This format inherently requires descriptions of technologies *which may be restricted or illegal to own or use.* Many electronic eavesdropping devices may be built as hobby kits for learning about electronics and may even be legal to use in classrooms or homes, but may be *illegal* to use under other circumstances.

Legal restrictions vary greatly from country to country as do export criteria for the technologies described here. *This book does not make any endorsements for the illegal use of surveillance technologies.* Make sure you familiarize yourself with relevant regulations before making a purchase. Some of the general restrictions and regulations are listed toward the end of each chapter. Vendors will usually let you know if there are restrictions on the use of specific devices.

Each chapter in this book focuses on a specific technology and includes an overview of some of the more significant laws or statutes related to individual technologies to aid you in better understanding how devices may or may not be used. Note that these are primarily American laws which tend to be somewhat unique in global terms. If you are in another country, different rules probably apply.

2.c. Categories of Surveillance Activities

Surveillance technologies can be categorized in a number of ways:

- according to the physical nature of the technology itself (infrared, X-ray, visual, etc.),
- according to the type of data derived (visual, aural, digital, etc.), or
- according to the nature of the surveillance with respect to the awareness of the person being surveilled.

This book is generally organized, chapter by chapter, according to the *physical nature* of the technology. Within each chapter, the more generic *data aspects* are described and cross-referenced to other chapters when appropriate, since there is overlap. The nature of the surveillance *with respect to the awareness of the surveillee(s)*, however, warrants further introduction as it is not covered in other chapters, but is important in the broader contexts of law and individual freedoms.

From the perspective of the dynamics of surveillance, there are five general categories of surveillance activities:

implied surveillance *Surveillance that is mimicked or faked* with a variety of devices, including nonfunctioning cameras or empty camera housings and/or stickers claiming that the area is monitored, when in fact it isn't. Implied surveillance is generally used as a low-cost deterrent to theft and vandalism.

overt surveillance *Surveillance in which the surveillee has been informed of the nature and scope of the surveillance or in which the surveillance devices are clearly labeled and displayed.* Thus, an employee badge that constantly tracks workplace movement (assuming the employee has been fully informed of its role) or video camera surveillance in a department store, in which surveillees clearly see themselves on a monitor as they enter an area, are examples of overt surveillance.

An example of overt surveillance in a retail store. 1) The sign in the window alerts customers of the video security system, 2) cameras are clearly visible throughout the store, and 3) the video surveillance images are displayed in plain view near the cash register. (Note that there are still issues of storage and subsequent use of the videos to consider.) [Classic Concepts photos copyright 2000, used with permission.]

Overt surveillance is most often found in workplace or retail security systems in which employees or customers are informed that they are being watched. However, it is not sufficient to assume a person understands the function of a surveillance device because it is in plain sight. A wall-mounted camera that is visible to occupants of a room technically is *not* overt surveillance unless the surveillee explicitly knows a) that the camera is operating and b) that it is focused on the surveillee. If *both* these conditions are not met, then a device in plain sight is categorized as *implied surveillance*, if it is not functioning, or *clandestine surveillance,* if it is.

covert surveillance *Hidden surveillance. Surveillance in which the surveillance is not intended to be known to the surveillee.* Covert wire taps, hidden cameras, cell phone intercepts, and unauthorized snooping in drawers or correspondence are examples of covert surveillance. Most covert surveillance is unlawful and requires special permission, a warrant, or other 'just cause' for its execution. Covert surveillance is commonly used in law enforcement, espionage, and unlawful activities. The jargon term 'black' is sometimes used to refer to covert operations, the deeper the black, the more secret it is. Some aspects of covert surveillance in retailing or the workplace are currently lawful, but are being challenged by privacy advocates who feel that prior notice of surveillance activities and clear identification of surveillance devices should be mandated by law. This may in fact happen in the next three or four years.

clandestine surveillance *Surveillance in which the surveilling system or its functioning is in the open but is not obvious to the surveillee.* The functions of two-way surveillance mirrors above cash registers and entrance cameras encased inside aesthetically streamlined domes are obvious to professionals and the personnel who requisitioned and installed them, but they are not obvious to surveillees. The author recently queried customers outside a financial institution at which a dome camera had been installed overlooking the sidewalk and street. In every case the person queried was surprised to be told that the black and silver dome was a security camera. Because all the cameras inside the building were in plain site (not covered with domes), the individuals had wrongly assumed that the dome outside was a new light fixture (which it resembled). This type of clandestine surveillance, in which the device is not overtly hidden but is nevertheless inconspicuous, due to its placement, size, coloration, or design, is typical of surveillance in many public areas including shopping malls, banks, and educational institutions.

This dome-covered video camera is aimed at an outdoor ATM machine and a public sidewalk outside a financial institution, but it does not qualify as overt surveillance because the public doesn't know where it's aimed or when it is active. In fact, several people outside the building mistook the surveillance camera for a light fixture, which it resembles. [Classic Concepts photos ©2000, used with permission.]

At the present time, intrusions on personal privacy from clandestine surveillance devices are significant. Many of them are aimed at public squares, sidewalks, park-ing lots, and meeting places. Many clandestine cameras are configured to broadcast live or almost-live over the Internet where anyone with a computer can capture and store the images without the knowledge or consent of the surveillees. Many surveillance systems which are claimed by their operators to be overt surveillance devices are actually *clandestine* surveillance devices. This has important ramifications for corporate and legislative policy-makers.

extraliminal surveillance *Surveillance outside the consciousness of the person/entity being surveilled.* Extraliminal means 'beyond consciousness.' Using video cameras or vital-sign devices to monitor an infant, a comatose hospital patient, or a mentally incompetent person who might be at risk of wandering or inflicting injury (on self or others) are examples of extraliminal surveillance. Extraliminal surveillance techniques, including tracking devices, may also be used for wildlife observation. Extraliminal surveillance is usually carried out to ensure the safety of the individual, or other people with whom the individual is interacting. It is primarily used in situations where informed consent is not possible.

It might be argued that anthropological observation of living primitive cultures or high-resolution satellite images of third-world cultures where technology is rare or nonexistent are forms of extraliminal surveillance, but since the surveillees are intellectually capable of understanding the concepts, given more information, surveillance of low-technology cultures are actually forms of covert or clandestine surveillance rather than extraliminal surveillance.

2.d. Categories of Surveillance Devices

Due to the limitations of space, this text can't describe every surveillance technology in existence, but it does include a good selection of representative examples of the prevalent technologies. In overview, this text includes the following general sections:

1. *Surveillance Technologies*

   This section provides a general overview of surveillance history, devices, and intelligence-gathering. This book is modular in design and the chapters can be read out of order, but it is probably helpful to read or scan the introductory section first.

2. *Acoustic Surveillance* - Audio, Infra/Ultrasound, Sonar

   Acoustic surveillance, an extensive field, has been divided into three chapters in this book. The first is *audio* technologies, those within the range of human hearing; the second is *infrasonic and ultrasonic* technologies, those which are primarily outside the range of human hearing; and the third is a specialized chapter for *sonar* because it is extensively used in marine surveillance and includes frequency ranges both inside and outside human hearing ranges.

3. *Electromagnetic Surveillance* - Radio, Infrared, Visible, Ultraviolet, X-Ray

   The technologies that are based primarily on specific electromagnetic phenomena have been grouped together in this section. Infared, Visible, and Ultraviolet have been further subgrouped as Light Surveillance technologies (some people call them optical surveillance technologies, though they are not limited to optical devices).

   Technologies that are not specifically electromagnetic but rely heavily on electromagnetic phenomena are also grouped into this section, including Radar and Aerial Surveillance which rely heavily on radio and light phenomena. It is helpful to cross-reference the Visual Surveillance and Aerial Surveillance chapters.

4. *Biochemical Surveillance* - Chemical/Biological, Biometrics, Animals, Genetics

   Chemical/Biological surveillance is a huge and highly technical field that takes place largely in scientific laboratories, so it is covered mainly in its introductory and law enforcement aspects in this book. Genetic surveillance, an important subset of chemical/biological surveillance, and biometric surveillance, which is biochemical in origin, are discussed in separate chapters.

   Animal surveillance is an important field, but it is not as prevalent as the other technologies and is given a correspondingly smaller amount of space in this text. It should be noted that it is a growing area of surveillance and dogs and dolphins are used in many types of land and marine surveillance activities.

5. *Miscellaneous Surveillance* - Magnetic, Cryptologic, Computer

   Magnetic surveillance is included in the miscellaneous section since it is not technically classed as part of the electromagnetic spectrum. Some technologies are more difficult to categorize because they are not primarily based on any one particular physical phenomenon, including *cryptology* and *computer surveillance* (the basic user aspects of computer surveillance are introduced).

2.e. Categories of Intelligence

This book is not about intelligence, per se, but rather about devices that can aid in intelligence-gathering specifically related to surveillance. However, it is helpful to have some idea of the general categories of intelligence, as it provides a framework for how particular classes of devices might be used. As described earlier, intelligence is information which has been processed and assessed within a given context. That context may require specific types of surveillance devices for effective information-gathering. And, as also stated, it often is not known in advance what information may later become part of a body of intelligence.

A few general categories of intelligence that are relevant will be described here. (Note that these are generic categories and not the specific definitions used by the U.S. government. U.S. government definitions include stipulations about who might be the subject of the intelligence that may not apply in the general sense of the category.) The term *agent* as used in these descriptions means any agent (human, electronic, or otherwise) which is involved in gathering the information.

Note, some of the following INTs (forms of INTelligence), are dual-meaning in that they can refer to the technology being used to gather information, or information being gathered on the technology. For example, electronics intelligence can mean the use of electronics to gather various types of data for intelligence, or the use of various types of intelligence methods to gather information on electronics. For dual-meaning INTs, the meaning in practical use can usually be discerned from the context in which it is used.

biological/chemical intelligence (BICHEMINT) Intelligence derived from or by biological and/or chemical sources, such as biometrics, chemical stains, blood or saliva, hair, urine, gases, pharmaceuticals, etc.

communications intelligence (COMINT) Intelligence derived from communications that are intercepted or derived by an agent *other than* the expected or intended recipient or which are not known by the sender to be of significance if overheard or intercepted by the COMINT agent. Oral and written communications, whether traditional or electronic, are the most common targets of surveillance for COMINT, but it may broadly include letters, radio transmissions, email, phone conversations, face-to-face communications, semaphore (flags or arms), sign language, etc.

In practice, the original data that form a body of COMINT may or may not reach the intended recipient. Data may be intercepted, or may reach the recipient at a later date than intended, or be intercepted, changed, and then forwarded on. However, the definition of COMINT does not include the process of relaying delayed or changed information, but rather focuses on intelligence that can be derived from the detection, location, processing, decryption, translation, or interpretation of the information in a social, economic, defense, or other context.

computer intelligence (COMPINT) Intelligence derived from or by computer networks, programs, algorithms, and data sources. This is an important and growing source of information contributing to intelligence.

corporate intelligence (CORPINT) Generically used to indicate general business intelligence, not just corporations, but a high proportion of CORPINT is corporate-competitor intelligence. General information on economic trends and imports and exports form part of CORPINT within ECONINT.

economic intelligence (ECONINT) Intelligence related to business services, resource exploration, allocation, or exploitation with the potential for global or local economic impact.

electronics intelligence (ELINT) Intelligence derived from electronics-related noncommunications (usually through electromagnetic, acoustic, or magnetic sources that are electronically generated or received) that are intercepted or derived by an agent *other than* the expected or intended recipient or which are not known by the sender to be of significance if overheard or intercepted by the ELINT agent. Radar signals, sonar pings, and magnetic disturbances are examples of ELINT information sources.

environmental/ecological intelligence (ECOINT) Intelligence derived from observations of environmental patterns and characteristics, weather, pollution indicators, and ecological trends. Weather intelligence (WEATHINT) is a subset of ECOINT, as is wildlife intelligence (WILDINT).

foreign instrumentation signals intelligence (FISINT) Mostly a military INT, this category isn't seen too often. It is a type of foreign TECHINT related to instrumentation within the broader category of SIGINT.

human intelligence (HUMINT) Human-derived intelligence about activities, strategies, customs, etc. This type of information is usually deliberately gathered by spies, agents, and operatives.

image intelligence (IMAGINT) Video or photographic intelligence, which forms a large proportion of intelligence-gathering. IMAGINT is varied and includes intelligence derived from remote-sensing technologies, aerial imagery, computer imagery, video footage, traditional photographs, infrared images, and more.

measurement and signature intelligence (MASINT) The determination of characteristics related to identity which might include size, shape, volume, velocity, color, electrical characteristics, or composition. Unique measurements can be used to determine 'signatures' for a fixed or moving object, such as an infrared or radar signature.

open-source intelligence (OPENINT) Openly published or otherwise distributed, freely available sources of information such as books, journals, signs, lectures, ads, phone directories, genealogies, etc. A large proportion of intelligence is acquired from OPENINT sources and these resources are increasing through the global Internet.

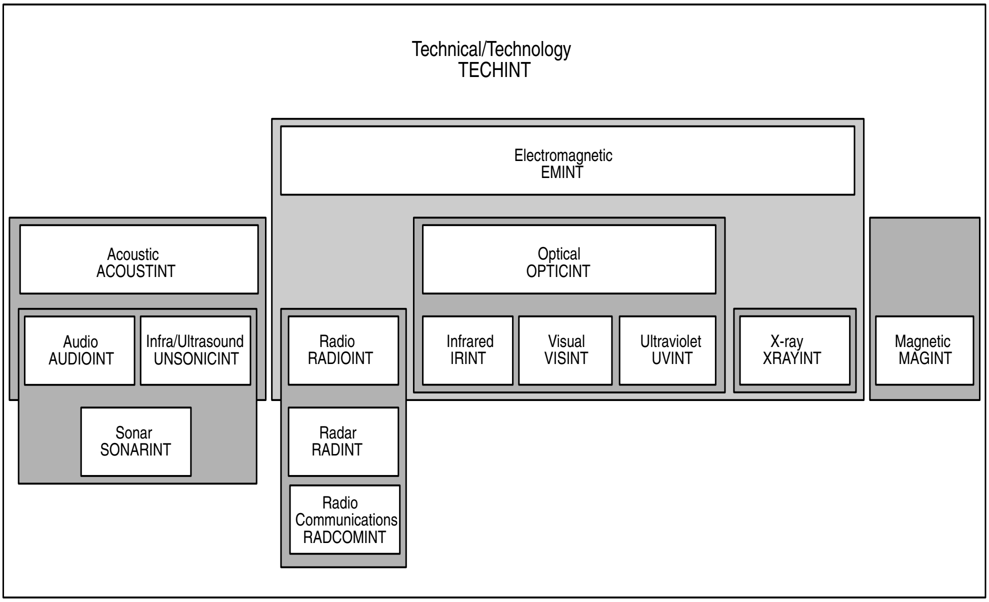
Sometimes also called OSCINT, OSINT, or OPSINT, but the author recommends the less ambiguous OPENINT.

signals intelligence (SIGINT) Signals intelligence is commonly treated in the military as a superset that includes COMINT, ELINT, FISINT, and TELINT.

technical intelligence (TECHINT) Intelligence derived from technical sources, usually machines, electronics, and instruments as opposed to intelligence derived from human sources. Most of the surveillance technologies described in this volume relate to TECHINT.

telemetry intelligence (TELINT) Intelligence derived from telemetric sources, that is, instruments that determine and calculate quantities or distances. Telemetric data are often used to orient and control vehicles, projectiles, and satellites. Since telemetric data may be electronically generated or received, in many cases the data can be considered a subset of electronics intelligence (ELINT) and also of technical intelligence (TECHINT).

The above alphabetical list represents a selection of some of the common and older INT designations. Due to a traditional preference for two-syllable INT names, there is increasing ambiguity in naming schemes as technology grows and new INTs are added. We can continue the two-syllable tradition and tolerate the ambiguity or use three-syllable INTs where appropriate. The trend appears to be toward using three-syllable INTs to clarify the meaning.



One Scheme for Organizing and Naming Common Technical Intelligence Categories

Many organizations have developed the definitions and jurisdictions of their INTs over a period of decades and they have become intrinsically linked to many carefully developed policies and departments. For this reason, it's difficult to sort out and change existing INT designations. However, for newer technologies, it may be useful to put them in some sort of logical order related to their physical properties. One possible scheme that could be used to organize the most common TECHINT-related surveillance technologies is shown in the chart on the preceding page.

Emphasis

The most widely used surveillance technologies are chemical, acoustic (particularly audio, radio, and sonar) and visual. Aerial surveillance consists mainly of visual and radio technologies and is covered in a separate chapter due to its growing importance. Radar is also widely used, and infrared is steadily increasing in both aerial- and ground-based applications. This text concentrates more heavily on the more prevalent technologies, but does not overlook some less-used but valuable fields, including magnetic, animal, and cryptologic surveillance. Biometric surveillance is not yet a large field, but it has a potential to grow and genetic surveillance may be the most significant technology of all. The technology that you ultimately choose depends on what you need to know, what you're allowed to do, and the type of environment in which the devices will be used.

3. Context

Surveillance is a very context-sensitive field; the technology may be incidental or highly important. A homeowner checking on a housekeeper who is suspected of stealing might use a simple pinhole camera hidden in a smoke detector to confirm or deny the suspicion. A private detective observing a client's spouse in a crowded shopping mall, where there is usually little need for elaborate plans, disguises, or expensive technologies, can usually accomplish the task with discretion and an unobtrusive camera.

Some types of surveillance, however, require planning and highly sophisticated technologies. Law enforcement agencies use a moderate amount of technology in stakeouts and investigations, including chemical dyes and powders, infrared sensors, bullet-analysis techniques, and sometimes helicopters. However, if a news correspondent or foreign agent is trying to gather information on potential hostilities or human rights abuses in foreign territory, a great deal more preparation and technology may be used. Clothing, cosmetics, contact lenses, language classes, wireless recorders, aerial photographs of the region, maps, telegraph transmissions, satellite-modem-equipped notebook computers, accomplices, and a boat tucked away under a dock in a harbor may all assist in achieving the desired ends.

When aerial images were expensive and limited in resolution ($4,000 per image a few years ago), they were primarily marketed to researchers, large corporations, and military analysts. As mentioned in the introduction, now that high resolution satellite images can be purchased for under $25 per square mile, a dramatic shift is occurring in the applications for which these images are used and in the scope of the people who use them.

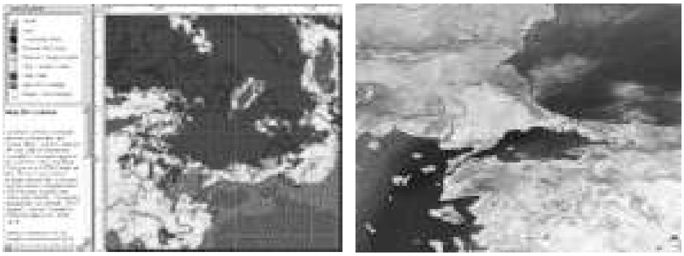
The human nervous system is still the most important surveillance 'technology.' All the sophisticated inventions in the world are worthless without strategies, data analysis, and interpretation of the results. Whether you are interested in personal, corporate, or military surveillance, it's a good idea to remember that the technological developments and devices introduced in this text are only effective if used in conjunction with careful planning and implementation. As they say in the computer programming industry, *garbage in, garbage out*. One way to ensure that the information gathered through surveillance isn't *garbage* or irrelevant or erroneous data is to carefully select the means and deployment of appropriate technologies in the first place.

Planning is particularly important when making the best use of limited resources in armed conflicts where lives may be at stake. Thus, law enforcement agencies and the various armed services make regular use of strategies and intelligence gathered with surveillance devices in planning their training exercises and operations.

Left: A Wing Intelligence Officer with the U.S. Air Force, Capt. Muellner, updates a map of Entebbe in 1994. Middle: A member of the TAW target intelligence branch, TSgt. Olague, transfers drop-zone map coordinates to a satellite photograph during an exercise in 1991. Right: TSgt. Hawman from the 1st SOS Intelligence checks a map of southern Thailand before a 1996 preflight briefing in Japan. [U.S. DoD news photos by Andy Dunaway, H. H. Deffner, and Val Gempis, released.]

Left: An Air Force intelligence and targeting chief in the U.S. Air Force, Capt. Muellner, indicates positioning on a map of Korea in 1993. Middle: An illustrator with a U.S. Marines Intelligence Company prepares a map for a 1996 orders brief in North Carolina. Right: A Navy intelligence specialist aboard an aircraft carrier in the Red Sea evaluates aerial photographs to assess 1991 battle damage. [U.S. DoD news photos by Michael Haggerty, Moore,and R. L. Kulger, Jr., released.]

3.a. Scientific Inquiry



Left: A sample fish-finding map from the OrbView-2 satellite. Images like this, which are of use to scientists, resource managers, and commercial harvesters are now available from commercial satellite image vendors at reasonable rates. Right: An OrbView satellite image of Turkey taken in August 1999 after a major earthquake. [News photos ©2000 Orbimage, www.orbimage.com, used as per copyright instructions.]

Surveillance technologies are used in virtually every field of scientific inquiry. Archaeologists, anthropologists, geologists, meteorologists, marine biologists, zoologists, astronomers, geneticists, forensic pathologists, and sociologists all use surveillance technologies, in one way or another, to monitor trends, conduct experiments, and gather scientific data.

Aerial surveillance technologies, especially those related to imagery, are especially useful in scientific inquiry including archeological digs, astronomy, and ecosystems monitoring (weather, pollution, climate change).

This volume includes a number of explanations and examples of some of the myriad ways in which surveillance technologies are used in scientific research.

3.b. Government Applications

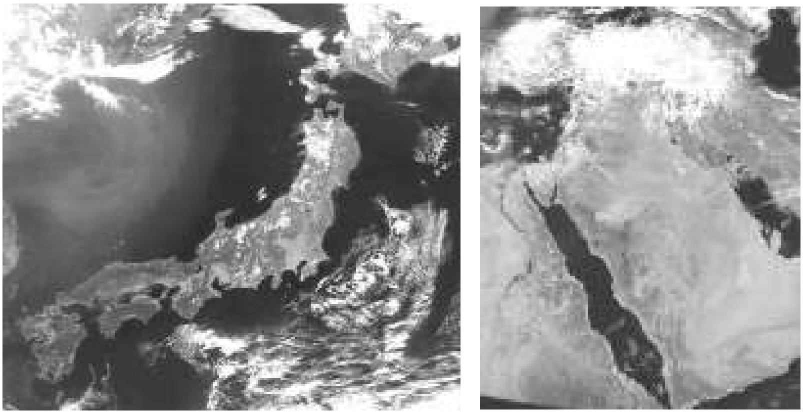
Surveillance technologies are extremely useful to many types of government and commercial activities, including national defense, local law enforcement, disaster assessment and relief, search and rescue, community planning, resource exploration, wildlife monitoring, property tax assessment, border patrol, camouflage detection, treaty negotiation and verification.

Left: Sgt. Lalita Mathais helps tourists into a Blackhawk helicopter after they were rescued near an avalanche in the Austrian Alps. Right: After severe flooding in Honduras following Hurricane Mitch, U.S. Army personnel from the 228th Aviation Regiment locate and airlift a child who had been trapped on top of a house. [U.S. Army news photos by Troy Darr and Terrence Hayes, released.]

U.S. Army hoist exercises provide training for airlift rescues. Here Ssg. Rosales of the 214th Medical Detachment hooks up a rescue basket to the cable and the ‘survivor’ is winched up into the helicopter. [U.S. Army news photos, released.]

Rescue operations during natural disasters are often complicated by sustained bad weather and poor visibility. Locating victims who are stranded on rooftops, in trees, in vehicles, and under debris can be a significant surveillance challenge.

Left: Intelligence briefing during peacekeeping and humanitarian operations training. Austrian and Canadian participants are shown in this Partnership for Peace exercise in North Carolina, which operates according to NATO IFOR standards. Right: A U.S. Marine, Capt. Nevshemal, gives an intelligence brief to Hungarian and Central Asian platoons at Camp Lejeune, North Carolina. [U.S. DoD 1996 Released Photos by LCpl. R. L. Kugler, Jr. and LCpl. C. E. Rolfes, released.]



Left: Satellite images of the islands of Japan, 9 May 1998. Right: Egypt, Saudi Arabia, and the Middle East, 3 April 1998. Government departments are making greater use of commercial image sources. [News photos ©1998 OrbImage, www.orbimage.com, as per copyright.]

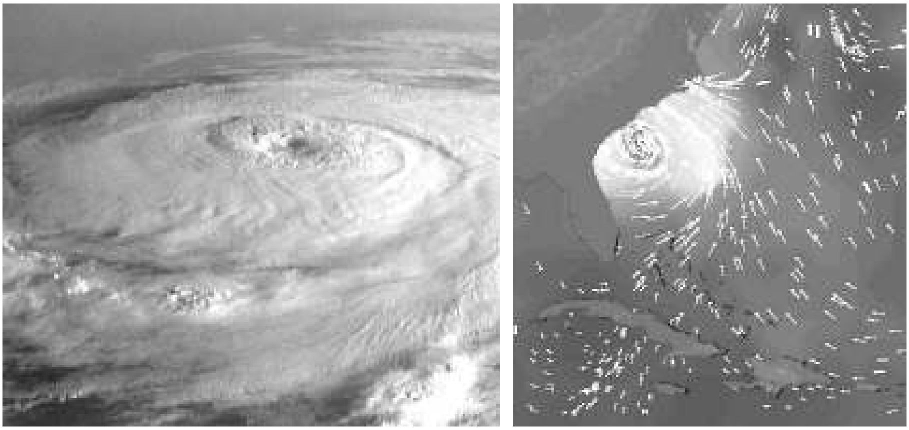
3.c. Commercial, Agricultural, and Government Applications

There are thousands of commercial applications for surveillance technologies that are unrelated to corporate spying, and thousands of devices specifically designed for corporate spying. Public safety in subway systems and protection of public artifacts and artworks in museums can be aided by surveillance devices. Seemingly innocuous technologies sometimes provide important financial or competitive information. The U.S. agricultural industry has gathered information on global agricultural production and mineral exploration in order to assess international markets and gather intelligence before speculating:

> “The first comprehensive inventory was called the Large Area Crop Inventory Experiment (LACIE) and was undertaken from 1974 to 1977 (MacDonald 1979). Wheat production of the USSR, Latin America, China, Australia, and India was estimated by multiplying the crop area derived from the Landsat sensor data by the estimated crop yield derived from meteorological satellite sensor data [Curran 1980a].”
>
> [Paul J. Curran, “Principles of Remote Sensing,” Longman Group, Ltd., 1985.]

Insurance adjustments, property value and damage assessment, marketing and promotion pictures, contractor planning, city planning, investigative journalism, weathercasting, architectural planning, ranching and livestock monitoring, surveying, fish finding, crop yield assessment, forestry and fire-fighting, and livestock management are all areas in which surveillance technologies aid in production and marketing.

Detailed satellite and aircraft-derived weather images of weather patterns, especially impending storms, are of commercial interest to newscasters, boaters, commercial fishers, firefighters, production companies, insurance adjusters, and homeowners and businesses in the path of dangerous storms.



Left: This image of Hurricane Elana over the Gulf of Mexico in September 1985 clearly shows the spiral formation and elevated cyclonic cloud berm. Right: This SeaWinds radar data chart of Hurricane Floyd, one of the most destructive hurricanes of the 20th century, was imaged in September 1999. Ocean wind speeds are indicated by adding colored arrows. SeaWinds is an orbiting imaging system managed by the Jet Propulsion Laboratories (JPL). [NASA/JSC and NASA/JPL news photos, released.]

3.d. Nonprofit and Public Welfare Applications

Surveillance technologies are used by public-concern watchdog agencies to monitor government and corporate activities, pollution, resources, and price policies. In turn, governments have used surveillance technologies to monitor radical militant groups and others suspected of terrorist intentions. Nonprofit applications include the monitoring of environments, crops, wildlife, pollution, international unrest, corporate management, manufacturing of consumer goods, and military activities.

3.e. Personal Applications

Since the mid-1990s, surveillance technologies, particularly motion detectors, video cameras, and computer-related devices, have become consumer items. Thus, there is a need to educate the public in terms of the forms and functions of the various devices and ways in which they could and should be used and the implications for personal freedoms and privacy. This book seeks to clarify some of the issues related to the proliferation of these devices in homes, playgrounds, private hospitals, and public spaces so that the public has a better grasp of the potential and future importance of surveillance tools.

4. Origins and Evolution

Each chapter in this book has a section in which the history related to that particular technology is described and illustrated. These historical notes help to put the technological development of a particular device or class of devices into its context in terms of mechanical/ electronic inventions and the factors that motivated people to invent them in the first place.

For the most part, the historical sections in each chapter stand on their own, except that there is a fair amount of overlap between the development of radio devices and audio listening devices which are covered separately in the Audio Surveillance and the Radio Surveillance chapters, so it is worthwhile to cross-reference these. There is also come overlap between the infrared and aerial surveillance chapters because infrared has become such an important aspect of aerial surveillance. These, too, should be cross-referenced. They don't necessarily have to be read in sequential order, however.

Important milestones and events of a general nature regarding surveillance and the organizations and policies that have governed their use are described here.

4.a. Introduction

As surprising as it may seem, most of the inventions that have evolved into current surveillance technologies originated thousands of years ago, including optics, deciphering, and audio eavesdropping. However, the sophisticated development and practical application of most of these devices originates around the time of the Renaissance. This was an era when tunnels, secret writings, and political intrigue were very prevalent.

Sir Francis, the Earl of Walsingham (c1531-1590) was appointed in 1573 as Queen Elizabeth I's (1533-1603) Joint Secretary of State. He is perhaps best known for having intercepted secret communications from Mary Queen of Scots who was imprisoned for almost two decades. Walsingham was a dedicated and meticulous administrator, who established a permanent peacetime intelligence service that set the precedent for the British secret services.

Enmity between England and France erupted periodically for hundreds of years, with many surveillance devices being adapted and developed as tools of warfare. In the 1600s, Armand-Jean du Plessis, Cardinal, Duc de Richelieu (1585-1642) used extensive intelligence services to protect his position and influence the unity and future of France. He is quoted as saying "Secrecy is the first essential in affairs of the State." At about the same time, in England, various writers and inventors mention the development of submarine devices for surreptitiously approaching surface vessels and "blowing them up."

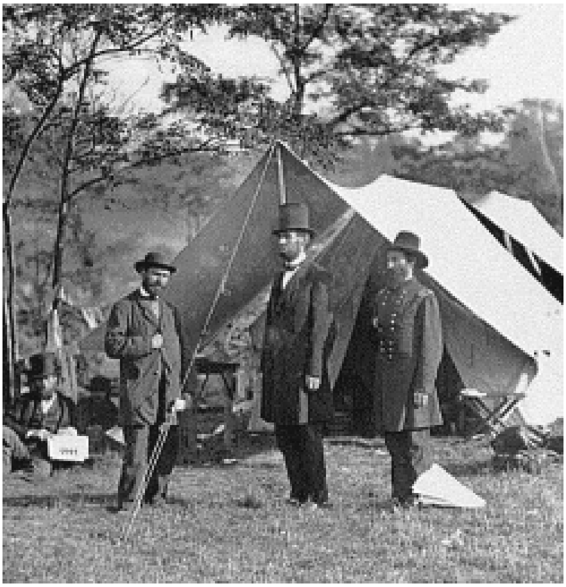
Rivalries between the English and French continued even across the Atlantic in the pioneer wilderness of North America. The War of the Spanish Succession erupted in 1702 followed by various outbreaks, increased surveillance, and tight security watches to prevent smuggling. In the mid-1770s, George Washington made regular use of coded messages, foreign agents, and other surveillance resources to further the American Revolution. In July 1789, Washington and the First Congress established the *U.S. Customs* service and the ports of entry it was entrusted to surveil.

4.b. Establishing Surveillance-Related Agencies

As the population migrated westward in the early 1800s, crime and gangsterism increased. This resulted in a higher emphasis on law enforcement and surveillance, especially as farmers and settlers, including women and children, began to supersede the original trappers. The populace became increasingly concerned about law and order and the safety of families.

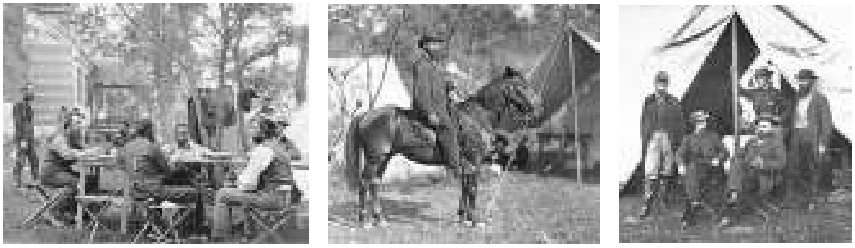
Smuggling wasn't the only problem in early America. A variety of regional currencies and a general wild west mentality resulted in many incidences of counterfeiting and train robbing. In 1806, the *Enforcement of Counterfeiting Prevention Act* was established to curb some of these problems. The Act provided U.S. Marshals and District Attorneys with a tool to officially deal with counterfeiting, a responsibility that was later transferred to the Secretary of the Treasury.

In 1846, Allan Pinkerton (1819-1884), a barrel-maker from Scotland, exposed a gang of counterfeiters, made history, and became the Deputy Sheriff. This marked the origins of one of the oldest and most prominent detective agencies in history. Pinkerton became Chicago's first official city detective and then founded Pinkerton's National Detective Agency in 1850. Over the decades that followed, his business and his reputation grew and he and his agents used surveillance techniques to investigate train robberies, embezzlement, assassination plans, spies, and much more. Part of the reason for his success was that, as a private establishment, he was able to pursue criminals across state lines. Abraham Lincoln appointed him as his first secret service agent in 1861. During the Civil War in America, Pinkerton organized a secret service within the U.S. Army.

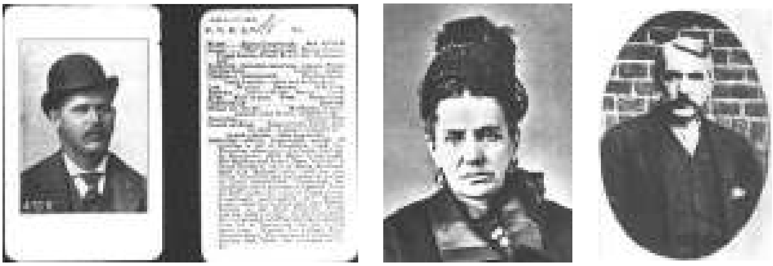


Left: Allan Pinkerton, who founded Pinkerton's Detective Agency in 1850. Right: Allan Pinkerton (also known at the time as E. J. Allen) in the field with Abraham Lincoln and Major General John A. McClernand. Detractors later claimed the 'plots' against Lincoln were fabricated to 'make work,' leading Lincoln to establish his own secret service. [Left photo courtesy of Pinkerton Global Intelligence; right photo Library of Congress, by Alexander Gardner, October 1862, copyright expired on both images by date.]

General George McClellan used Pinkerton to gather intelligence behind the lines of the Confederate forces during the War. Pinkerton provided information on defenses, supplies, and transportation routes; he engaged in counterintelligence as well. After McClellan was demoted, Pinkerton went back to private detective work.

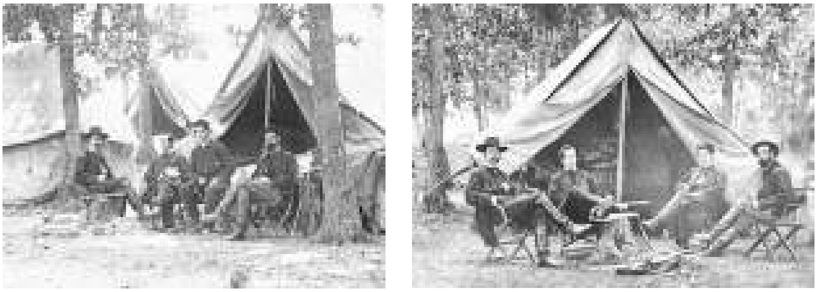


Left: Members of the Secret Service at Foller's House, Va. during the Peninsular Campaign. Middle: Allan Pinkerton known as "E. J. Allen" on horseback during his time in the Secret Service at the main eastern theater of the Battle of Antietam. Right: George Banks, William Moore, Allan Pinkerton, John Babcock, and Augustus Littlefield. [Library of Congress May and September 1862 photos by George Barnard, James Gibson, and Alexander Gardner, copyrights expired by date.]



Pinkerton's Detective Agency established one of the first extensive collections of 'mug shots,' pictures of criminals' faces that were used to identify and apprehend them. This tradition has continued to this day, with searchable computer databases gradually supplementing the print collections. From left to right, these are mug shots of famous criminals like the Sundance Kid, Lena Kleinschmidt, and Alan Worth. [Photos mid-1800s, courtesy of Pinkerton Global Intelligence, copyrights expired by date.]

The busy Pinkerton detectives began collecting criminals' pictures from posters and newspaper clippings, a practice that was eventually adopted by many local enforcement agencies. By the 1870s, Pinkerton's had developed the most extensive collection of 'mug shots' in America. Pinkerton's also became known for its logo, a picture of an eye, under which is the motto "We never sleep." This may have popularized the colloquial phrase 'private eye.'

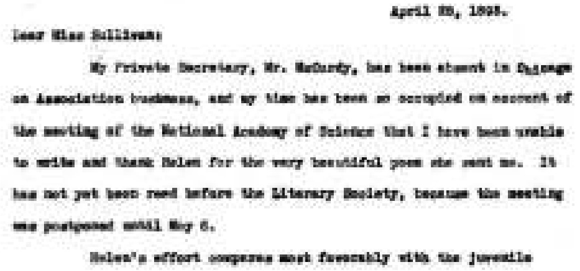


During 1863, officers of the *Bureau of Military Information* Secret Service were stationed in Bealeton, Virginia (left) and at Brandy Station in Feb. 1864 (right), which was set up at the time George Sharpe was chief of the Bureau. Numerous books and pamphlets are housed in the tent; which are probably reference materials, including maps. [Library of Congress Civil War collection photos, copyrights expired by date.]

In 1863, the *National Currency Act* was enacted to create a national currency and to provide tougher regulations against counterfeiting operations.

Scientific Input to Government

Scientists and inventors had been somewhat frustrated by the slow comprehension and adaptation of new inventions by Union leaders and discussed a number of review panels and commissions to try to expedite the process and provide more input from experts. Rear Admiral Charles Henry Davis, the great inventor Joseph Henry, and Alexander Dallas Bache suggested a commission or scientific organization, but no clear consensus was reached at first. Bache had wanted to institute a national science advisory body to aid the government in formulating policy and funding worthy projects. Finally, Joseph Henry effected the establishment of the Navy's *Permanent Commission* in 1863, with himself, Davis, and Bache as members. John G. Barnard was later appointed to represent the interests of the Army.



April [illegible], 1895.

Dear Miss Sullivan:

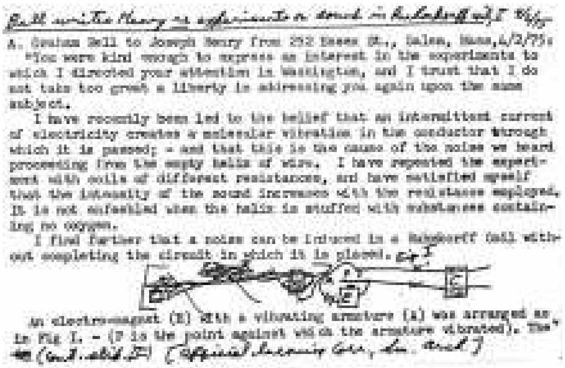
My Private Secretary, Mr. McCurdy, has been absent in Chicago on Association business, and my time has been so occupied on account of the meeting of the National Academy of Science that I have been unable to write and thank Helen for the very beautiful poem she sent me. It has not yet been read before the Literary Society, because the meeting was postponed until May 6.

Helen's effort compares most favorably with the juvenile

Left: The "Academy of National Science" as it looked at the turn of the century in Philadelphia, Pennsylvania not long after it was first established. A *Permanent Commission* of professionals had been founded in 1863 to provide expert advice to politicians regarding scientific inventions that could be used to further national interests. The founders hoped this effort would help expedite the critical review and recommendations of new technologies. This Commission led to the establishment of the Academy which still exists today. Right: A copy of an 1895 letter from Alexander Graham Bell to Anna Sullivan (Helen Keller's teacher) mentioning his attendance at a meeting of the National Academy of Science. He was one of many distinguished participants in the organization. [Library of Congress Detroit Publishing Company Collection and the Bell Family Papers collection, copyrights expired by date.]

By 1864, the Permanent Commission had created almost 200 reports, confirming its viability as an advisory body, thus paving the way for establishment of the National Academy of Sciences (NAS). Bache became the Academy's first President but due to illness leading to his death, Joseph Henry provided a substantial proportion of the leadership in its early days.

During the 1840s, Lt. Charles H. Davis (1807-1877) was involved with Alexander Bache on the *Coast Survey* and Davis authored the "Coast Survey of the United States" in 1849. It was only one of many surveillance- and technology-related projects in which he participated over the next three decades. Davis was promoted to Captain and later to Rear Admiral. In the 1860s, he was Chairman of the Western Navy Yard Commission and an advisor to President Lincoln. Under his direction, his assistants conducted numerous reconnaissance surveys, including the area around Vicksburg. That was also the period during which he aided Joseph Henry and Alexander Bache in establishing the National Academy of Sciences. In the 1870s, he headed up the U.S. Naval Observatory. From 1870 to 1873, he was Shipyard Commander at Norfolk Naval Shipyard with four hulls honoring his name.



Bell writes Henry re experiments on sound in Ruhmkorff coil [illegible]

A. Graham Bell to Joseph Henry from 292 Essex St., Salem, Mass, 4/2/75:
"You were kind enough to express an interest in the experiments to which I directed your attention in Washington, and I trust that I do not take too great a liberty in addressing you again upon the same subject.

I have recently been led to the belief that an intermittent current of electricity creates a molecular vibration in the conductor through which it is passed; - and that this is the cause of the noise we heard proceeding from the empty helix of wire. I have repeated the experiment with coils of different resistances, and have satisfied myself that the intensity of the sound increases with the resistance employed. It is not enfeebled when the helix is stuffed with substances containing no oxygen.

I find further that a noise can be induced in a Ruhmkorff Coil without completing the circuit in which it is placed. Fig I

An electromagnet (E) with a vibrating armature (A) was arranged as in Fig I. - (P is the point against which the armature vibrated). The"
(cont. [illegible]) [Official Inventory [illegible]]

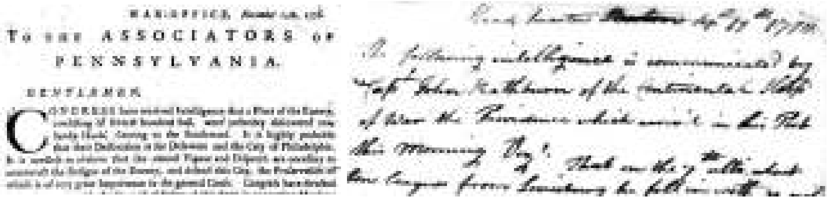
Left: A copy of correspondence about electromagnetism from Alexander Graham Bell to Joseph Henry in 1875. Joseph Henry also studied electromagnetism and provided encouragement and counsel to many prominent inventors, including Charles Wheatstone and Samuel Morse. He thus aided and influenced the original inventors of both telegraph and telephone technologies. Along with Charles H. Davis (right), Henry and Bache helped establish the National Academy of Sciences based on the 'Permanent Commission.' Right: Rear Admiral Charles H. Davis (1845-1921), painted in the early 1900s. [Library of Congress Bell Family Papers Collection and painting by F. P. Vinton, copyrights expired by date.]

Intelligence-Related Departments and Forensics

Within the Department of the U.S. Treasury, the Secret Service Division (SSD) operated from 1865 to 1879. One of their main concerns was the detection and apprehension of counterfeit rings, along with the investigation of forgery and securities violations.

The position of the U.S. Attorney General was first created in 1789. In 1870, the Attorney General was appointed the Director of the newly formed *Department of Justice* (DoJ). The Department of Justice is one of the oldest establishments to handle federal investigations and continues in this role today.

The armed forces were also establishing official intelligence departments at this time, with the *Office of Naval Intelligence* being created within the Bureau of Navigation in 1882.



WAR-OFFICE, [illegible] 1776.

TO THE ASSOCIATORS OF PENNSYLVANIA.

GENTLEMEN,

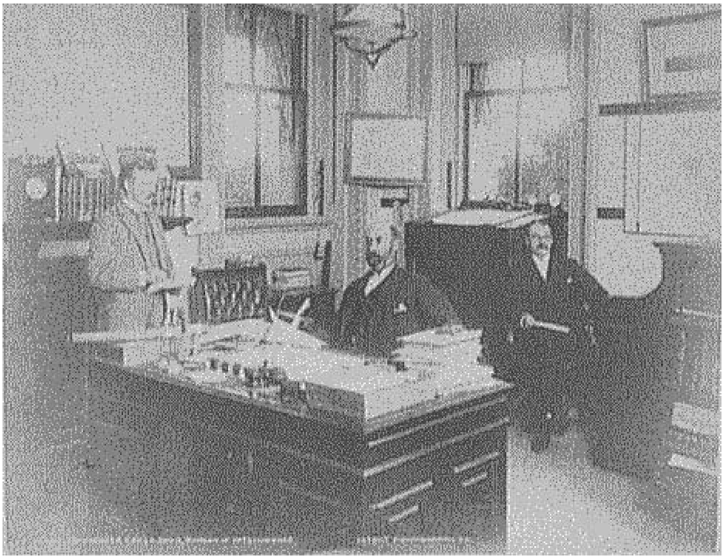
CONGRESS have received Intelligence that a Fleet of the Enemy, consisting of several hundred Sail, were yesterday discovered [illegible] Sandy Hook, steering to the Southward. It is highly probable that their Destination is the Delaware and the City of Philadelphia. It is needless to observe that the utmost Vigour and Dispatch are necessary to counteract the Designs of the Enemy, and defend this City, the Preservation of which is of very great Importance to the general Cause. Congress have directed

Camp [illegible] Aug 13th 1778

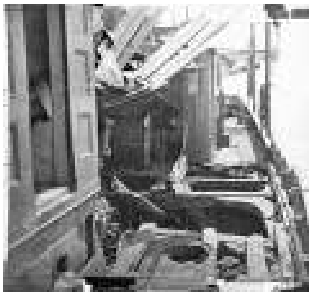
The following intelligence is communicated by Capt John Rathburn of the Continental Sloop of War the Providence which arrived in this Port this Morning Viz': That on the 7th ulto about [illegible] leagues from Louisbourg he fell in with [illegible]

Left: In 1776, Congress received "Intelligence that a Fleet of the Enemy, consisting of several hundred Sail were yesterday discovered in Sandy Hook." Right: In 1778, George Washington indicated in his correspondence that he had received intelligence from John Trathburn of the Continental Sloop of War, the Providence. These documents show how naval intelligence has an old tradition, leading up to the official establishment of an Office of Naval Intelligence in 1882. [Library of Congress, copyrights expired by date.]

In 1887, the Office of Naval Intelligence (ONI) directed naval forces to create a photographic record of coastal installations. Matthew Brady and Alexander Gardner were two important Civil War photographers who demonstrated the value of photo reconnaissance and the documentation of war (see photos on following page).



This photo is interesting because it provides a small surveillance challenge for readers who like solving historic puzzles. Here are some clues (or decoys): It is labeled (among other things) “Bureau of Intelligence” in small letters at the bottom and “Commander” Chas. H. Davis is seated at the desk. The Library of Congress dates it as 1890 to 1901, but if Davis was a Navy Commander at the time, a rank just above Captain, it is more likely to have originated in the 1850s. But ... that was before the Civil War in the early 1860s and an official intelligence office at that time seems unlikely. Another possibility is that ‘commander’ is used in a general sense or that the image is mislabeled (which is not uncommon). Is this the forerunner to the Bureau of Investigation, which wasn’t officially established until 1908? If you ferret out the date and actual name/department of the “intelligence bureau” pictured here, enlighten me by email at davisriddle@abiogenesis.com (I have a guess, but not a definitive answer). I’ll credit the first to submit a credible solution with sources on the Web site associated with this book. [Library of Congress collection, copyright expired by date.]



Left: Matthew B. Brady (c1823-1896), in 1889. Brady took many significant historic photos of political figures of the American Civil War. Middle: The shell-damaged deck of the Confederate gunboat “Teaser” which was captured by the U.S.S. Marantanza, photographed by James Gibson (1828-?) in July 1862. Right: The ruined buildings at a Navy Yard in Virginia in 1864, documented by Alexander Gardiner (1821-1882). Many strategic and documentary images of coastal installations were recorded during the War by these photographers. [Library of Congress (photo of Brady possibly by Levin Handy), copyrights expired by date.]

In 1890, the Office of Naval Intelligence was transferred to the Office of the Assistant Secretary of the Navy and later returned to the Bureau of Navigation in April 1898. Thus, many key agencies were taking form by the turn of the century.

4.c. New Public Laws and the Rise of Technologies

Radio-Echo Detection

In Europe, a German inventor, Christian Hülsmeyer (1881-1957) sought a way to improve navigation by bouncing radio waves off of objects and detecting the returned signal. On 30 April 1904, he registered patent DRP #165546 for a *Telemobiloskop* (far-moving scope), a radio device to aid marine craft in preventing collisions. This was the forerunner of modern radio-ranging techniques. (The evolution of radio communications and radar are described in the Radio and Radar Surveillance chapters.)

The "Progressive Era"

In America, in the early 1900s, travel and communications over long distances were difficult at best. Most of America was still a wilderness. The Northwest had barely been settled for 50 years, migrant shacks dotted the Mississippi, and native Americans still followed traditional hunting practices in the forests and rivers along the Canadian border. Mechanical devices were not easy to come by. Most surveillance at the time involved simple telescopes, or the bribing of loose-tongued, eavesdropping telephone and telegraph operators. Community disturbances were handled by local law enforcement agencies. But the population was growing and technology and distance communications were beginning to have an effect on nationalism and the structure of the country.

During the early 1900s, Secret Service agents, called 'operatives,' conducted investigations on behalf of the Department of Justice (DoJ). In 1905, the Department created the *Bureau of Criminal Identification* with a central repository for fingerprint cards. Local law enforcement agencies began developing their own fingerprint repositories, perhaps in part because the DoJ was using convicts to maintain the federal print registry, a practice that understandably seemed questionable to some.

Through political pressures, Attorney General Charles Bonaparte influenced Congress to allow him to have control of investigations under his jurisdiction and, on May 1908, a law was enacted preventing the Department of Justice from engaging Secret Service agents.

Origins of the FBI

In 1908, during the latter part of Theodore Roosevelt's Presidency, a *bureau of investigations* was established by Bonaparte to investigate a variety of interstate, antitrust, copyright, and land fraud cases. Two years later when the Mann Act ("White Slave") was passed, bureau responsibilities were broadened to include criminals who might not have committed federal violations, but who were evading state laws. After the outbreak of World War I, the *Espionage Act* and the *Selective Service Act* were passed and bureau responsibilities again increased. In the course of a decade, the bureau had grown from less than a dozen to over two hundred Special Agents. On completion of their terms in 1909, both President Roosevelt and Bonaparte recommended that the force of agents become a permanent part of the Department of Justice and General George Wickersham officially named this force the *Bureau of Investigation* (BOI).

War and Post-War Surveillance

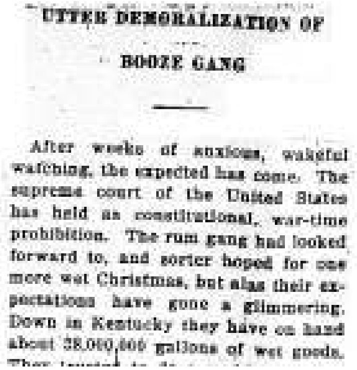
In 1917, during Woodrow Wilson's Presidency, the United States entered World War I. The war resulted in the deployment of surveillance technologies in a way that had never before been seen in the history of humankind. Submarine-spotting airships, airplanes, magnifying devices, code-breakers, etc. were all used in the arsenal to find out where hostile forces were and what they were doing (these are described in more detail in other chapters). As a result of the Great War, many new actions were taken to protect national interests.

The Bureau of Investigation acquired responsibility for the *Espionage Selective Service Act* and *Sabotage Act* and began to assist in the investigation of enemy aliens. Specialization in the department became an asset, with agents providing deciphering, foreign language, and problem-solving expertise. In 1919, the former head of the Secret Service, William J. Flynn, became the Director of the Bureau of Investigation.

In October 1919, the *National Motor Vehicle Theft Act* provided the BoI with tools by which it could prosecute criminals who tried to evade capture by crossing state lines.

Prohibition

The wages of war combined with a liberal political climate in America, (compared to the 'old countries' of the many new immigrants) had gradually resulted in a number of smuggling and export problems, as well as civil disobedience (that was in part attributed to the excessive use of alcohol).



UTTER DEMORALIZATION OF BOOZE GANG

After weeks of anxious, wakeful watching, the expected has come. The supreme court of the United States has held as constitutional, war-time prohibition. The rum gang had looked forward to, and sorter hoped for one more wet Christmas, but alas their expectations have gone a glimmering. Down in Kentucky they have on hand about 38,000,000 gallons of wet goods.

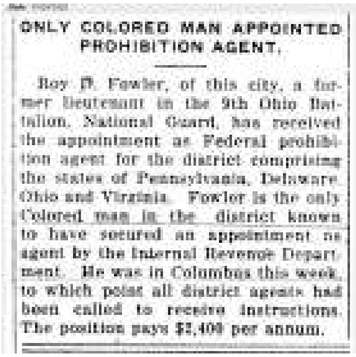
APPENDIX.

Prohibition of Slavery in Missouri.

[illegible]

PROHIBITION OF SLAVERY IN MISSOURI.

[illegible]



ONLY COLORED MAN APPOINTED PROHIBITION AGENT.

Roy B. Fowler, of this city, a former lieutenant in the 9th Ohio Battalion, National Guard, has received the appointment as Federal prohibition agent for the district comprising the states of Pennsylvania, Delaware, Ohio and Virginia. Fowler is the only Colored man in the district known to have secured an appointment as agent by the Internal Revenue Department. He was in Columbus this week, to which point all district agents had been called to receive instructions. The position pays $2,400 per annum.

Top Left: Announcement of 'Dry Christmas' after the Supreme Court upheld alcohol prohibition as constitutional in 1919. Top right: Prohibition didn't involve just alcohol; in the past, agents had been hired to uncover prohibited slavery and export violations, as well. Bottom Left: This clipping indicates that the IRS was hiring Federal Prohibition Agents in January 1920 to handle the detection and apprehension of those breaking the newly implemented alcohol prohibition laws. Bottom Right: Federal Agents at the Customs House with confiscated liquor in Brownsville, Texas in Dec. 1920. [Library of Congress clippings and photo from 1919 and 1920, copyrights expired by date.]

Civil and criminal disorders that were common at the time included fighting in streets and drinking establishments, molestation of women, and an increase in organized crime and 'gangsterism.' These factors and the War led to the implementation of *Prohibition*, the complete banning of a number of exports, social actions, and the sale and consumption of alcohol.* Prohibition granted Department of Treasury enforcement agents stronger powers with which to investigate and convict those involved in various types of crimes. The increased use of surveillance techniques allowed law enforcers to locate export contraband and many cleverly hidden stills and drinking establishments set up by those unwilling to accept the prohibitions or who were eager to earn a fortune selling them on the black market. However, most of this surveillance was conducted by local authorities, as the Bureau of Investigation, at this time still had limited powers of jurisdiction. In the early 1920s, the economy began recovering from the War and the U.S. entered the heady gaiety of the "Roaring Twenties." Technology contributed to the social order with gramophones, music boxes, telephones, and radios.

At national levels, many young men who had been trained in the war were looking for civilian work in related fields. A young law school graduate who had assisted in the *General Intelligence Division* during the war was appointed Assistant Director of the Bureau of Investigation. His name was J. Edgar Hoover. In 1924, the new President, Calvin Coolidge, appointed him the Director, at a time when the BoI had grown to over four hundred Special Agents. When he accepted the appointment, Hoover had many of them replaced. He also overhauled promotions and work appraisals and established inspections and training programs. Hoover further instituted one of the important tools of surveillance, an *Identification Division.* It was an important agency, since evidence is of no value if it cannot be associated with the persons responsible for leaving the clues. Local police fingerprint files and federal files began to be amalgamated into a central resource.

The Age of Communications

The campaign and administration of Calvin Coolidge in the 1920s was the first significant Presidential period in which extensive media coverage was used. Coolidge made liberal use of both photography and radio broadcasting to promote his political goals. Left: Coolidge sitting in the Oval Office. Right: Calvin Coolidge posing for press photos. More about this pivotal period of history is described in the Radio Surveillance chapter. [Library of Congress 1923 and 1924 Archive Photos, copyrights expired by date.]

*Total banishment of alcohol didn't work and was eventually repealed. Too many otherwise law-abiding citizens opposed it or flaunted the laws, but it had some lasting social effects nonetheless, as it resulted in restrictions that curbed the excessive use of alcohol which may have been contributing to crime at the time.

While Harding was the first President to greet Americans through the airwaves, radio truly came of age in the mid-1920s during the Presidency of Calvin Coolidge. Coolidge was the first U.S. President to make extensive use of press photography and radio technologies to further his campaign and administration goals.

The Great Depression

In 1929, the stock market crashed, the Great Depression descended, and up to a third of the population was unemployed at any one time over the next decade. It was an era of great need and crimes were being committed by individuals who tended to be law-abiding in better economic conditions. It was also a time when people craved entertainment and a respite from the hard economic realities. In spite of the difficulties, many great engineering feats and improvements in technology occurred during the 1930s, including the Hoover/Boulder Dam, cathode-ray tubes, better radar systems, and the rapid evolution of aircraft and radio communications.

In July 1932, the Bureau of Investigation was renamed the *U.S. Bureau of Investigation*, solidifying its national focus. The same year, the Bureau established a Technical Laboratory to engage in a number of types of forensic intelligence-gathering, surveillance, and analysis activities (see the Biological/Chemical Surveillance chapter).

In 1934, responding to gangster activities and increased crime due to the poverty and hardships of the Depression years, the U.S. Congress granted greater powers to the Bureau of Investigation. By 1934, Bureau agents were authorized to make arrests and carry firearms. In 1935, the Bureau was renamed the *Federal Bureau of Investigation.* The BoI had finally evolved into the FBI. The FBI National Academy was established to train police officers in modern investigative methods.

Just prior to World War II, scientific developments continued to progress. Cathode-ray tubes were incorporated into oscilloscopes and other types of display devices by the mid-1930s; radio ranging (radar) for air navigation was being promoted by 1937. Computers were being invented independently by Konrad Zuse in Germany and Professor J. Atanasoff and his graduate student Clifford Berry in America. An explosion of technology appeared imminent but the outbreak of the war changed priorities; some projects were shelved and others developed more rapidly in different directions to serve the needs of national security.

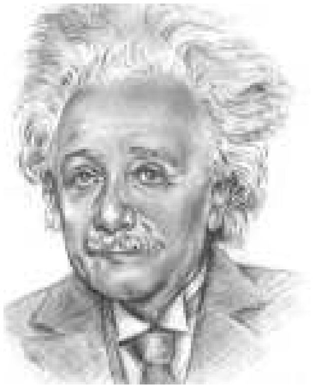
Thirty-three members of the Duquesne Nazi spy ring were found guilty by jury in Dec. 1941 through the investigative efforts of the FBI, with assistance from William Sebold. [FBI news photo, released. Identities obscured in deference to their descendants.]

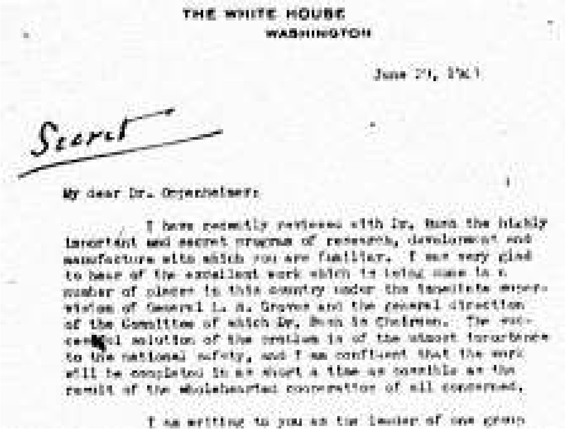
In 1939, after several years of localized unrest, the German-centered conflict broke out in Europe. Surveillance, espionage, and intelligence-gathering became major concerns for both the nations at war and those seeking to avoid war. Due to the surveillance efforts of William Sebold and the FBI, the Duquesne Nazi spy ring in the U.S. was uncovered and defeated.

In 1940, many secret service and war-related measures were taken. The U.S. Congress passed the *Smith Act*. The draft was re-established. FBI surveillance was no longer limited to monitoring foreign powers, but monitored American deserters and draft-dodgers as well. President Roosevelt established the *Special Intelligence Service* (SIS) in Latin America to monitor Axis activities and to disrupt Axis intelligence-gathering efforts.

4.d. Wartime Use of Surveillance Technologies

In December 1941, the Japanese successfully attacked Pearl Harbor, in spite of U.S. intelligence reports of a break in diplomatic relations, and the United States entered the War. By this time, increased surveillance technologies, including radar defense systems, were being put into service in the Continental U.S. and some U.S. possessions; during the course of the War, these technologies developed rapidly.





THE WHITE HOUSE
WASHINGTON

June 29, 1943

Secret

My dear Dr. Oppenheimer:

I have recently reviewed with Dr. Bush the highly important and secret program of research, development and manufacture with which you are familiar. I was very glad to hear of the excellent work which is being done in a number of places in this country under the immediate supervision of General L. R. Groves and the general direction of the Committee of which Dr. Bush is Chairman. The successful solution of the problem is of the utmost importance to the national safety, and I am confident that the work will be completed in as short a time as possible as the result of the wholehearted cooperation of all concerned.

I am writing to you as the leader of one group

Left: In 1939, Albert Einstein wrote to the President warning of a possible German nuclear threat. Right: In 1942, the Manhatten Project was initiated to build a superweapon based on nuclear fission. Shown here is a portion of a June 1943 communication marked “Secret” from President Franklin D. Roosevelt to Robert Oppenheimer, head of the Los Alamos scientists who were developing the atomic bomb. [Einstein drawing copyright 1998 by the author, used with permission; White House letter from Library of Congress, J. Robert Oppenheimer Papers.]

With the entry of the U.S. into the War, the number of FBI employees nearly doubled in three years. The War made it apparent that a wider umbrella for national surveillance/reconnaissance services was needed. President Franklin D. Roosevelt asked New York lawyer William J. Donovan to draft a plan for an American intelligence service. In July 1941, he was appointed as “Coordinator of Information.” As a result, the *Office of Strategic Services* (OSS), the forerunner of the Central Intelligence Agency, was established in June 1942, with Donovan as Director. The OSS was to collect and process strategic information as required by the Joint Chiefs of Staff and to conduct special operations not assigned to other agencies. At this time, the OSS did not have the wide-ranging jurisdiction of later organizations. The military forces and the Federal Bureau of Investigation still had their own significant responsibilities that included foreign matters.

These were turbulent times as the European war escalated into World War II. During the period of its operation, William Donovan formally suggested that the OSS be separated from the Joint Chiefs of Staff, with the new organization directly under the supervision of the President. He suggested that it would:

> "... procure intelligence both by overt and covert methods and will at the same time provide intelligence guidance, determine national intelligence objectives, and correlate the intelligence material collected by all government agencies."

The War was reaching a climax and the need for inelligence was greater than ever, but political reorganization made the OSS short-lived. In August 1945, the U.S. dropped an atomic bomb on Hiroshima; the next day Stalin appointed Lavrentii Beria to oversee the Soviet atomic bomb program and, in October 1945, the OSS was dismantled, with its functions transferred to the State and War Departments.

Then, in January 1946, President Harry S. Truman established the *Central Intelligence Group* (CIG), under the direction of the National Intelligence Authority, with a mandate to coordinate departmental intelligence to supplement existing services. Rear Admiral Sidney W. Souers, the Deputy Chief of Naval Intelligence, was appointed the first Director of Central Intelligence. The stage was set for a national, centralized approach to American intelligence operations in name if not yet in fact.

Though the records are fragmentary, it is apparent that the Soviets, unnerved by the sudden atomic offensive weapons superiority of the U.S., engaged in significant espionage at this time. Under pressure and time constraints to match the American atomic explosives capabilities, spies and informants at Los Alamos may have contributed substantially to the development of the bomb tested by the Soviets in 1949.

U.S. reconnaissance was also active in 1946. Historical notes from the 46th Reconnaissance Squadron indicate that Alaska-based personnel could air navigate in polar regions in any season. Fairbanks missions were initiated in July 1946 as reported by the Department of the Air Force:

> "... and in the following year flew more than 5,000 hours and 1,000,000 miles to test material and personnel. Its long-range project was to observe and photomap the Alaskan area for strategic location of defense installations. Other projects included ex-Magnetic Center Determined by Air Units. Exploratory flight for information necessary to establish regular air transport, service; and photomapping for oil formations, in cooperation with the Navy.... A system of reference-heading navigation which was worked out enables planes to fly anywhere and know their location to within one mile."

Thus, improvements in aerial reconnaissance and the deployment of the atomic bomb represented a shift in priorities with regard to technologies within the armed forces. For hundreds of years, naval forces had been a dominant line of defense. Now air forces were attaining a new prominence in the overall strategic picture. For thousands of years, sheer manpower had been a significant aspect of warfare, now technology was seen as an important means to enhance and perhaps someday even replace human beings on the battlefield.

> "From the earliest times through World War I, battles and wars were directed against people. The focus of effort was on killing enemy forces until the opposition withdrew or surrendered. Beginning with World War II and continuing through the Persian Gulf War, the main goal of battle made a transition from destroying people to destroying war machines. Tanks, airplanes, artillery, armored personnel carriers, air defense weapons and surface-to-surface missiles have been the prime objectives against which fire-

> power is planned and directed. Now, however, there is a new era emerging–information. Information is the key to successful military operations; strategically, operationally, tactically and technically. From war to operations other than war, the adversary who wins the information war prevails."
>
> [General Glenn K. Otis, U.S. Army, Retired, Information Campaigns, 1991 quoted in *Military Review*, July-August 1998.]

4.e. The Age of Post-War Politics

Responsibility for Security and Related Policies - The CIA and FBI

The definitions and responsibilities related to surveillance activities in the U.S. were more explicitly defined following World War II and the trend toward nationalization and centralization continued. It was clear that the interception of radio and sonar signals and the decryption of sensitive communications had been highly significant aspects influencing the outcome of the War. Post-war vigilance included the sounding of air raid drill sirens, the building of bomb shelters and bunkers, and increased foreign intelligence-gathering.

In the wake of the War, in September, the *National Security Act of 1947* was issued. This Act contained a body of important policy guidelines for U.S. intelligence activities, some of which appear to stem from recommendations made by Donovan three years earlier. It also represents another reorganization in which the National Intelligence Authority and the Central Intelligence Group were replaced by the *National Security Council* (NSC) and the *Central Intelligence Agency* (CIA).

The CIA was now responsible for coordinating America's intelligence activities with regard to matters of national security and for safeguarding intelligence methods and sources.

1945 to 1947 was a time during which a nervous post-war society turned wary eyes on Communist sympathizers in the U.S., particularly those who might be in higher levels of U.S. government. Political activists were surveilling the government and amassing classified U.S. documents. Secret service agents, especially those in the FBI were, in turn, surveilling those suspected of stealing U.S. secrets. In response, the 1946 *Atomic Energy Act* granted the FBI responsibility for determining "the loyalty of individuals ... having access to restricted Atomic Energy data." (This trend toward granting greater and greater powers for determining 'loyalty' to the United States continued for another decade.) Thus, the FBI's responsibility was broadened once again, to include background checks and monitoring of federal employees.

When Hitler died from suicide, national fears turned from Germany to the U.S.S.R. Foreign intelligence became a higher priority than ever before. Americans feared the Russians were now developing an atom bomb, which was true.

In July 1948, *National Security Council Intelligence Directive 9* (NSCID9) was issued to more clearly define national intelligence policies and responsibilities. This Directive remained in effect for some time.

The following year, in 1949, there were two significant milestones in national intelligence coordination within the U.S.:

- The CIA was granted broad powers of secrecy and funding exemptions through the terms of the new *Central Intelligence Agency Act.*
- On 20 May 1949, the *Armed Forces Security Agency* (AFSA) was formed within the U.S. Department of Defense, under the command of the Joint Chiefs of Staff.

It was intended that AFSA direct the *communications intelligence* (COMINT) and *electronic intelligence* (ELINT) sections of signals intelligence units in the military. Over time, concerns were expressed from within the government and from within AFSA itself that the organization was not effective in carrying out its functions. Over the next several decades COMINT responsibilities were scrutinized and redefined a number of times.

Korea was a strategic outpost following Japan's defeat in the War. Soviet troops occupied much of northern Korea, while Americans occupied the region south of the 38th parallel. By September 1945, South Korea was under U.S. military rule. A U.N. *Temporary Commission on Korea* had the task of drafting a constitution for a unified government for all of Korea. When denied access to the north, it continued with elections in the south, in May 1948. Shortly afterward, a constitution was adopted and the Republic of Korea was established. By late 1948, Soviet troops had withdrawn from North Korea, but maintained assistance; American troops similarly withdrew from the south in 1949, but maintained assistance.

On 29 August 1949, fears of a Soviet bomb were confirmed, when the U.S.S.R. carried out a test detonation of an atomic bomb. Cold War vigilance and surveillance of foreign atomic capabilities became a U.S. priority. Global instabilities were further heightened when, in June 1950, North Korea invaded South Korea and U.S. troops became involved in defending South Korea.

Military Intelligence Acquires a Broader National Scope

The early 1950s was an important time of development for technologies, especially microwave radio communications. New methods of broadcasting radio, television, and telephone messages were developed to take advantage of microwave frequencies. One of the most important aspects of microwave physics was that the very-short waves were not reflected off the ionosphere, but passed right through, out into space. This property enabled new types of scientific research in astronomy and in later decades was exploited to channel communications through orbiting satellites.

In March 1950, the *National Security Council Intelligence Directives* was established; it defined the responsibilities of the *U.S. Communications Intelligence Board.* The Board was responsible for providing coordination of government COMINT activities and for dvising the Director of the CIA in COMINT matters. Interestingly, COMINT activities were considered to be "outside the framework of other or general intelligence activities" and, conversely, other intelligence directives (e.g., electronic intelligence) were not considered directly applicable to COMINT. This point of view was later revised.

During 1952, a study was carried out under the chairmanship of Herbert Brownell to survey U.S. communications intelligence (COMINT), with a focus on the functions of AFSA. This became known as the "Brownell Committee Report." The Report suggested that better national coordination and direction were needed, provoking action on the part of President Harry S. Truman.

In an October 1952 Memorandum, President Truman designated the Secretaries of State and Defense as a *Special Committee of the National Security Council for COMINT* to establish COMINT policies and to provide policy advisement, with help from the Director of the CIA, through the National Security Council. This document further established the *Department of Defense* (DoD) as the executive agent for the production of COMINT information. The 1948 *Intelligence Directive No. 9* by the National Security Council was revised in December 1952 in response to this Memorandum.

The result of these studies and memoranda was that security responsibilities were shifted from AFSA to the National Security Agency (NSA), with a broader mandate of national responsibility for communications intelligence. The responsibilities of the U.S. Communications Intelligence Board were revised as well. Electronic intelligence remained within the mandate of the armed services. Two decades later, the NSA again was granted broader powers.

The National Security Act of 1947 was amended in 1953 empowering the President, with the support of the Senate, to appoint the Deputy Director of Central Intelligence (DDCI) who would stand in for the Director if he could not perform his duties or in the event of a vacancy in the position.

Post-War Prosperity and Baby-Boom Years

At this point in history, surveillance technologies were used almost exclusively by government and law enforcement agencies and were rarely seen in civilian applications. It was an era of trust and focus on personal responsibility. In the 1950s, in most towns with populations under 1/4 million, it was rare for people to lock their homes or their cars. Even when families went away for weekend outings, they would leave their homes unlocked, trusting that no one would disturb their belongings. In the United States and Canada in the fifties, burglar alarms in businesses were uncommon and in homes, extraordinarily rare. Post office buildings stayed open 24 hours a day so people with rented boxes could retrieve their mail when it was convenient and small children played in parks unattended.

In sharp contrast, at the national level, policies on national security were being revised in face of growing Cold War fears of Communist expansion.

Until this time, the FBI and other national investigative organizations had the reputation of being rather shadowy entities, but with the spread of television and long-distance communications in general, government agencies became more well-known to the general public. In the mid-1950s, the FBI's name became more prominently associated with solving terrorist crimes. When a plane exploded in 1955 in midair in Colorado, the Bureau pieced together evidence that assisted local law enforcement agents in winning a case against the person who planted the bomb.

The U.S. Congress then enacted laws which provided the FBI with greater powers to investigate racketeering, gambling, and civil rights violations. The powers of the NSA were also expanded. In September 1958, electronic intelligence (ELINT) was added by Directive (NSCID 6) to the responsibilities of the National Security Agency. This Directive was revised in January 1961.

At the same time, the perspective on intelligence functions was broadening and the motives and responsibilities of government were being scrutinized from new perspectives [underlined for emphasis]:

> "Information on the military strength and plans of a potential enemy is highly important, <u>but intelligence agencies cannot concentrate solely on the military because armed forces are only an instrument of policy. They must, at the same time, gather information on the aims and objectives of those who decide on the use of this instrument</u>. Military power is only one of many assets of the policy makers. Therefore, it is obvious that the collection of political intelligence is a matter of the first order, more so now than ever before, since the "hot war" has become a highly dangerous instrument of politics. The relative uselessness of the military instrument in the direct solution of political con-

> flicts has extraordinarily enhanced the importance of the nonmilitary spheres of the international power struggle–diplomacy, economic and cultural policies, propaganda, psychological warfare, and subversive activity...."
>
> [Dr. Georg Walter, "Intelligence Services," Military Review, August 1964.]

Public Announcements, Cuba, and Cold War Fears

Cars and TVs had profound effects on society in the 1960s. Prosperity and technology were enabling the population to become larger and more mobile. During the Baby Boom years, people had more children and bought more station wagons in which to tote around their children. 'Two-car families,' which were rare in the 1950s, began to emerge and automobiles made it possible for people to commute to work while living in less expensive houses in outlying areas now called suburbs. Neighborhoods changed and neighbors changed. Suspicions increased.

Public service announcers and insurance companies began using television to entreat people not to leave their keys in their cars and by the mid-1960s, were advising people to lock their cars at all times, even if they were only stepping into a store for a few moments or the car was parked in the driveway. In the same vein, people started locking their houses when no one was home. While it wasn't apparent at the time, this change of habits on a personal level and the gradual trends to more diligently safeguard property would eventually fuel public demand for consumer surveillance devices.

In the early 1960s, a significant political incident affected the nation. Cuba was invaded by Cuban exiles at the Bay of Pigs with support from the CIA in April 1961. Then, in October 1962, the *Cuban Missile Crisis* erupted when intelligence services discovered Soviet-manufactured nuclear missiles in Cuba capable of reaching the U.S.

This touched a nerve in a generation that still remembered the devastation of World War II. It also illustrates an aspect of American politics that is questionable in global terms. There is a general assumption by Americans that our democratic superpower knows what's best for the rest of the world and has a right to bear nuclear arms while suppressing those in the hands of other nations. There are examples of this general attitude right up to the present day. Most people would acknowledge that this is a double standard and those opposed to the incongruity might even argue that the U.S., in global terms, is hanging onto its 'might and right' in the same way the Confederates held onto their 'might and right' to preserve their superiority and status quo in pre-Civil War days. Regardless of the interpretation, the fear of nuclear proliferation in the sixties resulted in an increase in foreign surveillance in general, and technologies designed to find or defeat nuclear weapons, in particular, because the 'nuclear arms race' was no longer confined to the U.S. and the U.S.S.R.

New facilities and procedures were being implemented to improve international intelligence-related activities. The modeling of foreign terrain, buildings, and weapons systems is one way to build a composite picture of a foreign nation's priorities and capabilities. In the mid-1960s, the CIA established a workshop for creating hand-crafted 3D models based on surveillance photos and intelligence reports. This facility operated for the next three decades.

In physics labs, research was going on that would lead to the development of microprocessors. With microprocessors, it would be possible to develop smaller, lower-cost personal computers. In military and large corporate circles, visionary computer engineers began to develop networking and time-share systems, the germ that would grow into the ARPANET.

The Mid-1960s - Vietnam, Freedom of Information, and the Space Race

It's not clear how much of the social revolution and activism that occurred in the 1960s was due to increased news coverage and television viewing and how much was an evolution from earlier times, but clearly it was a era of significant scrutiny of the government by the populace. Student council meetings at universities in the 1980s were generally poorly attended, with often less than a dozen people showing up to express their views. In contrast, in the sixties, as much as 80% of the student body would sometimes attend, with megaphones broadcasting the debates and thousands of attendees spilling out into university squares.

In 1966, the U.S. enacted the *Freedom of Information Act* (FOIA), thus providing individuals with the right to request access to information or records held by federal agencies upon submitting a written request. The right was stated as being enforceable in a court of law. The scope of the Act, as it was written, was limited by nine exemptions and three exclusions. In spite of the exemptions, the FOIA was to become a driving force and an important tool of democracy.

Also in 1966, U.S. Coast Guard cutters were dispatched to aid Army and Naval forces engaged in surveillance activities in Vietnam. The Vietnam conflict was closely scrutinized, not just by avid peace demonstrators, but by many members of the general public. The interest in news media and underground publications increased. As government surveillance activities spread, apparently so did those of the public.

The U.S. Supreme Court granted the FBI greater leeway to investigate civil rights crimes. In 1968, the *Omnibus Crime Control and Safe Streets Act* paved the way for FBI use of electronic surveillance to investigate specific types of violations. The FBI was concerned about terrorist activities and used investigative personnel and counterintelligence programs (CointelPro) to counteract these activities. However, Hoover is said to have discouraged intrusive methods such as wiretapping (see Chapter 2 for contradictions to this claim). These were eventually forbidden unless they were covered under the terms of the Omnibus Crime Control and Safe Streets Act.

In the late 1960s, the world entered a new communications era with the introduction of geosynchronous satellites. By 1968, the U.S. was launching communications intelligence (COMINT) satellites (described in detail in the Aerial Surveillance chapter) specifically designed to carry out surveillance tasks. From this point on, both government and amateur satellite technologies developed rapidly. The following year, the Department of Defense (DoD) commissioned the *ARPANET*, the forerunner of the public Telenet network that was implemented in the mid-1970s.

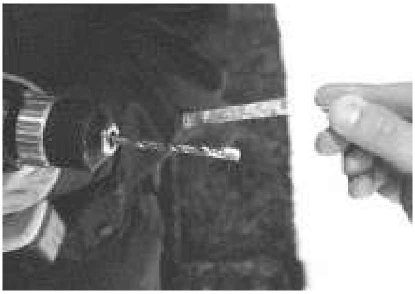
In April 1971, J. Edgar Hoover formally terminated CointelPro operations.

4.f. Nationalization, Computerization, and Government Scandals

The Establishment of Research and Technology Labs

In the 1970s, a number of government departments established or upgraded laboratory facilities to reflect advancements in science and electronics.

In 1970, U.S. Customs established a Research Laboratory to develop new analytical methods and to evaluate new instrumentation for use by Field Laboratories. The Laboratory would help maintain analytical uniformity among Field Labs and communication with other federal enforcement and technological agencies. It further would provide assistance to drug-screening and canine-enforcement programs.



Left: U.S. Customs Commissioner Kelly and Senator Campbell discussing high technology in law enforcement at a Senate Treasury Technology briefing and exhibit in Washington, D.C. Right: After a Customs canine had made a positive hit on the hull of a ship being inspected for drugs, the hull was drilled. The dust drawn out on the drill bit was placed in a chemical detector and turned blue, testing positive for the presence of cocaine. Sixty-five kilos of cocaine were subsequently seized from the vessel. [U.S. Customs news photos by James Tourtellotte, released.]

National Intelligence, and Personal Computers

In September 1971, the Kenbak-1, the first digital microcomputer, was advertised in Scientific American. The age of personal computers had begun, but few people took notice until the Altair was marketed in Popular Electronics and other electronics magazines three and a half years later.

Up to this time, the NSA was specifically concerned with communications intelligence (COMINT). COMINT is part of a broader category called signals intelligence (SIGINT) which also includes electronic intelligence (ELINT) and telemetry intelligence (TELINT) which means that COMINT, as defined by the U.S. Department of Defense (DoD), was limited in scope. However, there were even further stipulations incorporated into the administrative definitions for COMINT that restricted NSA's jurisdiction beyond a general definition of COMINT.

In order to understand why the Intelligence Community was criticized for stepping outside its mandate over the next several decades, it should be understood that the general meaning of INTs and the NSA-prescribed meaning of INTs are not the same. The general definition of COMINT encompasses all types of communications (not just foreign). However, the NSA definitions for various types of intelligence inherently included limitations as to their use. For example:

> COMINT in the early 1970s was defined as the collection and processing of "foreign communications" and was even further defined as restricted to communications that were "encrypted or intended to be encrypted." It did *not* include "unencrypted written communications, except ... [those] which have been encrypted or are intended for subsequent encryption." The NSA specifications for COMINT also explicitly excluded the interception of public broadcasts, except for "encrypted or 'hidden meaning' passages in such broadcasts."

These distinctions, in effect in the early 1970s, became important on several occasions in the 1990s, when NSA activities related to satellite and computer-network surveillance were questioned. They form the foundation for NSA statements that NSA personnel operate according to very specific guidelines.

In December 1971, NSA jurisdiction was increased. The Department of Defense issued a Directive prescribing the "authorities, functions, and responsibilities of the National Security Agency (NSA) and the Central Security Service (CSS)." This document identified the NSA as responsible for providing "the Signals Intelligence (SIGINT) mission of the United States and to insure secure communications systems for all departments and agencies of the U.S. Government." It further named the Central Security Service to conduct "collection, processing and other SIGINT operations as assigned."

In 1972, the National Security Council issued *Intelligence Directive No. 6* (NSCID6), "Signals Intelligence," prescribing the SIGINT activities and responsibilities of the Director of Intelligence. This document superseded the NSCID 6 which had been in effect since September 1958.

In May 1972, J. Edgar Hoover died. He had been the Director of the FBI for almost 48 years. L. Patrick Gray was appointed by President Nixon as Acting Director the day after Hoover's death. Gray initiated progressive hiring practices by appointing the first women Special Agents to the FBI since the 1920s.

In September 1972, the Defense Security Service (DSS) was established to consolidate personnel security investigations within the Department of Defense (DoD).

The 1970s - The Watergate Scandal

In 1972, an incident at the Democratic National Headquarters in the Watergate Building involving undercover operations demonstrated the importance of understanding many aspects of surveillance, including wiretapping, investigative surveillance, and surveillance of government activities by the news media and the public.

In connection with Watergate, five men authorized by Republican Party officials were arrested for breaking in and allegedly photographing confidential Democratic documents. A blatant coverup followed which took years to untangle. At a key period in history, just before the birth of microcomputer technologies, the behavior of President Nixon and his party members had demonstrated to the country at large that trusted government officials were not above using surveillance devices, tape recordings, and wiretaps in illegal and unethical ways.

As turmoil erupted in the Nixon White House, progress in computer networking began to take hold as distributed computing evolved on the ARPANET and the first network email programs were developed. These innovations were enthusiastically adapted by computer users. The ARPANET was demonstrated at the International Conference on Computer Communications (ICCC), resulting in the formation of the *Internet Network Working Group* (INWG).

In July 1973, Clarence Kelley was appointed to be the new Director of the FBI. Gray's opportunity to become Director had been sullied by the scandal in the Nixon White House. Kelley came from within the department, having been an FBI Agent for twenty-one years prior to his appointment. The following year, the FBI moved from a shared building with the Department of Justice to its own premises on Pennsylvania Avenue.

1974 was a time of great public scrutiny and outcry, resulting in a number of important events and changes in U.S. policy directly related to surveillance and privacy.

The discovery of Watergate and the subsequent obstruction of justice by members of the White House turned a battery of surveilling eyes toward the Presidential administration, resulting in the resignation of Vice President Spiro Agnew (after charges of tax evasion) and, later, the resignation of President Nixon, in August 1974.

Also in 1974, the public and Congress scrutinized FBI methods to ensure that they didn't violate Constitutional rights. Further, the U.S. Congress passed the *Privacy Act* to ensure access and the right to correct information about oneself held in federal files.

In spite of significant political upheavals at the time, research continued in the computer networking world. In 1974, Vint Cerf and Bob Kahn published a document which became a significant milestone that inspired computer developers. "A Protocol for Packet Network Interconnection" specified Transmission Control Program (TCP), a practical means of sending data over computer networks. Telenet, the first packet-based system for non-military use, introduced network computing to the public. Telenet was essentially an open version of the ARPANET and it evolved rapidly.

Meanwhile, public and government housekeeping activities did not end with Watergate or investigations of the FBI. The NSA was now also under scrutiny.

In August 1975, the Director of the NSA admitted to the U.S. House of Representatives that the NSA "systematically intercepts international communications, both voice and cable." He acknowledged that domestic conversations were sometimes picked up in the course of gathering foreign intelligence, a fact which was later investigated and reported as 'incidental.' This exoneration didn't appear to alleviate watchdog concerns or reduce the scrutiny of NSA activities. The public was demanding the right to surveil the actions of tax-supported intelligence agencies.

The Birth of the Personal Computer

In 1975, a highly significant event occurred in electronics. Until this time, computers were very large, very expensive, and very awkward technologies which were primarily owned by governments, a few large corporations, and educational institutions. A few 'bleeding edge' personal computers had been unsuccessfully marketed since the Kenbak-1 was introduced in September 1971, but the Altair computer, introduced in kit form late in 1974, became commercially successful and spurred the creation and growth of an explosive new consumer industry. COMINT would have to grow and adapt to keep pace with the flood of information exchange that resulted from the expansion of personal computers.

The FBI had been reasonably autonomous in its intelligence methods up to this time. As a result of the scrutiny over the last several years, however, much more detailed specifications were handed down by Attorney General Edward Levi in March 1976 (foreign investigations) and again in April (domestic investigations).

As Director of the FBI, Kelley continued to carry out his responsibilities in spite of the turmoil. He implemented equal-opportunity hiring practices and established three clear national priorities consisting of foreign intelligence, organized crime, and white-collar crime.

The furor over internal intelligence activities continued. The Church and Pike Committees investigated these matters in 1975. The Church Committee focused on allegations of assassination plots and harassment of individuals and the overall structure and operations of the Intelligence Community. The Pike Committee focused more on the last decade or so of defense intelligence performance of the Intelligence Community. The resulting Pike Committee Report was withheld by a vote of the House (a draft was leaked to the press), but the Church Committee's Final Report was submitted to the public in April 1976. Responding to one of the Church report's main recommendations, a permanent *Senate Select Committee on Intelligence* (SSCI) was established by the U.S. Senate in May 1976.

In 1977, the Carter administration created the U.S. *Department of Energy* (DoE) as a response to the energy crisis and to act as an umbrella organization for energy-related enterprises and scientific research. Over the years, concerns were raised that security was not being handled as comprehensively and expertly as were scientific activities within the department. One of the cited examples was classified documents about advanced nuclear weapons being openly available to the public in a Los Alamos library.

Responding to reports of surveillance abuse on the one hand and laxity on the other, President Carter signed Executive Order 12036 on January 1978, providing explicit guidance on the execution of intelligence activities, and reorganized the intelligence structure. The *Foreign Intelligence Surveillance Act of 1978* resulted from the findings and allegations of the Pike and Church Committee reports.

4.g. The Computer Age and Space Technologies

Proliferation of Computers and Eyes in the Sky

In the mid- to late-1970s in the computing world, personal computers as we know them began to create a new industry. The Radio Shack TRS-80 and Apple Computer were the two most prominent and successful products in the personal computing industry at the time. New stores, called 'Computing Centers' began to spring up throughout the country. Software programmers sold their software on cassette tapes and 8" floppy diskettes in plastic baggies with eight-page photocopied manuals for $30 to $200 per product, making more money than they knew how to spend. Some of the most successful programmers, creating games, earned royalties as high as $14,000 per month.

With the evolution of computer technology came new opportunities to commit mischief and crime. A new breed of computer 'spy' emerged, called a hacker. A hacker was a computer techie who had the talent and ambition to 'break in' to other people's computers, examining their system configurations and the content of their data files. When modems and computer bulletin board systems (BBSs) were established, hackers started breaking in through network connections as well.

Computer electronics weren't used just in computers; they were incorporated into many other types of technologies. Toward the end of the 1970s, the U.S. implemented a new series of communications intelligence satellites as successors to the CANYON series. Sensitized members of watchdog agencies and the press were now on the constant lookout for surveillance satellite projects and it was becoming more difficult to carry out covert aerial surveillance without accountability and public relations efforts.

In 1978, William H. Webster, a former federal Judge, became Director of the FBI, following the resignation of Clarence Kelley.

By the 1980s, the global population had grown to 5.5 billion people, cities swelled, people moved frequently, neighbors were less familiar, and safety and security became important concerns. In contrast to the 1960s, people began locking the doors of their houses even when they were at home, and home and business burglar alarm systems began to sell well. The phrase 'home invasions' was coined to describe violent burglaries that occurred when the perpetrators knew, prior to entering the premises, that the occupants were home. Car-theft-deterrent devices became common. The computer era picked up momentum as personal computers reached business and home markets. Video cameras dropped in price. It was a time of relative economic stability and significant social and technological change.

Broadening Government Scope of Surveillance of U.S. Persons

The emphasis on surveillance and countersurveillance increased as society moved into the 1980s, with a particular focus on evaluating and incorporating the new microcomputer technologies.

In March 1980, the Secretary of the Treasury delegated authority for technical surveillance countermeasures to the Assistant Secretary (Enforcement and Operations) under *Procedures for the Conduct of United States Secret Service Technical Surveillance Countermeasures* who reports to the *Under Secretary for Enforcement.* Most of the U.S. Treasury functions related to security and surveillance, including the U.S. Customs Service and the U.S. Secret Service, are currently under the jurisdiction of the Under Secretary, Department of the Treasury.

While it is hard to make generalizations based solely on unclassified documents, it appears that one of the trends over the past three decades, in the issuance of NSA-related intelligence directives, is that they were becoming wordier and more encumbered by the greater explicitness of the definitions.

In October 1980, the NSA/CSS issued the *United States Signals Intelligence Directive* (USSID) which prescribes policies and procedures, and assigns responsibilities related to the SIGINT System (USSS) with a stipulation to safeguard "the constitutional rights and privacy of U.S. persons." The Directive, titled "Limitations and Procedures in Signals Intelligence Operations of the USSS (FOUO)," superseded USSID 18 from May 1976.

The 1980 Directive specifically declares who or what might be considered 'foreign' persons and thus subject to SIGINT. Previous documents had indicated that U.S. citizens and permanent residents would not be considered foreign and implied that they were thus exempt from SIGINT; this document specified that an "agent of a foreign power" meant, among other things [underlined for emphasis]:

> "b. Any person, including a U.S. person, who -
>
> (1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a foreign power, which activities involved, or may involve a violation of the criminal statues of the United States; ....
>
> (2) ....
>
> (3) ....
>
> (4) ....
>
> c. A U.S. person, residing abroad, who holds an official position in a foreign government or the military forces of a foreign national and information about whose activities in that position would constitute foreign intelligence."

Later in the document *U.S. Person* is defined as:

> "... a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association organized in the United States or substantially composed of United States citizens or aliens admitted for permanent residence, or a corporation incorporated in the United States.
>
> a. The term "U.S. person" includes U.S. flag, nongovernmental aircraft or vessels. The term does not include a corporation incorporated in the United States that is openly acknowledged as a foreign government or governments to be directed and controlled by such foreign government or governments. [definition continues]"

As previously stated, it's difficult to make informed generalizations based only on declassified documents, but some trends can be extrapolated from the declassified U.S. Directives and the information at large. They indicate that

- surveillance was becoming more complex,
- NSA responsibilities were gradually broadening in scope,
- technology was increasing in importance in overall intelligence-gathering methods,
- secrecy and broad funding of U.S. secret services were being safeguarded,
- intelligence-related documents were becoming wordier and more complex,
- the scope of SIGINT had been explicitly broadened in the 1980 Directive to include possible surveillance of U.S. persons who the government considered to be security risks, and
- privacy advocacy, the desire for government accountability of surveillance activities, and the desire for access to information on the part of the public was increasing.

In October 1981, the Reagan administration revamped the President's Foreign Intelligence Advisory Board and named a number of distinguished citizens to serve on the Board. In December, clear goals were set and ambiguities clarified for the Intelligence Community.

In May 1982, William Casey, Director of Central Intelligence, issued a Directive which established a *Signals Intelligence* (SIGINT) *Committee* to advise and assist the Director of Central Intelligence (DCI) and the Director, National Security Agency (DIRNSA), within the Intelligence Community.

In June, President Reagan signed the *Intelligence Identities Protection Act of 1982* into Public Law 97-200. This imposed criminal penalties on anyone who wrongfully divulged the identities of covert intelligence personnel, a measure intended to protect vulnerable members of the Intelligence Community. In 1984, the President exempted the CIA from the search and review requirements of the Freedom of Information Act with respect to sensitive files through the *Central Intelligence Agency Information Act of 1984*.

Following a number of international terrorist bombings, the Director of the FBI added counterterrorism as a fourth national priority. The FBI was also granted greater jurisdiction along with the Drug Enforcement Administration (DEA) to handle narcotics investigations.

Evolution of the ARPANET and Network Addressing

By 1983, the ARPANET computer network had been split into two sections: ARPANET and MILNET (military network). MILNET continued to be used for nonclassified military communications while ARPANET came under the administration of the National Science Foundation.

In 1984, the development of *name servers* and the evolution of routing technologies allowed networked computers to exchange messages without the prior declaration of an explicit end-to-end path. In less technical terms, this means that a message could be sent from A to F without declaring a specific route through B, C, D, or E. It's like sending a letter to your friend across the country with the understanding that the postal service will find the best way to route it (and that the routing might change, depending on what is currently most efficient). In the same way, a name-server system decides electronically on how to route your email (or other data communication) on your behalf.

This approach to networking made systems more powerful and flexible; developers created ways to process packets and send them to their intended destination regardless of how many computers were attached to a system and which ones were active at any given time.

However, it also meant that a centralized authority was needed to issue unique identifiers to each server in order for the system to work. In other words, a postal system needs an *address* in order for your friend to receive your letter, and a networked computer needs an *electronic address* in order for the destination computer to receive your electronic communication. Thus, the Domain Name System (DNS) was introduced in 1984.

Since computer communications now increasingly relied on name-server concepts, it didn't matter which route the communications packets took. They could even be split up, sent through different routes, and reassembled at their destination. This made it more difficult for those seeking to eavesdrop on electronic communications to intercept messages en route. Not knowing *where* to intercept the message or how much of the message could be retrieved at any particular time increased the security on distributed networks and made the task of surveillance much more difficult. The weakest link in surveillance terms was no longer the network itself, but rather the less secure computers at each endpoint and the less security-conscious people who were using them.

Surveillance of Social Events and Government Consolidation

In 1984, Los Angeles hosted the international Olympic Games. Everyone associated with the Games wanted to prevent hostage situations as had occurred in the 1972 Munich Games. Surveillance to safeguard the athletes and the public were put into effect. The FBI established a *Hostage Rescue Team* to aid in public safety efforts. Since that time, many of the types of surveillance activities associated with the L.A. Games are used in a variety of large-scale sports, music, and religious events.

In 1984, the Assistant Chief of Staff for Intelligence established a new agency, the *Army Intelligence Agency* (AIA), to direct scientific, technical, and general intelligence (except for medical intelligence). In 1985 several departments were put under the direct control of the AIA, including the Intelligence and Threat Analysis Center (ITAC), the Foreign Science and Technology Center (FSTC), and the Army Missile and Space Intelligence Center (AMSIC).

Counterintelligence Efforts

1985 was dubbed 'The Year of the Spy' due to the discovery of penetration into America's sensitive agencies. The FBI uncovered a surprising number of espionage activities during this time and the CIA was investigating internal security breaches that were in part traced to Edward Lee Howard and Aldrich H. Ames. *Due to these revelations, counterintelligence became a higher national priority.*

While the U.S. intelligence agencies were investigating internal security concerns, the public was requesting increasing numbers of documents through the Freedom of Information Act (FOIA). It became apparent that a national clearinghouse for these documents would reduce redundancy and provide a valuable central resource for further research and analysis. Thus, in 1985, the *National Security Archive* was founded as a nonprofit, nongovernmental library, archive, and research resource. It was established to gather and study information on international affairs and declassified U.S. documents obtained through FOIA and a public-interest law firm. Supported by public revenues, private foundations, and many donations of documents from individuals, it has grown significantly.

In 1986, the Lawrence Livermore Laboratory established a formal counterintelligence program to identify trends in foreign intelligence threats against personnel and to educate employees about counterintelligence issues.

In 1987, Judge Webster, head of the FBI, became the Director of the CIA. John E. Otto, Acting FBI Director in Webster's absence, established drug investigations as the fifth national priority. Judge William Steele Sessions then became Director of the FBI. Sessions began working with educational and community institutions to implement drug-use reduction programs for the youth.

Two important political trends were emerging in the mid-1980s in the United States: a greater emphasis on security within government circles and increased access to, and dissemination of, government information by private and independent agencies. These opposing trends of increased security and increased openness could ultimately be self-defeating or could indicate a healthy balancing dynamic characteristic of a democratic free society. Which interpretation is correct may not be knowable until a span of years has passed. What is known about the mid- and late-1980s is that investigations into domestic affairs and corruption in high levels of the government and financial institutions were turning up some unsettling facts.

FBI investigations at this time unearthed corruption and bribery within the U.S. Congress (ABSCAM) and other levels of government. Investigations of bank failures by the FBI and by investigative journalists gradually revealed a pattern of deliberate manipulation of real estate holdings and bank loans to further personal goals, especially those of certain directors associated with these institutions. In pursuit of money that became accessible through deregulation, the perpetrators falsified documents, committed bribery and, apparently, even committed murders. This internal looting resulted in the eventual collapse of several dozen savings and loan institutions.

Members of the Intelligence Community

It is not unusual for members of the Intelligence Community to transfer among different intelligence/security departments or for senior members to be involved in special commissions and surveys.

Members of the Intelligence Community come from different walks of life, but many of them have military backgrounds. It is outside the scope of this chapter (and this book) to list prominent individuals in the intelligence community, since the focus is on technology and not human intelligence (HUMINT), but it is useful to read the profile of at least one intelligence professional with strong ties to the technology community. This puts a 'face' on the field and gives insight into the types of roles intelligence professionals play in government and industry.

Admiral Bobby R. Inman earned a Masters degree from the National War College in 1972 and subsequently held secret service positions for many years. He was Director of Naval Intelligence from 1974 to 1976, after which he became Vice Director of the Defense Intelligence Agency (DIA). He was the first naval intelligence specialist to reach a four-star rank. In 1977, he was appointed as Director of the National Security Agency (NSA).

In 1980, Inman established a National Security Agency Director's Trophy to recognize outstanding performance by U.S. cryptologic mobile units which support military commanders. His career indicates a strong interest in cryptologic technologies and he has made public statements regarding the role of cryptology in security.

In January 1981, the Reagan Administration nominated Inman for Deputy Director of the CIA, a position that he subsequently assumed.

In February 1982, *Aviation Week and Space Technology* printed an article by Inman "Classifying Science: A Government Proposal," which describes tension between the goals and climate of research and the government's national security aims, especially with regard to cryptologic research and applications. In the article, Inman suggests that scientists should include review of possible implications for national security before initiating a project:

> "A potential balance between national security and science may lie in an agreement to include in the peer review process (prior to the start of research and prior to publication) the question of potential harm to the nation. The details of such a system would have to be resolved, of course, but cooperation will be better for all of us than confrontation.
>
> Included in such a system should be goals to simultaneously preclude harm to U.S. national security and to impose no unreasonable restrictions on scientific research, publication, or the use of the results. And when restrictions are judged necessary, speedy procedures for appeals, review and appropriate compensation should be included."

This is a tall order, given that the eventual results of any particular line of research are difficult and sometimes impossible to predict and that any government veto process would be strenuously opposed by many members of the scientific community. Inman continues:

> "One example of this type of process is that recommended in the Public Cryptography Study Group. It is not easy to create workable and just solutions that will simultaneously satisfy the wide-ranging needs of national security and science, but I believe it is necessary before significant harm does occur which could well prompt the federal government to overreact."

Is this statement a veiled warning or a premonition of the heated government/private sector computer-encryption debates that erupted ten years later? (See the chapter on Cryptologic Surveillance for more information on encryption debates.)

In July 1982, Admiral Inman retired from the U.S. Navy, and his focus changed from government to the technology sector. He accepted positions on the Boards of Directors of numerous companies. He chaired a number of technology companies. Considering the challenge inherent in managing just one high-tech company, the diversity and overlap of Inman's corporate affiliations are surprising. Inman founded and became Chairman and CEO of the Microelectronics and Computer Technology Corporation (MCC)* from 1983 to 1986. From 1986 to 1989 he was Chairman, President, and CEO of Westmark System, Inc., an electronics holding company, and simultaneously held the position of Chairman of the Federal Reserve Bank of Dallas from 1987 to 1990.

In 1984, Inman convinced Douglas B. Lenat, a programmer with an interest in artificial intelligence and heuristic problem-solving algorithms, to join the newly formed MCC in Austin, Texas. Lenat would assemble a team to create "CYC," a computer program with common-sense reasoning skills. A new company, Cycorp, was spun off from MCC in 1994 and CYC showed promise in the area of intelligent searching, such as information retrieval from an image library in ways different from the traditional keyword-lookup structure.

In the mid-1980s, while chairing MCC, Inman was still involved in national security and reported on international diplomatic security through the Inman Commission Findings, submitted in 1985. These resulted from a panel set up by Secretary of State George P. Shultz.

The Findings made recommendations for improving international security, including modifications to physical structures. Recommendations included removing glass and blast-channeling corridors, moving people from the vicinity of windows, and creating high walls and longer building setbacks from streets (to protect from car bombs). Further recommenda-

*Among other products, MCC sells ExecuSleuth, a corporate surveillance software product with 'intelligent agents' designed to manage information by reading and understanding text, databases, and images. It is further designed to generate alerts when tactical and strategic changes occur. The product claims to track information on key competitors in realtime, to monitor changing market conditions, and to track changes in market conditions, technologies, and the infrastructure.

tions involved improving surveillance and having guards inspect delivery vehicles at some distance from the embassy sites before accompanying them to the site. The Findings further suggested that technological upgrades and increased operational countersurveillance could help deter terrorists.

In the mid-1990s, the Clinton Administration nominated Inman for the position of Secretary of Defense. To the surprise of many, Inman held a press conference in January 1994, withdrawing his nomination Those who witnessed the conference claimed that it was very odd. In a disjointed, rambling address, Inman cited personal attacks on him in the media among other reasons for withdrawing. Supporters speculated that perhaps Inman had doubts about returning to public service. William J. Perrey was replaced as nominee for the position.

Inman serves on the Boards of several prominent companies, including Science Applications International Corporation (SAIC). In March 1995, SAIC bought out Network Solutions Incorporated, the administrator of the domain name registry for the Internet, and a fee system was instituted for domain names through NSI. SAIC handles many government contracts that are directly or indirectly related to intelligence, defense, and law enforcement. By December 1997, SAIC was listed as the 41st largest private company in America with a high percentage of employee ownership.

Although mainly involved in the private sector, Inman's opinion was still being sought with regard to the government Intelligence Community. In January 1996, Inman testified at a *Hearing of the Commission on the Roles and Capabilities of the United States Intelligence Community.* At the hearing, he offered his opinions on reorganization, made suggestions about priorities, emphasized the continued importance of human intelligence (HUMINT) activities, and expressed his opinion on the issue of disclosure of intelligence expenditures to the public.

Inman's affiliations are many. He holds the position of Adjunct Professor in the Department of Management at the University of Texas at Austin. He is listed as "Investor" on the Board of Directors of the Xerox Corporation and as an individual donor to RAND, a national security research organization. He serves or has served on the Boards of Directors of Fluor, Science Applications International, SBC Communications, Temple Inland, the Public Agenda Foundation, Southwestern Bell, and others. He further is a Trustee of the American Assembly, the Center for Excellence in Education, and the California Institute of Technology. He serves on the Executive Committee of the Public Agenda Foundation and is a member of the National Academy of Public Administration.

In spring 1999, Inman was interviewed about secret ECHELON global surveillance activities by a number of members of the press, despite the fact that he had not been affiliated with the NSA and the CIA since the early 1980s. Nevertheless, he is quoted as saying that the organization was not involved in intercepting and sharing economic secrets, but only "fair trade issues and trade violations ...."

In 1998, U.S. embassies in East Africa were bombed. Following the bombings, Kenneth H. Bacon reported to a Department of Defense news briefing on the U.S. response to the bombings. In the brief, Bacon cited the 1985 Inman recommendations, stating that since 1986, many changes had occurred in the security of existing embassy buildings, and new buildings had incorporated 'Inman standards,' that is, they were well-fortified, with high walls and long setbacks from the streets.

Thus, Inman had continued to influence aspects of security through the Inman Findings long after his departure from public service and the press apparently perceives him as a liaison to the government, as it continues to seek out his perspective on Intelligence Community (IC) activities. This short profile indicates that specific individuals within the IC can have significant influence on both government and business developments over a long period of time.

4.h. Global Commerce, Government, and Communications

The Internet

In the field of technology, a computer revolution was underway. Cpt. Ralph Peters in "Perspectives on the Future: The Army of the Future," *Military Review*, September 1987 wrote:

> "At present, technology is outstripping the military imagination so swiftly that available hardware will continue to define tactics for a long time."

The growing global computer network was now known as the *Internet* and the security of the Internet, or the lack thereof, made a media splash when the 'Internet Worm' spread through thousands of host computers in November 1988. To add to the commotion, the doctoral student who created the Worm turned out to be the son of the former Chief Scientist of the National Security Agency (NSA).

The use of computers for NSA intelligence-gathering was brought to public attention in August 1988, when Duncan Campbell's article in *New Statesman* described a multinational electronic surveillance system called Project P415. Campbell reported that witnesses had been subpoenaed to provide the plans and manuals for the "ECHELON" system and described government projects for monitoring long-range radio and satellite communications.

Shortly thereafter, "The Cuckoo's Egg," Clifford Stoll's autobiographical account of foreign agents infiltrating U.S. computer networks, lent further fuel to concerns about the potential for the misuse of electronic communications.

Late 1980s - Concerns About Personal and Computer Security

Airport security began to tighten up in the late 1970s after two decades of very low security and relative calm. However, plane hijackings and bombings had prompted spot-checks and metal detectors to be installed. By the late 1980s, the sensitivity of gate surveillance devices had been increased and X-ray machines had been added to the security arsenal at airports.

In America, communities continued to grow and change. Gated communities began to spring up in smaller towns. Previously these had been confined to large or wealthy neighborhoods, but concerns over the protection of property and people had increased and some people felt gates would solve the problem.

Humans are social beings. They want to spend time with friends and relatives, so gated communities had to be designed to accommodate the social needs of their occupants. Gates that are monitored around the clock were sometimes staffed with human attendants in kiosks (three shifts a day). With wages, benefits, and utilities, it added up to about $8,000/month, an expense that had to be borne by the people in the community. To reduce costs, many gated neighborhoods substituted surveillance devices, including cameras, door openers, and motion detectors. Electronic sensors weren't as effective as human attendants; door opening systems were easy to defeat, and compensations had to be made to provide emergency vehicle access.

In the computer community, security concerns were also being felt and adjustments were being made. Security breaches of the Internet made those who were beginning to depend on it for personal and business communications painfully aware of its vulnerability to attack. *Firewalls*, a means of restricting network access, were more widely established, and computer security experts were called in by many of the larger business firms.

This vulnerability was also being felt in official circles responsible for national security. DARPA (Defense Advanced Research Projects Agency) responded to network security concerns by forming the *Computer Emergency Response Team* (CERT) and the Department of Defense looked into the adoption of OSI instead of TCP/IP as a transmission protocol.

1990s - Provisions for Privacy, ECHELON, and Public Concerns

Internet growth exploded in the 1990s, from a quarter million hosts and less than 10,000 domains to more than 40 million hosts and two million domains. Much of this growth can be attributed to the development of the World Wide Web (WWW), a basic document-serving system released in 1991 that made Web sites possible. The WWW, originally developed by Tim Berners-Lee, represented only a subset of the content of the Internet, but it was an important subset because it was accessible to businesses and the ordinary user.

Most of the new growth on the Internet came from home and small business Web users, people with no former background or technical expertise in computers. They were delighted to find a simple hypercard-like means of accessing computer files. The Internet was originally a small community of technically proficient programmers and researchers but now included a majority of people with minimal understanding of the vulnerability of their communications content or systems.

The 1990s represents an era of tremendous growth in communications and the implementation of electronic surveillance technologies. The trends include

- greatly increased technological surveillance in both civilian and government activities, including search and rescue, domestic and business security, law enforcement, and national security;
- on an international level, a trend away from larger, more generalized conflicts, to smaller localized conflicts fought with advanced tools of warfare;
- persistent rumors of a reported “Big Brother” ECHELON project;
- the expansion and evolution of the global Internet;
- government concerns about keeping up with the pace of technological change and effective deployment of new technologies;
- the establishment of a number of Net-based organizations for safeguarding privacy and freedom of information and expression on the Net, including the Electronic Frontier Foundation; and
- public concerns for uses and possible abuses of surveillance technology by government agencies.

In the general marketplace, detection systems and other surveillance technologies were becoming common. Car buyers no longer had to install their own automobile alarm systems, as car alarms were being factory installed. Video cameras were added to home and office security to expand existing burglar alarm systems and nannycams were placed in nurseries. Retail stores installed hidden or visible camera systems (sometimes both) in increasing numbers.

In terms of surveillance and security, another highly significant change occurred in the 1990s. Up to now, most communications technologies were analog, but digital technologies were increasing steadily. Digital systems made it easier to encode and encrypt broadcast communications. New means of encryption, spread-spectrum technology, and other ways to ensure privacy and anonymity were being developed by computer programmers and electronics engineers. As the technology changed from analog to digital, the interception and decryption of telephone conversations and satellite communications now required skill and dedication.

ECHELON Rumors and Privacy Constraints

Since the early-1990s, rumors about a secret global surveillance system called ECHELON have circulated through the Internet community and some individuals have characterized it as a U.S. Government see-all/hear-all global surveillance network that monitors and records every electronic communication on the planet. Given the massive, unwieldy volume of information that would result from such a mandate, and the poor signal-to-noise information-ratio that is inherent in most computer communications, it is more likely that ECHELON has specific operational foci and goals, and priorities that relate to national security. There are U.S. Government declassified documents that have been released which confirm the existence of ECHELON, but do not indicate the project's scope or focus. More telling perhaps are the privacy stipulations that are alluded to in other parts of documents that mention ECHELON.

In March 1991, the Central Intelligence Agency (CIA) moved into its new expanded headquarters. A 'time capsule' was built into the cornerstone with documents and photos representative of the period.

In September 1991, the U.S. Naval Security Group Command issued *NAVSECGRU Instruction C5450.48A* (cancelling C5450.48). The Instruction prescribed the missions, functions, and tasks of Naval Security Group Activity *Sugar Grove*, West Virginia, which was described as an active (fully operational) shore activity. The 544th Intelligence Group was included in the Tenant Commands. The Group was tasked with processing and reporting intelligence information and maintaining and operating an ECHELON site (the wording suggests there may be other ECHELON sites), and [underlined for emphasis] to:

> "(3)(U) Ensure the privacy of U.S. citizens are properly safeguarded pursuant to the provisions of USSID 18.
>
> (4) ....
>
> (5)(U) Operate special security communications facilities, as directed."

Note that intelligence Directives from the late 1940s to at least the 1980s, including USSID 18, had clauses that stipulated the safeguarding of the privacy of "U.S. Persons" . It is not clear whether the wording of Instruction C5450.48A, which stipulates "U.S. citizens" rather than "U.S. Persons," indicates a change in direction or priorities, but from a legal point of view, such wording distinctions can be significant. Reading between the lines suggests that the ECHELON project mentioned in the same document has been defined and established in previous documents and may be just one installation in a multiple-site network.

The President's Foreign Intelligence Advisory Board (PFIAB) cited a classified document in reporting that listening devices were discovered in U.S. weapons-related facilities in the late 1980s. The PFIAB further reported in January 1998 that "Anecdotal evidence corroborates, and intelligence assessments agree, that foreign powers stepped up targeting of DOE" during the early part of 1992. The Department of Energy (DoE) is an important agency in the American resource and economic structure and its security is a high national priority. Perceived security weaknesses in the DoE and weapons facilities may have generated internal support for increased domestic and foreign security as well as projects like ECHELON.

In 1992, a *Memorandum of Understanding* aided in establishing a formal relationship between the FBI and the DoE with regard to counterintelligence activities.

In September 1992, Gerald E. McDowell of the U.S. Department of Justice received a response to his inquiries from Stewart A. Baker, General Counsel, representing the National Security Agency/Central Security Service. This document lends some support to the theory that there had been a gradual shift in priorities with regard to privacy, from 'U.S. persons' to 'U.S. citizens,' and from foreign communications to some that may have been domestic and thus were questionable. It further indicates an increased sensitivity to these privacy protections following reported abuses. Remember that it was stated and quoted from Directives in earlier decades that SIGINT and other intelligence aspects were explicitly restricted to *foreign* communications. Baker sought to allay concerns about government monitoring of the Banca Nazionale del Lavoro (BNL) and clarifies the agency's position on surveillance as a result of admitted abuses in the 1970s [underlined for emphasis]:

> "... The interception of communications by this Agency is extremely sensitive because of the danger it poses to the privacy of American citizens. In the early 1970s, this Agency improperly targeted the communications of a number of Americans opposed to the Vietnam War. In response to these abuses, uncovered by the Church and Pike Committees in 1975 and 1976, the Foreign Intelligence Surveillance Act of 1978, Executive Order 12333, numerous regulations now limit the targets of our collection efforts. As a result, NSA may only target communications for the purpose of producing foreign intelligence; we have no authority to target communications for law enforcement purposes. Our responses to you are thus based on a review of intelligence reports issued by NSA, and not a new review of intercepted raw traffic."

A declassified government document from December 1995, "Air Intelligence History," includes information on the "Activation of Echelon Units" which describes agreements to increase the Air Intelligence Agency's (AIA) participation by establishing new AIA units, with activation of these detachments in 1 January 1995. Portions of this document have been expunged, but in the ECHELON section, it mentions sites in West Virginia, Puerto Rico, and Guam.

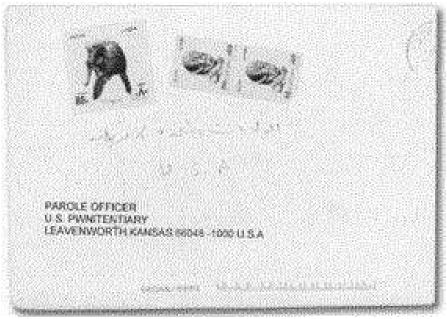
In October 1996, the Center for International Policy (CIP), a watchdog agency and independent advocate for peaceful U.S. foreign policies held a *Seminar on Intelligence Reform.*

4.i. Mid-1990s - Terrorism, Upgrades, and International Smuggling

The mid-1990s was a time when many organizations began assessing programs and installing surveillance technologies for both government and private uses. Museums, service stations, department stores, grocery outlets, schools, and border stations added new systems or upgraded existing surveillance systems, especially motion-detector and visual surveillance devices.

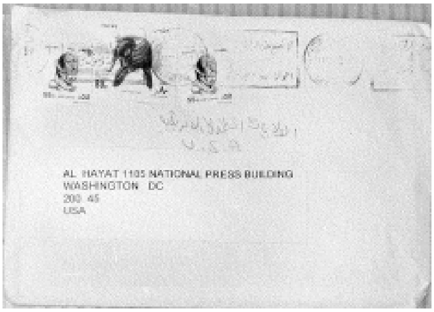
In January 1993, a foreign terrorist stood in front of CIA headquarters and shot at motorists, murdering two people and injuring three others. Then, in February 1993, the world was stunned when a great explosion damaged the World Trade Center in New York City, injuring over 1,000 people and killing six. Children were trapped for hours in the smoke-filled building.

Smuggling concerns continued in the 1990s. The influx of human cargo from developing or repressive nations received greater media coverage than ever before as news surveillance choppers flew over seized ships and cargo containers. Newer X-ray technologies were used to inspect containers and uncovered a surprising number of stowaways. Often these refugees and illegal aliens had paid $10,000 to $60,000 per person to be transported, yet were found in poor health: hungry, thirsty, and diseased. Often the ships carrying them were unseaworthy. Sometimes the stowaways died before reaching their promised destinations. Major surveillance efforts by the DoJ in conjunction with the Secret Service, the IRS, and the Customs Service resulted in the apprehension in 1994 of a large international ring of smugglers of human refugee and nonrefugee aliens. The smugglers were also subject to prosecution on a number of other charges, including bribery, fraud, and money laundering.



U.S.A

PAROLE OFFICER
U.S. PWNITENTIARY
LEAVENWORTH KANSAS 66048-1000 U.S.A



U.S.A

AL HAYAT 1105 NATIONAL PRESS BUILDING
WASHINGTON DC
200 45
USA

Letter bombs disguised as holiday greeting cards were delivered to the U.S. and the U.K. Unfortunately, one bomb exploded in London, injuring two people. Three others were discovered at the U.S. Federal Penitentiary in Leavenworth. This prompted the offer of a reward leading to the apprehension of those responsible and increased surveillance checks of shipping packages by the U.S. Postal Service and private courier agencies were implemented. [U.S. Diplomatic Security Service news photos, released.]

Letter bombs have existed for a long time and there have been intermittent news reports about them, but in less than two months during the winter of 1996, more than a dozen letter bombs disguised as holiday greeting cards were delivered to U.S. and U.K. recipients, prompting the U.S. Postal Service to change regulations regarding the submission of packages for posting. Packages weighing more than a pound could no longer be conveniently dropped in postal slots, but had to be handed directly to postal employees during business hours. The private courier companies also stepped up routine surveillance of shipping packages.

4.j. Society in Transition

Greater Awareness and The Struggle for Balance

The Internet has given the public the opportunity to exchange information and to organize lobbying bodies in a way that has never before existed in human society. Never have modern governments been more closely surveilled, never have they been more accountable for their actions, nor have they encountered so much resistance to activities that they may deem necessary for the safety and security of citizens and which they might have carried out with impunity and secrecy in previous administrations.

In 1993, U.S. Attorney Louis J. Freeh was appointed to the position of Director of the FBI.

In 1994, the U.S. established the *Civilian Career Management Program* (CCMP) which, in part, developed future civilian leaders for the Air Force intelligence community.

A number of government satellite imaging programs were declassified in 1995, increasing public awareness of aerial surveillance and creating an aura of general unease. A September 1995 memorandum from Daniel C. Kurtzer, Acting Assistant Secretary, Bureau of Intelligence and Research, to the Director of the NSA, J. M. McConnell, illustrates this struggle when the pursuit of security and privacy from different quarters of society shifts the balance:

> "In response to NSA's request for a community reaction to the NRO proposal that the "fact of" SIGINT collection from space be declassified, we have looked at possible ramifications from a foreign policy as well as an intelligence perspective. We believe that official confirmation could have undesirable repercussions in those countries where _ are located -- _ -- and that certain steps are necessary before reaching any decision on the NRO proposal.
>
> In the cases of _ we strongly recommend that the US initiate formal consultations on the NRO proposal. As you are aware, the _ _ _ _ _ _ _ press and public already have concerns about activities at _ and there are aperiodic [sic] allegations in the press that the Americans are monitoring _ _ _ _ _ _ _ communications. _ that government will be particularly sensitive to unfavorable speculation with regard to the _ _ _ _ _ facilities. The consultations could take place in intelligence channels, provided the Department has an opportunity to review the record correspondence in advance...."

Another significant struggle for power in the mid-1990s was the battle over computer encryption systems. When news of government proposals to restrict encryption and supply keys to the NSA were circulated over the Internet, the response from the public was swift, vocal, heated, and well-organized. The Internet was seen as a vehicle for a fundamental change in society. Before the Internet, the government would have been able to establish the proposed encryption restrictions and to provide access by law enforcement and national security agencies to certain communications with far less debate and revision. But electronic communications forged a different relationship between government and the voting public. The paternalistic structure, in which public officials were entrusted to do 'what was best' for those they represented, was shifting to a more decentralized structure, in which the public was demanding equal access, equal privacy, and more direct input into the drafting of legislative bills through electronic communication. This shift became even more apparent when the issue of encryption came up again five years later. (More about the encryption debate and the eventual outcome is included in the Cryptologic Surveillance chapter.)

The *Electronic Freedom of Information Act Amendments of 1996* became Public Law 104-231, thus amending the Act to provide for public access to information in electronic format. This action, along with a number of subsequent actions on the part of the U.S. Government, indicates an apparent trend to more openness in the late 1990s.

The Late 1990s - Reorganization, More Openness, More Surveillance

By the mid-1990s, Global Positioning Systems (GPS), which permit the precise pinpointing of a location through satellite technologies, were showing up in discount catalogs. These and other types of tracking devices were being used on prison inmates on parole or with limited movement privileges and were available for children or older people who might wander unattended. By the late-1990s, they were available for less than $200. Similarly, pinhole cameras and digital camcorders were dropping in price. Sophisticated surveillance devices had entered the mainstream of consumer goods.

The late 1990s was characterized by some remarkable changes in western society, stemming from the Internet and the greater openness of society in general. Changes in the media reflected these changes in society. Broadcast stations have always vied for 'ratings' (a measure of the number of viewers watching their shows). When ratings decline, broadcasters are sometimes willing to take greater risks. New spy devices made it possible to create a new genre of television programming called 'reality programming.' In this type of programming, real events and real people (as opposed to actors and scripts) are surveilled and recorded ('caught on tape'), often without the surveillee's knowledge. The results are broadcast to the viewing public either prerecorded or live. When the broadcast is live, it places an even higher level of risk on the producers.

A similar change has occurred in daytime TV, with talk shows gradually edging out many long-standing soap operas. Talk shows began to feature ordinary people instead of celebrities, another type of reality programming in which nonactors tell some astonishing stories. Coincident with the rise of 'real' TV has been intercommunication on the Internet in a no-holds-barred, 'truth'-oriented, uncensored forum in which the most intimate details are described in unprecedented detail for anyone with an Internet connection to read (or see).

The result of this enormous open exchange of information is that by the turn of the millennium, the number of 'taboo' subjects in North American society decreased and the sanctioning of personal and professional 'spying' on people's private lives increased. In other words, an individual might not like having his most private activities watched and recorded, but he didn't seem to mind other people's private lives watched and recorded if he could view it on TV or on the Internet. This double standard continues to pervade many decisions and policies about the use of surveillance devices.

A side-effect of the public appetite for open and honest information, coupled with general economic stability in the U.S., appears to have been a greater willingness, on the part of government, to reveal information that hitherto would have been kept quiet, even if declassified. This trend was evident in the early 1990s and became more apparent by the end of the decade.

In 1997 the *Openness Advisory Panel* was established within the U.S. Department of Energy (DoE) to provide advice regarding classification and declassification policies and programs as well as other aspects of the *Openness Initiative*. It further was tasked with public relations through:

> "An independent evaluation of all DOE policies and procedures relating to enhancing public trust and confidence in the Department and its programs, with special emphasis on classification, declassification and openness policies;
>
> ....
>
> ROLES AND RESPONSIBILITIES
>
> The Panel will focus on issues of primary interest to the public and on measures to ensure the Department remains responsive to public policy needs and continues to foster confidence with the public and the Congress...."

One example of this policy of 'openness' was the distribution of a 1998 organizational chart of the NSA Operations Directorate, a type of document that would previously have been kept secret. Such charts were not required to be released, even if unclassified, as per Public Law 86-36.

In some respects, 1998 was a banner year for the release of classified documents. The CIA alone responded to Executive Order 12958 by releasing more than a million pages of material, the largest amount ever declassified and released at one time.

In January 1998, The U.S. Energy Secretary, Federico Peña announced a reorganization of intelligence programs in the Department of Energy (DoE). The goal was to improve counterintelligence capabilities and coordination with the FBI and other law enforcement agencies. As a result, functions of the Office of Energy Intelligence were reformed into two new offices to ensure effective programs through the DoE complex and labs. Thus, foreign, local, and counterintelligence would now fall variously under the jurisdiction of the *Office of Intelligence* and the *Office of Counterintelligence*, both reporting directly to the Secretary and Deputy Secretary.

On 7 August 1998, U.S. embassy buildings in Kenya and Tanzania were devastated by terrorist bombs with the loss of many lives. On 20 August, the U.S. government launched missile attacks on installations in Afghanistan and the al-Shifa pharmaceutical factory, claiming it was being used for the creation of chemical weapons, a claim that stirred international controversy and is still being disputed.

In 1998, more than 100 U.S. overseas diplomatic posts were installed with surveillance detection programs, and more were planned, but the embassy bombings, along with previous terrorist bombings such as the World Trade Center in 1993 and the Oklahoma Federal Building in 1995, prompted a reappraisal of global U.S. security. In April 1999, diplomatic security personnel expressed concern about diplomats stationed or traveling abroad and made recommendations to Congress for increased surveillance and warning systems, to guard against car bombs and other similar terrorist attacks. Such changes would be subject to approval by the Overseas Security Policy Board chaired by the Director of the Diplomatic Security Service. The recommendations included, among other things, the installation of security lighting and cameras and other unspecified security items.

In June 1999, the President's Foreign Intelligence Advisory Board presented a report on security problems at the U.S. Department of Energy (DoE) titled "Science at its Best | Security at its Worst." Based on research and interviews, the Report described some of the persistent organizational and administrative security problems associated with the DoE, particularly with regard to nuclear weapons, some of which reflected policies and procedures and some of which reflected differences in philosophy and priorities. Openness and security are goals that do not always share an easy coexistence. The Board recommended some general organizational changes and specific changes related to "personnel assurance, cyber-security, program management, and interdepartmental cooperation under the Foreign Intelligence Surveillance Act of 1978."

The Internet, Global Surveillance, and Open-Source Information

The growth of the Internet is a milestone development in terms of changing the dynamics of global surveillance. Within a period of five years, the Internet community changed from a relatively small group of government, education, and computer network users, to a society of over 30 million (and growing) personal, commercial, and governmental users.

The very nature of the Internet changed dramatically during this period of growth. What was originally a military communications medium became a research communications medium and then evolved into a dominantly personal and business communications medium, with research occupying a smaller percentage in the gold rush for entrepreneurial niches. Investment brokerage and investor habits also changed dramatically as the availability of personal and business information and service sites expanded dramatically. Some examples of personal information that became open to the public which were previously difficult or awkward to obtain, include

- Voluminous personal genealogies of family relations, personal journals, and oral histories.
- Course catalogs from academic societies, course outlines, lecture notes, research findings, and conference proceedings.
- The balance sheets of public companies accessible through the Securities Exchange Commission in a manner that greatly increased their distribution over traditional methods; histories, goals, and product lines of businesses and not-for-profit agencies.
- The ideas, opinions, and information sources of individuals on USENET newsgroups.
- Reverse directories and public directories of almost everyone in North America with a phone number or address.
- Public records that were previously difficult to find or access could now be easily retrieved without having to physically travel to the county of origin to request a copy.
- Armed forces agencies' news photos and documents for broad distribution.
- Patent documents that were previously difficult to view or search without professional assistance.

This bonanza of information, originating mostly in North America and Western Europe, and to some extent, Japan, could now be downloaded in minutes by anyone, anywhere, with Internet access.

Changes in Communications Infrastructures

At the same time information sources were changing, many traditional methods of seeking and transmitting information were being superseded by electronic technologies. People were beginning to use digital Internet technologies to place long-distance telephone calls. Commercial satellites capable of providing high-resolution imagery were being placed in orbit. Computer graphics algorithms and displays were now used in many types of surveillance, including radar scopes, infrared imaging systems, satellite-interpretation programs, image and facial recognition programs, and 3D modeling of foreign territories (formerly crafted by hand in a CIA workshop for more than three decades).

Within the CIA, the *Directorate of Science and Technology* was assuming a greater importance with an increased emphasis on the gathering and processing of information through technology.

The age of easily accessed electronic open-source surveillance and computer imaging was in full swing by 1998.

Selective Security

International scandal erupted in northern Europe in 1997 when it was discovered that widely used computer correspondence and videoconferencing products purchased from U.S. vendors were not secure. A number of European government agencies and big businesses were using the products for sensitive communications, assuming that they provided 64-bit encryption. This wasn't true of all versions, however.

Because of U.S. software export laws, foreign-sold products had to be restricted to 40 bits, an encryption level that was easier to decode. In order to get around the export limitations some U.S. software vendors, like Lotus, shipped their products with 64-bit keys, but designed them so that 24 bits of the code were broadcast along with the message. The U.S. National Security Agency (NSA) was then supplied with the key to decode the 24 broadcast bits, making it much easier for them to decrypt the remaining 40 bits. Lotus initially expressed satisfaction with this solution, as it allowed them to sell products abroad while still satisfying export restrictions. Foreign purchasers were not so happy; the United States was the chief supplier of global commercial software programs and U.S. users were getting reasonably good encryption (64 bits), but foreign users were buying the same products and getting only limited encryption. Actually, in spite of the fact that it requires some fairly substantial computing resources to decrypt a 40-bit scheme, some people felt that 40-bit encryption was insecure enough to be termed 'data scrambling' rather than 'data encryption.' European users felt betrayed that they had not been explicitly informed of NSA involvement and the security weakness in their purchases.

This is just one example of growing concerns, on the part of the U.S. Intelligence Community, about how to curb illegal communications, and communications about illegal activities, which might affect U.S. national security. It is also an example of fears in some segments of society that U.S. Government intelligence agents might monitor private communications. The conflicts and debate were not immediately resolved and a few years later some surprising amendments were made to software export regulations.

Economic Espionage and ECHELON Revisited

Three years after the *Economic Espionage Act of 1996* was enacted, the FBI announced the conviction of foreign company members accused of stealing trade secrets from an Ohio manufacturing firm. The case began when Avery Dennison's own internal corporate surveillance turned up evidence of possible espionage and turned the investigation over to the FBI. The perpetrators were found guilty in April 1999 by a Federal Jury, thus becoming the first foreign company to be found guilty under the *Economic Espionage Act*.

By the late 1990s ECHELON rumors had attained folklore status on the Internet as a symbol of government use and abuse of surveillance technologies. By 1998, Internet users organized to 'fight back' against this as yet unconfirmed 'ear on the Net' by inserting politically volatile keywords in all their email messages, including *bomb, secret, Iran,* etc. The logic was that the government couldn't monitor everything and thus might be singling out sensitive documents for closer scrutiny by using keywords (it's reasonable to assume that there is selective filtering of data). By encouraging everyone to insert the conjectured 'hot' keywords into email, protestors intended to 'flood the spooks' with volumes of information too massive to process in order to subvert the surveillance system. Whether or not this grass roots protest was effective, it nevertheless illustrates that privacy advocates were concerned about the Big Brother implications of an extensive global surveillance net.

Even if ECHELON wasn't as pervasive as rumored, it brought to the foreground the fact that it was now technologically possible to mount a total global surveillance machine with wide-ranging powers of observation. By spring 2000, cable networks were running programs describing ECHELON as a top secret government project to monitor anything and everything that could be electronically seen or heard on the planet. This, in addition to the proliferation of video cameras in retail outlets, educational institutions, and voyeur sites on the Web, ignited a small, but vocal segment of the population to strongly scrutinize not just Big Brother but the burgeoning numbers of Little Brothers. As the year 2000 was ushered in, concerns about the incremental loss of personal privacy were voiced in increasing numbers, concerns that are not entirely unjustified.

Interdepartmental Cooperation and Public Input

The 1990s was a time of substantial social and technological change, but it was also a time when long-distance interdepartmental communication increased and specialized facilities for deploying new technologies were established.

It was not unusual for federal agencies to cooperate in the investigation of crimes, but the means to do so were not always readily available. The global Internet has been a key factor in interconnecting various law enforcement agencies. Multiple-state arsons, serial killings, and kidnappings are easier to solve if investigators discover a pattern of crimes in other jurisdictions and work together to solve them. The Internet facilitated this type of cooperation and the trend to share project information was increasing by the mid-1990s.

In November 1997, integration of various Department of Defense (DoD) departments such as the Polygraph Institute and the Personnel Security Research Center into the Defense Investigative Service (DIS) resulted in the creation of the Defense Security Service (DSS) to reflect its broader mission. The three primary missions of the DSS are personnel security, industrial security, and security education/training.

One example of effective interdepartmental cooperation was the *National Church Arson Investigation* established in June 1996, which involved the combined resources of several federal agencies. Another was the May 1999 agreement between the Bureau of Alcohol, Tobacco and Firearms (ATF) and the FBI to create the *National Integrated Ballistics Information Network* (NIBIN) *Board* to unify ballistics technology resources.

Left: The *Reference Firearms Collection* (RFC) aids the FBI in identifying firearms and their components. It provides a way to test and match firearms that might be associated with crimes. The *Standard Ammunition File* (SAF) is another collection maintained by the FBI, which includes whole and disassembled cartridges, shot wads, pellets, and other ammunition accessories, similar to those on the right, for study and comparison. [FBI Forensic Science Communications, released; Classic Concepts ©2000 photo, used with permission.]

Forensic scientists have helped law enforcement agencies for many years in the identification of ammunition and firearms that are linked to various crimes and now computer systems are helping as well. The ATF maintained an Integrated Ballistics Information System (IBIS) and the FBI maintained the DRUGFIRE system which were brought together in 1999 to establish a comprehensive computer database of cartridge case and bullet images. The system is capable of searching almost a million images for a match, using evidence associated with a crime.

Another example of cooperative use of database identification techniques went into effect November 1999 when the *National Instant Check System* began processing background checks on people seeking to purchase firearms. About half the states began participating, with the other half handling their own checks. It was found that about 10% of the people applying for the firearms had outstanding warrants for arrest on a variety of charges. The computerized database system was developed through a cooperative effort between the FBI and the ATF and state and local enforcement agencies. Gun dealers could access the information in the system by personal computer or telephone inquiry.

In December 1999, the ATF began ground-breaking activities for a new National Laboratory Center, a complex of three labs, the ATF Alcohol Laboratory, the ATF Forensic Science Laboratory, and the Fire Research Laboratory. These labs provide a variety of investigative services including chemical surveillance, biometrics, explosives analysis, and various physical and instrumental analyses.

Another interesting foray into new strategies and alliances occurred in 1999 when the CIA established *In-Q-It*, a venture capital firm to fund promising Internet-related technologies in an effort to continue to try to attract high-caliber expertise to the service. The director was a Silicon Valley entrepreneur who earned his money and reputation creating video games. The connection between the CIA and video games is not as distant as some might think. Simulations have always been a valuable tool of intelligence-gathering and strategic planning and video games require fast, multiple-media resources beyond those of almost any other type of computer application: capabilities that are relevant to many types of visual and electronic surveillance.

In March 2000, the FBI announced that it had cooperated with Canada and Wales in bringing about the arrest of two 18-year-old males accused of international cybercrimes, associated with losses estimated to exceed $3,000,000. Banking and credit card companies also cooperated in the apprehension of the two young men.

Meanwhile, as cooperative alliances were being explored and tested in the U.S., satellite surveillance cooperation on an international scale was being critically scrutinized from some quarters, as well as turning up in news headlines.

Domestic and Foreign Concerns Regarding ECHELON

By March 2000, concerns about ECHELON had received worldwide attention and the international community began taking measures to sort out the truth from rumors through official channels. The European Parliament was scheduled to discuss these matters in April 2000 with plans to mount a commission to inquire into ECHELON-related activities, to more fully understand the role played by the United Kingdom, Denmark, and Germany (members of the European Union), in cooperation with the United States.

Demands from the public, both at home and abroad, included inquiries into rumors of ECHELON surveillance of nongovernmental humanitarian organizations and large overseas aerospace contractors. In response, in April 2000, the NSA and the CIA reported to the House Intelligence Committee, explicitly denying accusations of surveillance of ordinary Americans or of industrial espionage to benefit U.S. firms.

There is nothing surprising about this sudden attention on U.S.-related alleged surveillance activities. It is indeed true that the U.S. and other nations have been increasing their surveillance capabilities over the last several decades and that the U.S. has been involved, with a number of foreign allies, in various conflicts and peacekeeping activities. As a wealthy superpower, the U.S. is in a superior economic position to use the latest in electronic devices. As a nation with many world-class scientists, the U.S. is able to experiment with new technologies and techniques with relative freedom.

Thus, economic/scientific factors at the present time favor the U.S. as one of the dominant technological forces in surveillance technologies. American social factors also tend to further the proliferation of 'spy' technologies. The American public is humane and caring, but doesn't always have an in-depth understanding of the needs and concerns of people in foreign nations. Americans are also fiercely competitive and there are many who take for granted the democratic freedoms, and wealth of resources and technology, that have been given to us from birth. These social factors may influence national policies and security activities in such a way that other countries may justifiably take issue with how we use surveillance technologies.

With new technologies there is always the 'temptation of opportunity' in which a technology put into use in good faith for one purpose may be used by unscrupulous individuals for another. Policing from within is as important as policing from without.

ECHELON has become a symbol and a focus for concerns over the growth and deployment of global surveillance technologies. The international furor that is emerging may continue for some years until international checks and balances are established and sorted out. While this process continues, it is equally important that the use of surveillance technologies by private citizens and corporations be examined for their potential benefits and their potential to erode personal privacy and freedoms. It is the intent of this book to further the understanding of the prevalence and capabilities of these technologies so that informed choices and policies can be developed to serve everyone's needs.

5. Descriptions and Functions

This introduction does not seek to duplicate the descriptions of individual technologies included in each chapter, but there are some general procedures that are common across a variety of surveillance devices that are summarized here.

Scene investigation involves surveillance that is confined to a particular area. Surveillance technologies including ground-penetrating radar, magnetometers, cameras, plaster casting, and fingerprinting are often used to investigate a scene. Scene investigation is used in archaeology, wildlife conservation, civil disputes, accident evaluations, insurance claims, arson, and other crime scene investigations.

Crime Scene Investigation

Crime scene investigation is an important aspect of surveillance. Arsonists are often caught because they hang around to watch the firefighters battling the blaze, thieves sometimes strike the same business or home multiple times, and clues at a crime can lead to the apprehension of the criminal(s).

Crime scene investigation involves demarcating the scene, protecting the integrity of the area from contamination or disruption, recording the scene, searching for clues, and 'picking up' the clues in whatever way is appropriate. It then involves lab analysis, deduction, and cooperation with everyone involved in the process. In cases of arson or homicide, it may also involve monitoring the site from a distance to see if any suspects are lingering near the scene of the crime.

Crime scene investigators are often dismayed by destruction and contamination of important clues. Footprints get trampled by bystanders, associates, or even by law enforcement agents themselves. Fingerprints become contaminated, items associated with the crime are moved, removed, or lost. Most of the time these actions are accidental, though, sometimes they are deliberate.

Members of the *Bureau of Alcohol, Tobacco, and Firearms* (ATF) utilize a fleet of *National Response Team* (NRT) vehicles equipped to support arson and explosives investigations. Here, ATF agents sift through the debris at the scene of a fire looking for evidence of arson. Canine assistants are sometimes used to sniff out explosives or accelerants. The ATF cooperates with other law enforcement agencies in federal investigations involving alcohol, tobacco, and firearms. [ATF news photos, released.]

Archaeological Investigation

Archaeological surveillance of a dig site shares many similarities with the investigation of a crime scene (and archaeologists are sometimes called to aid criminal investigators). Demarcation of the site and its protection from treasure-hunters or vandals are usually established first. Concerns about disturbing ‘evidence’ or contaminating a site are similar to those of law enforcement agencies investigating a crime scene.

Tape (or string) is now commonly used to mark a crime or anthropological/archaeological study site. The area may also be marked out into a grid for precise location. If there is concern about theft or vandalism, security guards or electric fences are sometimes established.*

To search a site, many electronic devices are now available. Ground-penetrating radar and magnetometers can provide information about underground objects (and prevent unnecessary digging or disturbance of the site). Geographic Positioning System (GPS) devices can show latitude and longitude. These types of devices are described in subsequent chapters.

Technology has made it possible to glean volumes of information from minute pieces of evidence but now, more than ever, it is important not to contaminate a scene. Gloves are routinely worn and face masks and body suits may also be worn to reduce falling hair and skin from the investigators, particularly if sensitive DNA-profiling techniques are used on trace amounts of blood or hair. Environmental suits may also be worn to safeguard the examiners in the case of hazardous or hostile situations. Environmental suits are described in the Visual Surveillance chapter and biochemical clues are discussed in the Chemical & Biological Surveillance and Genetics Surveillance chapters.

6. Applications

Surveillance technologies are of no use until they are applied toward a specific goal or task. Each chapter includes a section on applications which provide insight into how surveillance technologies are commonly used and who uses them. It isn't possible to include all the possible uses for every case, but there are enough to provide you with a better understanding of the common applications. Included here are some of the more generic aspects.

*In one of history's twists of fate, the famous Pinkerton agency recently supplied site security at an investigation scene when the alleged remains of Jesse James were exhumed to see if a positive identification could be made through DNA technology. Ironically, the notorious criminal was never apprehended by Pinkerton's Detective Agency in the 1880s, despite many attempts.

6.a. Search and Rescue

Surveillance technologies are essential tools in search and rescue operations. When searching for individuals lost in lakes, oceans, avalanches, and forests, where hypothermia and hunger can claim a life in a very short period of time, technology can make a difference. Surveillance devices are also used in investigations and to find people and animals when buildings collapse from bombings or earthquakes.

Surveillance devices serve many roles in search and rescue. In disasters such as hurricanes and floods, surveillance devices not only help in finding victims, but can help assess the scale of a disaster, determine the character or status of chemical leakages, assess what it might take to rebuild a region, and aid insurance adjusters in surveying the damage and providing relief. They can be used further to predict and warn citizens of impending danger. Infrared detectors, radar, satellite images of terrain, radio sets, and tracking beacons are all examples of technologies that can aid in relevant prevention, lifesaving, and administrative activities.

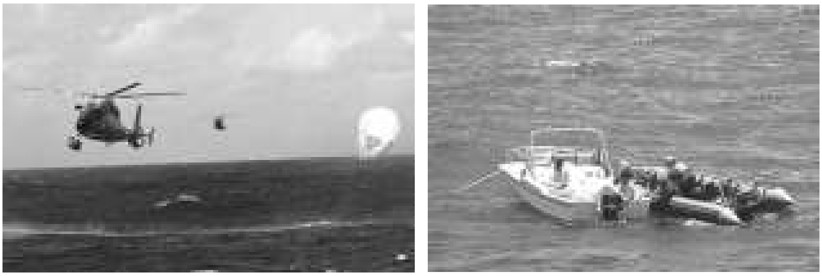
The U.S. Coast Guard is an organization that participates regularly in search and rescue operations using both air and marine vessels.

Left: Surveillance technology is only useful when combined with good strategies. Here LtJG Steve Rutz, a controller with the Coast Guard Command Center in Juneau, is shown plotting a search pattern for a missing sailing vessel in January 1998. Right: C2PC, a computerized global command and control system, being used by Pearson and Behner to plan a search. The C2PC is also used for law enforcement activities. [U.S. Coast Guard news photos by Mark Hunt and Chuck Wollenjohn, released.]

Left: A burning fishing vessel from which the U.S. Coast Guard rescued five men and a dog off the coast of Unimak Island. Right: Coast Guard members assist a pilot and five tourists at the site of a helicopter crash from a ‘white-out’ on the Herbert Glacier near Juneau, Alaska. The search team brought food, shelter, and survival gear to help the stranded victims make it through the night. [U.S. Coast Guard news photos by USCG and Mark Hunt, released.]

In the U.S., in 1989, the *National Urban Search and Research* (US&R) Response System was formed under the authority of the Federal Emergency Management Agency (FEMA). FEMA provides a framework for local emergency services to aid victims of structural collapse. The members of the Task Force come from many disciplines. They include hazardous materials experts, structural engineers, search specialists, highly trained dogs, medical practitioners, and pilots. All of these specialists use surveillance technologies of one type or another in their work.

Examples of search and rescue technologies are covered more fully in the Sonar, Light, Aerial, and Animal Surveillance chapters. DNA identification of remains is described in the Genetics Surveillance chapter.



Left: Balloonists attempting to circle the Earth crash into the Pacific Ocean halfway through their journey. Search and rescue helicopters travel to the site from Air Station Barbers Point in Hawaii. Right: Coast Guard cutter crew members rescue three sport fishers adrift in a disabled vessel in eight foot seas near the island of Kauai. [U.S. Coast Guard news photos by Marc Alarcon and Eric Hedaa, released.]

6.b. Border Patrol

Border patrol is an important aspect of national security in every nation. Customs and immigration officials seek to prevent abuses of trade laws and human rights and the transport of hazardous materials, plants, and weapons. To achieve these aims, they regularly use a variety of surveillance devices.

The technology in customs and immigration administration is becoming increasingly sophisticated. Infrared sensors, aerial surveillance, and X-ray machines have been used for some time, but high-resolution cameras, electronic databases, and intelligent recognition software (now available) will begin to play dramatic roles when they are incorporated into future border surveillance.

By the end of the 1990s, cameras were installed at many of the Mexican and Canadian border stations. Cameras like these can be connected to computers to monitor when and how often specific vehicles or people cross the border and can alert border officials about unusual patterns or activities. The patrolling of borders away from the crossings is a greater challenge and technologies like aerial surveillance and infrared imagery can be used from airplanes, helicopters, and unstaffed aerial vehicles on or over land or sea. Some of these are used now and some may be added in the future.

Marine patrols are also benefiting from improved sonar and remote-controlled marine and aerial vehicles which greatly extend the surveillance 'reach' of patroling vessels. Marine surveillance helps protect endangered species and prevents poaching or abuses of commercial fishing licenses. It also aids in search and rescue operations and stems the flow of smuggled goods and refugees.

The human cargo trade, in which refugees pay up to $60,000 per person to be transported, in unsafe ships or containers, is of great concern to authorities. The refugees often die or succumb to illness due to lack of food and sanitation and they often bring diseases like tuberculosis and hepatitis into the country of illegal entry. Customs and immigration officials have stepped up their surveillance of tankers or containers that may contain human contraband. Sonar, X-rays, infrared sensors, cameras, and dogs are just some of the surveillance technologies now regularly used to detect border-runners and refugee claimants.

Left: An illegal alien found on board a fishing vessel by the Coast Guard is turned over to the U.S. Border Patrol. Various law enforcement agencies often cooperate in various operations, especially those involving smuggling, trafficking, or border-running. Right: Cuban refugees rescued from an unseaworthy homemade boat near the coast of Miami Beach, Fl. [U.S. Coast Guard 1999 news photos by Keith Alholm and Chris Hollingshead, released.]

6.c. Natural Resources Management and Protection

Left: Coast Guard members discuss tactics for searching fishing vessel spaces in 1990. Illegal fishing methods, catches, or contraband are sometimes found by the Coast Guard on routine checks. Right: A fish catch is inspected during a routine 1993 Coast Guard fishery patrol. Fishing vessels are also checked for compliance with regulations and minimum safety standards. [U.S. Coast Guard news photos by Robin Ressler, Ron Mench, released.]

The protection and management of natural resources, whether or not they are food sources, are an important aspect of a nation's cultural and economic survival. Surveillance strategies and technologies are used to monitor commercial harvesting, wildlife ecology, and poaching activities throughout the world. Without these protections, our resources might soon be completely depleted, as has happened in the past in unregulated areas. DNA-monitoring, radio-collar tracking, sonar, and optical surveillance are examples of technologies that are used regularly to monitor natural resources and those who seek to abuse them.

Coast Guard crew members are successfully able to disentangle a humpback whale from a lobster trap. Humpback whale populations were on the endangered species list when their population dropped to only about 12,000 surviving in the world; in human terms, that's barely enough to populate one small town. Several surveillance technologies, including radio tracking beacons and DNA matching, are being used in wildlife management and protection. [U.S. Coast Guard 1999 news photo by Brent M. Erb, released.]

6.d. Drug Laws Enforcement

Surveillance technologies are widely used by law enforcement agencies to uncover illegal activities such as drug manufacture and distribution. Infrared sensing, power-consumption monitoring, phone tapping, aerial photography, chemical sniffers, and canine scouts are all used to identify individuals, facilities, and vessels used in the drug trade.

Bails of marijuana were found hidden below decks on a fishing vessel inspected by the U.S. Coast Guard. [U.S. Coast Guard News 1997 news photo, released.]

Sometimes illegal drug-related suggling is discovered in the course of other activities, such as rescues from fire or violence indirectly related or unrelated to the drug activities. In these cases, several agencies may be involved in the search and seizure of drug caches and paraphernalia.

As an example of the accidental discovery of contraband drugs, the U.S. Coast Guard and the Mexican Navy responded to a fire onboard the vessel "Valera" off the coast of Mexico, in January 2000. The members of the Valera had abandoned ship and were rescued from the water by a small Coast Guard boat. While investigating the cause of the blaze, over three metric tons of cocaine were discovered and seized from two large compartments aboard the vessel. Cocaine is one of the more common drugs smuggled across maritime borders between Mexico and the United States.

Once found, various methods are used by different agencies to determine the chemical makeup of suspected illegal drugs. Most enforcement agents are trained to make a preliminary guess by visual inspection, smell, and sometimes taste. Portable kits are available to assist in preliminary analysis and generally larger samples are then sent to a lab for confirmation or more extensive analysis in the case of mixed samples or blended drugs.

6.e. National Intelligence Agencies

In 1992, Robert Gates, the Director of the Central Intelligence Agency (CIA), established an Office of Military Affairs in order to create a closer connection between the CIA and other members of the intelligence community. The main goal of this alliance was to provide intelligence that would enhance awareness during conflicts, particularly on the battlefield. The CIA gathers imagery and information from signals (radar, sonar, etc.), processes the information (e.g., through simulations) and provides it to battlefield commanders. The gathered data may include constant weather updates and continuous surveillance of the battle environment. John Deutch, Director of the CIA, in June 1995 stated "if the enemy does not have similar information, it means that victory will come more rapidly and therefore the casualties will be lower." Plans were in effect at the time to create a "national imagery agency" to serve in the collection, analysis, and distribution of intelligence imagery.

6.f. Commercial Products

Each chapter in this book includes a section on some interesting or representative commercial products and lists volume and price information on some.

Any commercial products listed are included for informational purposes only. Their inclusion does it imply an endorsement of the quality of their products or services. The included examples are intended as educational examples only, to provide an introduction to the types of products that may be purchased on the market as they relate to individual topics.

The following products are those of general interest to the topic of surveillance technologies; specific technologies are listed in individual chapters. In general, surveillance product vendors tend to fall into five main categories: personnel services (trained security officers equipped with surveillance skills and devices), training services (instructors and computer simulators), research and development services (firms that create and test new technologies), manufacturing services (firms that build products), and distribution services (firms that distribute and sell products).

Advanced Paradigms Inc. - Applications development, communications and training to federal agencies and commercial organizations. API has a number of prominent clients in the federal government and technology industries.

Alliant TechSystems - Markets to military, law enforcement, and the security industry. Products include quick-reaction products and high-speed cryptography.

Analytical & Research Technology Inc. - Systems development and integration. Provides the intelligence community with hardware, software, and integration services for data handling.

Applied Signal Technology - Designs and manufactures signal-processing equipment for a wide variety of telecommunications sources. The equipment is used for foreign signals reconnaissance by government and the private sector. Incorporated in 1984. Each office has a government-approved facility clearance.

Cloak and Dagger Books - A specialized bookstore with volumes on many aspects of intelligence, including military history, counterintelligence, codes and ciphers, espionage, and more. Bedford, New Hampshire.

Executive Intelligence Services - (EIS) An investigation company specializing in research and surveillance in workers' compensation, personal injury, fraud, and medical malpractice.

Executive Resource - A competitive intelligence consulting firm based in Montreal, Canada which provides corporate intelligence/strategic planning training and coaching services. Executive Resource also supplies a by-subscription online news journal, Competia Online.

Loyal Security, Inc. (LSI) - Leading-edge products for law enforcement, including access control, training, security consulting, counterintelligence, videoscopes, infrared illuminators, electronics belt-packs, and head-mounted displays. Based in North Carolina.

Mega Worldwide, Inc. (MWI) - A group of international companies which specialize in fields of high-threat security. MWI provides specialized equipment, training, and investigations services to state, federal, and foreign governments with experts in more than 50 countries.

National Security Archive - Microfiche and written publications based on declassified and unclassified government documents and scholarly research associated with these documents. Some of these are of general interest, some of academic interest, and some are priced for the library market.

Pacific-Sierra Research Corp - Founded in 1971 to carry out applied research. It markets to various defense and intelligence agencies and foreign and domestic clients. Primarily information technology, high-performance computing, software development, and submarine communications. Employee-owned.

The TEAL Team, Inc. (TTT) - Advanced security training and consulting in high-risk security tasks. Services are aimed at governments, law enforcement units, emergency response units, and large corporations. TTT claims that the staff includes senior experts drawn from organizations such as the Secret Service, FBI, SEALs, etc. Based in New Jersey.

In the surveillance industry, there are also 'shadow' organizations that are often loosely affiliated with large contractors, but which keep a low profile. These companies typically market covert services and technologies.

7. Problems and Limitations

Each chapter in this book has a section on problems and limitations that are specific to the technologies discussed in that chapter.

8. Restrictions and Regulations

The more relevant or interesting legal issues related to particular technologies are summarized in each chapter.

Some issues of general interest with regard to surveillance, information access, and privacy are described here. This is a sampling, it is in no way complete, and those seeking further information are encouraged to consult government and public legal archives on the Internet and in local libraries. (See also the Cryptologic Surveillance chapter for computer-related legislation.)

Freedom of Information Act (FOIA). USC, Title 5, Subsection 552. Enacted by the U.S. Government in 1966 to provide individuals with the right to request access to information or records held or controlled by federal executive branch agencies upon submission of a written request. The Act stipulated nine exemptions and three exclusions. The exemptions generally cover issues relating to physical and financial security including national defense and foreign relations, inter/intra-agency communications, internal rules and practices, trade and financial secrets, law enforcement investigative information, and geological information on oil wells. The FOIA "does not apply to Congress, the courts, or the immediate office of the White House, nor does it apply to records of state or local governments." Most states enacted FOIA-type statutes which can generally be queried by writing to the state Attorney General. FOIA requests must be made in writing to the relevant federal agency. Search fees typically range from $10 to $30/hour plus copying fees with the first two hours of search and 100 pages of copying not charged for noncommercial requests. Response is up to 10 working days.

Privacy Act. Public Law 93-579. USC, Title 5, Subsection 552a. The U.S. Government acknowledges that it compiles federal records on individuals, including taxpayers, people in the military or employed by federal agencies, and those who receive social benefits such as student loans or social security. In response to this, in 1974, the U.S. Congress passed the Privacy Act to establish "certain controls over what personal information is collected by the federal government and how it is used." The act guarantees three rights to U.S. citizens and lawful permanent residents:

"1) the right to see records about oneself, subject to the Privacy Act's exemptions;

2) the right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete; and

3) the right to sue the government for violations of the statute, including permitting others to see your records, unless specifically permitted by the act."

The Privacy Act further establishes certain limitations on agency information practices and prohibits agencies from maintaining information describing "how an individual exercises his or her First amendment rights" unless there is consent or a statute permitting it or it is "within the scope of an authorized law enforcement investigation."

Like the Freedom of Information Act, the Privacy Act pertains to U.S. citizens and legal permanent residents and has certain exemptions which permit agencies to withhold information. The exemptions generally relate to information that could compromise national security or criminal investigations or which would identify a confidential source. Privacy Act requests must be made in writing to the relevant federal agency. Search fees are not charged, but copying fees may be charged. The response time is up to 10 working days.

Foreign Intelligence Surveillance Act of 1978 (FISA). Public Law 95-511, 50 USC §1805 (expanded in 1994), signed by President Carter. This Act establishes the procedures for an authorized government official to acquire a judicial order to authorize electronic surveillance or physical search in foreign cases. Probable cause must be shown that the target is associated with a foreign power and the surveilled premises are being used by the foreign power. Certain acquisition and disclosure requirements must be met. The Foreign Intelligence Surveillance Act Records System (FISARS) is the information system for FISA applications. Access to FISARS is restricted to personnel with TOP SECRET/SCI (Sensitive Compartmented Information) clearance with the Office of Intelligence Policy and Review (OIPR). The OIPR is not an investigative department, but rather a system for managing information received from the Intelligence Community.

Intelligence Oversight Act of 1980. Following allegations of wrongdoing by U.S. intelligence agencies, two committees were established, the Senate Select Committee on Intelligence (SSCI) in 1976 and the House Permanent Select Committee on Intelligence (HPSCI) in 1977. These, along with the Armed Services and the Foreign Relations and Foreign Affairs Committees, were to oversee and authorize the activities of the intelligence agencies. The Hughes-Ryan Amendment required that covert action notifications be given only to the two intelligence committees (other committees no longer had to be notified).

United States Intelligence Activities, Executive Order 12036, 24 January 1978. Signed by President Carter. This revoked Executive Order 11902 of 2 February 1976. It reorganized the intelligence structure and provided guidelines on the execution of intelligence activities. The Director of Central Intelligence (DCI) was given increased management authority over the Intelligence Community. The Secretary of Defense was designated to be the Executive Agent for Communications Security and the Director of the NSA was to execute the responsibilities for the Secretary of Defense. Senior officials of each agency were to report violations to the Attorney General.

Executive Order 12333, 4 December 1981. Signed by President Reagan. "Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available...." The Order describes goals, direction, duties, and responsibilities of the national intelligence effort to provide information to the President, the National Security Council (NSC), the Secretaries of State and Defense, and other Executive Branch officials. The Director of Central Intelligence is made responsible directly to the President and the NSC and duties of the CIA are put forth. The Department of Defense, Secretary of Defense, Department of Energy, and the Federal Bureau of Investigation (FBI) responsibilities are put forth. The Order further describes the execution of intelligence activities.

Intelligence Identities Protection Act, 23 June 1982. Signed into Public Law 97-200 by President Reagan. This imposed criminal penalties on anyone who wrongfully divulged the identities of covert intelligence personnel ("undercover intelligence officers, agents, informants, and sources"). In 1984, the President exempted the CIA from the search and review requirements of the Freedom of Information Act with respect to sensitive files through the Central Intelligence Agency Information Act of 1984.

Department of Defense Surveillance Countermeasures Survey Program, 23 May 1984. This is a Department of Defense (DoD) Instruction to update policies, responsibilities, and procedures for Technical Surveillance Countermeasures (TSCM) services which are included within the Defense Investigative Program.

Intelligence Organization Act of 1992. Organizational guidelines established by Congress for the Intelligence Community. This is one of the most significant Acts since the National Security Act of 1947. The oversight committees that had been established by the Intelligence Oversight Act of 1980 introduced intelligence reorganization bills leading to this Act. This basically established the actions the DCI had been taking to restructure the Intelligence community since 1980, establishing a legal framework, recognizing the DCI as the statutory adviser to the National Security Council and establishing the National Intelligence Council as the authority for intelligence analysis. It further defined the composition of the Intelligence Community.

Classified National Security Information, Executive Order 12958, 17 April 1995. A reform of the U.S. Government system of secrecy to create a uniform system for classifying, safeguarding, and declassifying information related to national security while supporting progress through the free flow of information. Sets out classification levels, standards, associated markings, guidelines for review, and associated authorities. Interpretation authority rests with the Attorney General. Signed by President Clinton. 12958 revokes 12356; it was later amended by EO 12972 (1995) and EO 13142 (1999).

Executive Order 12968, 2 August 1995. Describes access to classified information, financial disclosures, etc., which includes definitions, access eligibility, nondisclosure requirements, types of documents and reports that fall under this Order, and financial disclosure, including disclosure of codes and cryptographic equipment and systems, use of automated databases, access eligibility policy and procedure, standards, implementation, and general provisions.

Electronic Freedom of Information Act Amendments of 1996. Public Law 104-231. Established requirements for making information falling within Freedom of Information Act (FOIA) guidelines electronically available.

Economic Espionage Act of 1996. Public Law 104-294. A vehicle for prosecuting those who are found to be engaged in economic espionage, that is, the stealing of trade secrets and other business information. (Note that a war-related Espionage Act was enacted in May 1918.)

National Information Infrastructure Protection Act of 1996. Amends USC Title 18, the Computer Fraud and Abuse Act, to protect proprietary economic information. This amendment is Title II of Public Law 104-294 (see previous citation). It has important ramifications for 'computer hacking.'

Presidential Decision Directive No. 61 (DoE declassified version). A February 1998 restructuring Decision to form two independent intelligence offices within the Department of Energy (DoE), new counterintelligence (CI) measures, and a stronger cooperative relationship between the DoE and the FBI. Other measures include improved threat and vulnerability assessment and oversight and performance assurance. Coordination is provided by the National Counterintelligence Policy Board (NACIPB).

Act to Combat International Terrorism. Public Law 98-533. This in part establishes the Rewards for Justice Program in which cooperating individuals may be financially rewarded and/or relocated for providing information leading to the prevention of terrorism or the arrest and conviction of terrorists. This program is handled by the Diplomatic Security Service (DSS) of the U.S. Department of State.

United States Title 50 - War and National Defense, Chapter 36 - Foreign Intelligence Surveillance. This chapter covers electronic surveillance authorization, designation of judges, court order applications, order issuance, use of information, reports, criminal sanctions, civil liability, and authorization during time of war.

The law-making process is often slow, requiring three or more years for definitions and priorities to be sorted out before they pass through all the bureaucratic hurdles. In addition to general administrative and organization measures, there are also periodic acts and bills associated with funding, including

Intelligence Authorization Act for Fiscal Year 1995, 14 October 1994. Public Law 103-359. This established a Commission on the Roles and Capabilities of the U.S. Intelligence Community who were to review and report on the efficacy and appropriateness of activities of the U.S. Intelligence Community by March 1996. Periodic authorization acts establish spending priorities and allocations for intelligence-related matters.

FY2000 Intelligence Authorization Bill. Budget appropriations for the fiscal year 2000 for U.S. Government intelligence-related activities. Similar to the above in that it is a periodic funds authorization act.

9. Implications of Use

Information on history, prices, and types of devices is useful, but not really complete unless the impact of the use of the technologies is also discussed, even if only briefly. Each chapter has a section which describes some of the social consequences and trends related to the individual categories of technologies that can provide a focus for thought and further discussion.

This book is about exciting new technologies that fulfill a range of political and social needs and, if used judiciously, can improve our quality of life. However, it is hoped that our increasing dependence on electronic devices doesn't completely supersede traditional methods (including common sense) because nothing is invulnerable to attack.

A large predator, like a lion, doesn't have to fear smaller, weaker animals in its home range, but the large predator is the first to die if its range is diminished or food sources become scarce. The same vulnerability applies to electronics societies. Computers and surveillance devices might give Western nations an immediate political or economic advantage, but it also makes them extraordinarily vulnerable to electronic dependence and electronic attack. A high-energy radio-frequency (HERF) 'bomb' can instantaneously disable dozens or thousands of electronic devices with a concentrated burst of radio waves. Imagine the impact that could potentially have on a fully automated infrastructure. Such a threat could completely disable computerized power grids, transportation systems, and financial establishments. This isn't science fiction, it isn't even really high tech; such a terrorist weapon currently costs less than a few thousand dollars to build and terrorists aren't going to seek FCC approval before using it.

Another important aspect of surveillance is increased use of viewing and recording devices by citizens and the newsmedia, sometimes with offers of financial rewards for those who submit graphic and sensationalist examples. One of the consequences of 'reality programming,' broadcasts based on the experiences of nonactors, detectives, law enforcers, search and rescue personnel, and others, is that the public gains a better understanding of how our society and our public safety systems work. One of the negative consequences is that the families of loved ones who are brutally killed in murders or kidnap attempts or who have died from terrible falls or accidents practically have to stop watching television and using the Internet or they find themselves enduring an extended mourning period in which wounds may be opened again and again when someone unexpectedly replays the graphic events.

Since gruesome and explicit images of victims are now broadcast with increasing frequency, families who thought they had buried their loved ones and come to terms with the deaths sometimes find themselves reliving horrific events without warning. A viewer rarely knows when the images are going to be aired because the original videographers often license the footage to other broadcasters. Repeat airings can be painful and, in some cases, cruel. The definition of 'news' versus 'reruns' should be re-evaluated and the consequences to surviving families should be considered when capturing and airing surveillance videos.

There should be some public discussion as to whether the news media are justified in replaying these events or selling them to outside non-news broadcasters without permission from the victims or, if they are deceased, from their immediate families. The material may fit the definition of 'news' the first time it is played in association with the event, but it can be argued that *replays* are no longer news (especially when they are licensed out to third parties). This is arguably commercial exploitation, a means of using unpaid 'actors,' which should require the permission of the families and compensation for repeated broadcasts, just as actors get 'residual' payments for reruns.

Technological devices are rarely inherently good or bad. Like other tools, what matters is how we use them. In the race for electronic superiority, it is hoped that the important ethical ramifications of using surveillance technologies will not be overlooked, since they form the basis for electing our representatives, safeguarding our freedoms, and enhancing and maximizing our quality of life and interactions with others.

This book is intended to provide a balanced view of complex issues, both bad and good, and a sampling of practical examples of interest, in order to broaden our understanding of surveillance. Good raw materials aid good decision-making, now and for the future.

10. Resources

10.a. Organizations

Each chapter has a section listing organizations of relevance to that particular category of technology. In addition, here are some references of general relevance to surveillance technologies and intelligence-gathering. No endorsement of companies is intended.

Advanced Technology Office (ATO) - Created as a result of a DARPA reorganization, ATO focuses on 'high payoff' maritime communications, early entry, and special operations. Communications projects include superconducting filters and secure large-scale wireless networks and mobile systems. http://www.darpa.mil/ato/

Air Force Foreign Technology Division (FTD) - One of several intelligence divisions in the U.S. Air Force, along with the Office of the Assistant Chief of Staff, Intelligence, the Air Force Intelligence Support Agency, the Air Force Electronic Security Command, and the Air Force Technical Applications Center. Originally established as the Foreign Data Section in 1917, the FTD publishes a regular bulletin.

Air Force Intelligence, Surveillance, and Reconnaissance (ISR) - Ensures U.S. military information superiority in partnership with other military services and national intelligence agencies. The U.S. Air Force operates a variety of ground sites and airborne reconnaissance and surveillance platforms around the world. Managed by the Director of Intelligence, Surveillance, and Reconnaissance which also handles the AIA. http://www.cia.gov/ic/afi.html

American Civil Liberties Union (ACLU) - A prominent, nonpartisan individual rights advocate providing education on a broad array of individual freedoms issues in the United States. Founded by Roger Baldwin in 1920, the ACLU seeks to assure preservation of the Bill of Rights which is associated with the U.S. Constitution. http://www.aclu.org/

American Institute of Physics (AIP) - Founded in 1931, the AIP has over 100,000 members worldwide in all branches of physics. AIP publishes a number of professional journals (*Acoustical Physics, Applied Physics Letters, Virtual Journal of Biological Physics Research, Computers in Physics, Computing in Science and Engineering, Journal of Applied Physics, Journal of Biomedical Optics, Journal of Electronic Imaging, Optics and Spectroscopy,* etc.) and provides searchable online access for subscribers. http://www.aip.org/

Army Intelligence Agency (AIA) - Established in the mid-1980s by the Assistant Chief of Staff for Intelligence to direct scientific (nonmedical), technical, and general intelligence. It was originally a counterintelligence and HUMINT agency which was rolled into the Intelligence and Security Command (INSCOM) in 1977 to unify intelligence services in the Army. It was then separated out again, but INSCOM reassumed command of the AIA in 1991. It was then discontinued and INSCOM created the National Ground Intelligence Center from the remaining Army units. See next listing.

Army Intelligence and Security Command (INSCOM) - A major operational intelligence agency of the U.S. Army, established in 1977 from the Army Security Agency (ASA), which dates back to 1930. INSCOM conducts intelligence and information operations in multiple disciplines for U.S. military commanders and national decision-makers. The organization also conducts a variety of production activities, including imagery exploitation, intelligence battlefield preparation, and science and technology intelligence production. It further engages in counterintelligence and force protection, electronic and information warfare, and support to force modernization and training. The European arm is located in Griesheim, Germany. http://www.vulcan.belvoir.army.mil/

Association of Former Intelligence Officers (AFIO) - AFIO is a nonprofit, nonpolitical educational association founded in 1975. Members comprise intelligence professionals engaged in promoting understanding of the role and functions of U.S. intelligence activities. AFIO publishes the journal *Intelligencer* and *Weekly Intelligence Notes* (WIN). http://www.afio.com/

Association for Crime Scene Reconstruction (ACSR) - Founded in 1991 to provide support to law enforcement investigators, forensic experts, and educators in the understanding of a crime scene, its reconstruction, and the gathering and preservation of evidence. http://www.acsr.com/

Atlantic Intelligence Command Joint Reserve Intelligence Program (AIC) - AIC is engaged in coastal studies, expeditionary support, evacuation-planning and other logistical services. It maintains the JIVA Operational Laboratory which processes SIGINT and IMINT and their integration. It also stands watch and aids in evacuation planning.

Bureau of Alcohol, Tobacco, and Firearms (BATF or more commonly ATF) - A U.S. Treasury Department law enforcement department dedicated to enforcing federal laws in order to prevent and suppress violent crimes, to collect revenues, and to protect the public in matters related to alcohol, tobacco, and firearms. BATF manages the Firearms Licensing Program to ensure compliance with federal laws. It also assists law enforcement agencies in the handling of violent crimes through the National Tracing Center. http://www.atf.treas.gov/

Bureau of Intelligence and Research (INR, sometimes called BIR in the popular media) - Originally the Interim Research and Intelligence Service, it has been designated as the Bureau of Intelligence and Research since 1957. It is now part of the U.S. State Department. INR publishes intelligence reports and collects normal diplomatic information and open-source intelligence. See State Department Bureau of Intelligence and Research.

Canadian Forces Intelligence Branch Association (CFIBA) - The professional organization of the Canadian Forces Intelligence Branch which fosters and promotes the traditions and well-being of its members. The Web site includes the "Intelligence Note Book" which provides an introduction to intelligence concepts and suggestions for further reading. http://www.intbranch.org/

Canadian Security Intelligence Service (CSIS) - Promotes Canada's national security and the safety of Canadian residents. CSIS provides information and assistance to safeguard scientific and commercial secrets. Founded in 1984 when an Act of Parliament disbanded the Royal Canadian Mounted Police Security Service which had carried out this mandate for 120 years. http://www.csis-scrs.gc.ca/

Center for Defense Information (CDI) - A national, independent military research organization founded in 1972 funded by public and foundation donations rather than government or military funding. The organization researches military spending, policies, and weapons systems. The military is studied from the public perspective and CDI provides information through the media and various publications. CDI provides assistance to the government by request. http://www.cdi.org/

Center for International Policy (CIP) - Founded in 1975 to promote U.S. foreign policies that reflect democratic values. CIP promotes a non-militaristic approach to international relations through education and advocacy. It promotes the restoration of democracy in oppressed nations and the removal of landmines. It sponsors an intelligence reform program. http://www.us.net/cip/

Central Intelligence Agency (CIA) - An independent agency established in 1947 through the signing of the National Security Act. The Director of Central Intelligence (DCI) was charged with coordinating national intelligence. The DCI is the head of the U.S. Intelligence Community as principal adviser to the President for intelligence matters. http://www.cia.gov/ (Office of the Director of Central Intelligence) http://www.odci.gov/

The Directorate of Intelligence (DI) - The analytical arm of the CIA that provides intelligence analysis on national security and foreign policy issues.

The Directorate of Science and Technology (DS&T) - Involved in science and technical innovation relevant to intelligence activities, such as imaging systems.

The Center for the Study of Intelligence (CSI) - Provides research, publications, and a variety of educational programs. Houses historical materials.

The Electronic Document Release Center (EDRC) - Provides document collection and information to provide an overview of access to CIA information.

Arms Control Intelligence Staff (ACIS) - Arms control intelligence information.

Consumer Information Center (CIC) - A U.S. General Services Administration agency which publishes a free Consumer Information Catalog which lists more than 200 free or low-cost booklets on a wide variety of consumer-related topics. The Catalog can be downloaded. http://www.gsa.pueblo.gov/

Council of Intelligence Occupations (CIO) - A department of the Directorate of Intelligence (DI) which assesses skill levels against needed intelligence requirements and ensures a supply of expertise and talent in political, military, economic, scientific, leadership, imagery, and other intelligence fields. http://www.odci.gov/cia/di/mission/cioc.html

Counterintelligence Corps (CIC) - A branch of the U.S. Army descended from the Military Intelligence Service Counterintelligence Branch. The Corps was established in 1942 to handle both domestic and foreign missions.

Counterterrorist Center (CTC) - A Directorate of Intelligence (DI) facility that tracks international terrorist activities to provide analysis and intelligence which assists in prevention and policy-making related to countering terrorist threats.

Crime and Narcotics Center (CNC) - A department within the Directorate of Intelligence (DI) which provides intelligence and analysis on international organized crime, smuggling, and narcotics trafficking. Supports implementation of the Presidential International Crime Control Strategy for identifying and evaluating organized crime that affects U.S. economics and security. Computer databases are used to track the flow of goods and enforcement efforts.
http://www.odci.gov/cia/di/mission/cnc.html

Defense Computer Forensics Lab (DCFL) - A Department of Defense (DoD) facility near Baltimore announced in September 1999. The DCFL employs agents and computers to engage in 'digital forensics' in order to trace and process computer-related activities, particularly viruses, files, corrupted, encrypted, or modified data to protect national interests. Information can assist military forces as well as aiding the FBI and local law enforcement organizations.

Defense Intelligence Agency (DIA) - Established in 1961 to handle non-SIGINT, non-aerial, non-organic military intelligence activities. The DIA serves as a combat support agency for the Department of Defense. The DIA publishes a number of publications including the Defense Intelligence Estimates, Special Defense Intelligence Estimates, and Weekly Intelligence Summaries.
http://www.dia.mil/

Defense Security Service (DSS) - A Department of Defense security agency which, among other things, conducts background investigations on Pentagon employees and contractors. The DSS handles the Personnel Security Investigations Program, the Industrial Security Program, and Security Education and Training. (Formerly the Defense Investigative Service (DIS)) http://www.dss.mil/

Defense Technical Information Center (DTIC) - A Department of Defense facility for providing access to and facilitating the exchange of scientific and technical information. It is part of the Defense Information Systems Agency (DISA). http://www.dtic.mil/

Department of Defense (DoD) - The U.S. DoD provides the U.S. military forces needed to deter war and ensure protection of the United States. It is headquartered at the Pentagon in Washington, D.C. The DoD provides a large archive of official press releases about defense agencies, priorities, and photos of activities of the combined forces of the U.S. at home and abroad. http://www.defenselink.mil/

Department of Energy (DoE) - This important U.S. federal body, founded in 1977 in response to the energy crisis, includes an Office of Intelligence and an Office of Counterintelligence which support DoE facilities and labs and work in cooperation with the FBI and other law enforcement bodies. http://gils.doe.gov/

Department of Justice (DoJ) - Under the direction of the Attorney General, the U.S. DoJ is charged with attaining and maintaining justice and fair treatment for Americans through the combined services of almost 100,000 attorneys, law enforcement professionals, and employees. Part of the DoJ responsibility involves detecting criminal offenders. It is headquartered in Washington, D.C. with almost 2,000 installations throughout the country. http://www.usdoj.gov/

Diplomatic Security Service (DSS) - A U.S. Department of State service which handles diplomatic Department of State service which handles diplomatic. It also handles the "Rewards for Justice" counterterrorism program which provides rewards and relocation to people providing information leading to the arrest and conviction of those planning or perpetrating terrorist crimes. http://www.heroes.net/

Electronic Frontier Foundation (EFF) - A prominant Internet-related organization established in 1990 by Mitch Kapor to serve as a lobbying body and information resource to safeguard public freedoms, particularly freedeom of expression and privacy, on and through the Net. http://www.eff.org/

Federal Bureau of Investigation (FBI) - This U.S. national investigative agency was first established as the Bureau of Investigation (BOI) in 1908. The FBI handles federal investigations and investigations of crimes that cross state lines. The FBI manages a lab with some of the most sophisticated forensic surveillance technologies and procedures in the world. More recently the FBI has been called in by NATO to aid in international investigations such as those which occurred in Kosovo. The National Infrastructure Protection Center is located at the FBI headquarters. http://fbi.gov/

Federal Information Center (FIC) - A U.S. General Services Administration agency which provides information to the public about the Freedom of Information Act and the Privacy Act. It can further aid an individual in locating the correct agency for information requests pertaining to the FOIA and the Privacy Act. Established in 1966. http://fic.info.gov/

Federation of American Scientists (FAS) - A prominent, privately funded, nonprofit organization which provides advocacy and analysis of public policy related to global security through science, technology, and education. Its distinguished membership includes many Nobel Prize Laureates. FAS evolved from the Federation of Atomic Scientists, founded in 1945 by members of the Manhattan Project. The site has extensive educational information on the U.S. Intelligence Community and global security topics. http://www.fas.org/

International Association for Identification (IAI) - A nonprofit organization for professionals engaged in forensic identification and scientific examination of physical evidence. The IAI provides a range of education and certification programs including latent fingerprint examination, crime scene certification, forensic artistry, etc. Descended from the International Association for Criminal Identification, founded in 1915. http://www.theiai.org/

International Centre for Security Analysis (ICSA) - A London-based consultancy research arm at King's College. Provides seminars, research, and publications on major topics in security and intelligence. http://www.kcl.ac.uk/orgs/icsa/

International Intelligence History Study Group - Founded in 1993 to promote scholarly research on intelligence organizations and their impact on historical development and international relations. The membership includes historians, scientists, cryptologists, former intelligence personnel, and politicians. The organization publishes a newsletter and provides excerpts online. As it is based in Germany, there is interesting information for historians from a European perspective. http://intelligence-history.wiso.uni-erlangen.de/

House Permanent Select Committee on Intelligence (HPSCI) - The CIA reports to this Committee as per the terms of the Intelligence Oversight Act of 1980 and pertinent executive orders. (See Restrictions and Regulations for more information on this.)

Marine Corps Intelligence Activity (MCIA) - Among other things, the MCIA provides intelligence and educational materials related to urban warfare.

Mercyhurst College - An educational institution at which a professional intelligence/counterintelligence library is being organized. The college has been building an undergraduate intelligence studies program with assistance from R. Heibel (retired FBI), a member of the AFIO Board of Directors.

National Air Intelligence Center (NAIC) - Air Force intelligence production center within the Air Intelligence Agency. NAIC assesses foreign forces, threats, and weapons capabilities. It provides foreign air intelligence to Air Force operational units and the Department of Defense (DoD). Founded in 1993 from the amalgamation of the 480th Intelligence Group and the Foreign Aerospace Science and Technology Center. Members are also involved in community educational and humanitarian activities.

National Archives and Records Administration (NARA) - A significant archiving body for the United States which includes documents, histories, lists of agencies, artifacts, and images. The collection is extensive, including veterans' service records, federal records schedules, federal laws and Presidential documents. There is also an online exhibit featuring the Declaration of Independence and other historical artifacts. The Web site provides search capabilties. http://www.nara.gov/

National Association of Background Investigators (NABI) - A professional organization that provides education, newsletters, and other support services to members. http://www.background.org/

National Counterintelligence Center (NACIC) - Coordinates U.S. Government threats to national and economic security under the auspices of the National Security Council. NACIC personnel are drawn from various organizations related to the Intelligence Community. NACIC funds counterintelligence activities through courses and seminars and various public and private training programs. http://www.nacic.gov/

National Drug Intelligence Center (NDIC) - Supports counter-drug operations by training, investigating and preparing strategic intelligence, and threat analysis/reporting.

National Foreign Intelligence Council (NFIC) - Created in 1982 to deal with budget issues and priorities related to foreign intelligence production.

National Ground Intelligence Center (NGIC) - Through a number of separate buildings, the NGIC provides scientific, technical, and general military assessments and recommendations including projects such as the identification and removal of landmines.

National Intelligence Council (NIC) - A council of National Intelligence offices which serves the DCI with strategic information and production to assist policy-makers in managing foreign policy. The Council draws on academic and private sector resources. http://www.odci.gov/ic/nic.html

National Military Intelligence Association (NMIA) - A professional forum for national and military intelligence personnel established in 1974 for the exchange of ideas and professional development. NMIA has approximately 200 members. It publishes the NMIA Newsletter and the American Intelligence Journal. http://www.nmia.org/

National Security Agency (NSA) - Originally descended from the U.S. Armed Forces Security Agency (AFSA) which was established in 1949, the organization was disbanded and then re-established as the NSA. The NSA has a broad set of responsibilities including aerial surveillance, SIGINT, cryptologic activities, computer communications, and counterintelligence strategies. http://www.nas.gov/

National Security Archive (NSA) - An independent non-governmental research institute and library located in the George Washington University in Washington, D.C. The Archive staff collects and publishes declassified government documents acquired through the Freedom of Information Act (FOIA). It receives non-governmental funding and donations of materials by private parties and foundations. http://www.gwu.edu/~nsarchiv/

National Security Council (NSC) - The NSC is an important unit that reports to the President and oversees intelligence activities, primarily national security and foreign policy. The statutory military advisor to the Council is the Chairman, Joint Chiefs of Staff. The NSC periodically issues National Security Intelligence Directives (NSCIDs) specifying definitions, duties, and responsibilities, some of which are described in the History and Evolution section earlier in this chapter. Created through the National Security Act of 1947. http://www.whitehouse.gov/WH/EOP/NSC/html/nschome.html

National Security Institute (NSI) - Product news, computer alerts, travel advisories, and a calendar of events for security professionals. NSI sponsors an annual forum on corporate and government security threats. http://www.nsi.org/

National Security Study Group (NSSG) - Also known as the Hart-Rudman Commission, this group has studied and documented national security in terms of threats and opportunities along with technology looking into the future. It has produced a series of reports for the NSSG Senior Advisory Board. NSSG sponsors the Future Tech Forum. http://www.nssg.gov/

National Technical Investigators Association (NATIA) - NATIA's members are surveillance professionals drawn from a number of fields, including law enforcement, the armed forces, and the government. Membership is not open to private detectives or vendors. The organization sponsors an annual seminar and exhibition. NATIA has one of the most interesting crests in the industry, an eagle holding two thunderbolts in its claws, with radio earphones and the motto "In God We Trust, All Others We Monitor." http://www.natia.org/

Naval Criminal Investigative Service (NCIS) - Uses and provides services and products for the investigation of crimes. Provides the NCIS System and Technology Threat Advisory that issues threat warnings related to foreign targeting of U.S. Navy critical program information.
http://www.ogc.secnav.hq.navy.mil/

Navy Operational Intelligence Center (NOIC) - This evolved from the Navy Field Operational Intelligence Office (NFOIC) and functions below the Naval Intelligence Command. The NOIC monitors foreign marine-related vessel histories, locations, and activities.

Nonproliferation and International Security Division (NIS) - NIS centers report to the Associate Laboratory Director for Threat Reduction and respond to proliferation threats involving weapons of mass destruction (WMD) and develop and apply science and technology to deter proliferation to ensure U.S. and global security. http://www.lanl.gov/orgs/nis/

President's Foreign Intelligence Advisory Board (PFIAB) - An agency of the National Foreign Intelligence Program (NFIP), which also encompasses the DCI and the CIA.

Securities Exchange Commission (SEC) - The SEC Division of Enforcement surveils securities-related activities on the Internet. National Association of Securities Dealers (NASD) Regulation (NASDR) has an electronic surveillance department devoted to detecting and monitoring suspected insider trading violations, short selling, options trading, and 'drive-by manipulations.'

Senate Select Committee on Intelligence (SSCI) - The CIA reports to this Committe as per the terms of the Intelligence Oversight Act of 1980 and pertinent executive orders.

Society of Competitive Intelligence Professionals (SCIP) - International organization of competitive intelligence professionals. SCIP provides publications and educational seminars of particular interest to corporate intelligence personnel and business students. http://www.scip.org/

State Department Bureau of Intelligence and Research (INR) - INR was originally the Interim Research and Intelligence Service. The State INR established the Geographic Learning Site in 1998. It produces intelligence assessments related to foreign policy and international issues and educational funding management and training services. It is sometimes referred to as BIR in the popular media.

Unified and Specified Command Intelligence Directorates (USCID) - Local installations of forces drawn from across U.S. military services. This intelligence is channeled to appropriate national agencies such as the NSA and the CIA.

10.b. Print Resources

Each chapter includes print resources that describe a few introductory texts and many intermediate and advanced texts pertaining to the topic of that chapter. Those of general interest to intelligence and surveillance are listed here.

The author has tried to read and review as many of these resources as possible before listing them, but sometimes had to rely on publishers' descriptions or the recommendations of colleagues. The annotations will assist you in selecting additional reading. It's a good idea to preview books before buying them or to seek out reviews by authors with interests similar to your own.

This list may include out-of-print publications. These can sometimes be found in local libraries and second-hand book stores, or through inter-library loan systems.

Abrams, M.; Jajodia, S.; Podell, H. (editors), "Information Security - An Integrated Collection of Essays," IEEE Computer Society Press, January 1995.

Adler, Allan, "Using the Freedom of Information Act: A Step by Step Guide," Washington, D.C.: American Civil Liberties Union, 1987.

Bamford, James, "The Puzzle Palace: A Report on NSA, America's Most Secret Agency," Boston, Ma.: Houghton-Mifflin, 1982. The book is frequently cited by writers who specialize in the field of intelligence.

Berkowitz, Bruce D.; Goodman, Allan E., "Best Truth: Intelligence in the Information Age," New Haven: Yale University Press, 2000, 224 pages. An analysis of the changing role of intelligence in the information age and a proposal to outsource or decentralize intelligence activities through new models and policies that include commercial resources.

Brin, David, "The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom," Reading, Ma.: Addison-Wesley, 1999. Brin, a physicist and science fiction author provides nonfiction examples of trends and activities that erode our privacy along with a call for 'reciprocal transparency,' in order to balance increasing technology tool use in government with that of the other members of society.

Brookes, Paul, "Electronic Surveillance Devices," Butterworth-Heinemann, 1996, 112 pages. Provides an overview of circuit diagrams and parts lists for a variety of electronic bugs. Does not go into detailed explanations of the circuits.

Brugioni, Dino A., "Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis," listed as out of print. The author is a former CIA member who was a founding officer of the National Photographic Interpretation Center.

Brydon, John, "Best-kept Secret: Canadian Secret Intelligence in the Second World War," Toronto: Lester Pub., 1993. A history of the Canadian contribution to Allied SIGINT operations and the evolution of the CSE.

Cain, Frank, "COCOM and its Intelligence Ramifications," IIHSG 1996 annual conference presentation. How western industrial nations quelled exports of military technologies into Iron Curtain countries. The COCOM acted as a trade-control organization.

Campbell, Duncan, "Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies for political control)," Working Document for the Scientific and Technological Options Assessment (STOA) Panel, Dick Holdsworth, editor, Luxembourg, April 1999.

Caravella, Frank J. "Achieving Sensor-to-Shooter Synergy," Military Review, July-August 1998. This is a personal account of the use of surveillance technologies (sensors, UAVs, intelligence reports, infrared satellite imagery, etc.) in armed conflict and the capabilities and limitations of the technology within the limits of current knowledge and procedures.

Commission on National Security, "New World Coming: American Security in the 21st Century," first installment of a 1999 report from the DoD-appointed panel to assess defense requirements and predict American vulnerability to terrorism. Available in Adobe PDF and HTML formats.

Committee on Government Reform and Oversight, U.S. House of Representatives "A Citizens Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records," a booklet providing a detailed explanation of the Freedom of Information Act and Privacy Act. Available through the U.S. Superintendent of Documents.

Deforest, Peter; Lee, Henry C., "Forensic Science: An Introduction to Criminalistics," McGraw-Hill, 1983, 512 pages. Suitable for technicians and law enforcement personnel.

Devereux, Tony, "Messenger Gods of Battle: Radio, Radar, Sonar: The Story of Electronics in War," London: Brasseys, 1991. Introductory physical principles and history of technology in warfare.

Dorwart, Jeffrey M., "The Office of Naval Intelligence: The Birth of America's First Intelligence Agency 1865-1918," Annapolis, Md.: Naval Institute Press, 1979. A history based on published and unpublished archival materials.

Dulles, Allen W., "The Craft of Intelligence," New York: Harper & Row, 1963. The author (1893-1969) was a long-time Director of the CIA and is known for shaping the Intelligence Community in America. Princeton University has an extensive collection of his writings, speeches, and related photographs documenting his life.

Eftimiades, Nicholas, "Chinese Intelligence Operations," Arlington, Va.: Newcomb Pub. Inc., 1998.

Eliopulos, L., "Death Investigators' Handbook: A Field Guide to Crime Scene Processing, Forensic Evaluations, and Investigative Techniques," Colorado: Paladin, 1993.

Ellit, S.R., "Scarlet to Green: A History of Intelligence in the Canadian Army 1903-1963," Canadian Intelligence and Security Association, 1981, over 500 pages. Historical reference that includes the organization and activities of each military intelligence unit.

Feklissov, Alexandre, "Confession d'un Agent Soviétique," Paris: Éditions du Rocher, 1999, 422 pages. The author, in his eighties, recounts his career in Soviet intelligence, including descriptions of the Rosenberg recruitment, development, and training in photographic techniques, and communications during the Cuban Missile Crisis.

Fisher, A. J.; Block, Sherman, "Techniques of Crime Scene Investigation," Boca Raton, Fl.: CRC Press, 1998 (revised). Used in the International Association for Identification's Crime Scene Certification, Level 1. Clinical analysis of crime scene investigation and real life examples.

Flaherty, David H., "Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States," Chapel Hill, N.C.; University of North Carolina Press, 1992.

Fuld, Leonard M., "The New Competitor Intelligence," New York: John Wiley & Sons, 1995. Identifies information sources, includes analyses of case studies, discusses ethics. This is being used as a text in business courses.

Garrison, D. H., Jr., "Protecting the Crime Scene," FBI Law Enforcement Bulletin, September 1994.

Jacob, John, "The CIA's Black Ops: Covert Action, Foreign Policy, and Democracy," Amherst, Prometheus Books, 1999, 350 pages. A discussion of CIA secret ("black") operations and their role in international politics and domestic policy.

Justice Department's Office of Information and Privacy, "Freedom of Information Act Case List," includes lists of cases decided under the Freedom of Information Act, the Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act. Includes statutes and related law review articles. Updated every second (even) year.

Justice Department's Office of Information and Privacy, "Justice Department's Guide to the Freedom of Information Act Guide" and "The Privacy Act Overview," are federal booklets that are updated annually. These documents are also available for download. http://www.usdoj.gov/oip/

Kahaner, Larry, “Competitive Intelligence,” New York: Simon & Schuster, 1996. This is being used as a text in business courses.

Law Enforcement Associates, “The Science of Electronic Surveillance,” Raleigh, NC: Search, 1983.

MacKay, James A., “Allan Pinkerton: The First Private Eye,” Edinburgh: Mainstream Publishing, 1997, 256 pages.

Madsen, Wayne, “Intelligence Agency Threats to Computer Security,” International Journal of Intelligence and Counterintelligence, V.6(4), 1993, 413-488. Includes an international listing of computer-communications espionage capabilities of intelligence and law enforcement agencies.

McGarvey, Robert; Caitlin, Elise, “The Complete Spy: An Insider’s Guide to the Latest in High Tech Espionage and Equipment,” New York: Perigee, 1983.

McLean, Donald B., “The Plumber’s Kitchen: The Secret Story of American Spy Weapons,” Cornville, Az: Desert Publications, 1975.

Melton, H. Keith, “CIA Special Weapons and Equipment: Spy Devices of the Cold War,” New York: Sterling Publishing, 1993. Illustrates and describes tools of the trade. This author has a personal collection of spy devices.

Melton, H. Keith, “OSS Special Weapons and Equipment: Spy Devices of WWII,” 1991, listed as out of print.

Melton, H. Keith, “The Ultimate Spy Book,” London & New York: Dorling Kindersley, Ltd, 1996. A visual encyclopedia of intelligence operations and equipment from about renaissance times to the present.

Melvern, Linda; Anning, Nick; Hebditch, David, “Techno-Bandits,” Boston: Houghton-Mifflin Co., 1984. Addresses issues of illegal technology transfer for military/industrial support of Communist nations.

Minnery, John, “CIA Catalog of Clandestine Weapons, Tools, and Gadgets,” Boulder, Co.: Paladin, 1990. Describes devices which the author claims are designed by CIA Technical Services.

National Security Archive, “Military Uses of Space: The Making of U.S. Policy, 1945-1991,” The Fund for Peace. See also the National Security Archive’s “U.S. Espionage and Intelligence, 1947-1996.”

National Security Study Group, “The Hart-Rudman Commission Reports,” a series of reports regarding national security threats and opportunities and their relationships to future technologies, available in Adobe PDF format at http://www.nssg.gov/

Osterburg, James W.; Ward, Richard H., “Criminal Investigation: A Method for Reconstructing the Past,” Anderson Publishing Company, 1996.

Peake, Hayden B., “The Reader’s Guide to Intelligence Periodicals,” Washington, D.C.: NIBC Press, 1992. Lists over 100 intelligence-related sources.

Peterson, J.; Mihajlovic, S.; Gilliland, M., “Forensic Evidence and the Police: The Effects of Scientific Evidence on Criminal Investigations,” National Institute of Justice Research Report, Washington, D.C., U.S. Government Printing Office, 1984.

Poole, Patrick S., “ECHELON: America’s Secret Global Surveillance Network,” Washington, D.C.: Free Congress Foundation, October 1998.

Price, Alfred, “The History of U.S. Electronic Warfare: The Renaissance Years, 1946 to 1964,” Association of Old Crows, 1989. A history of the development and use of electronic warfare emphasizing intelligence-gathering and countermeasures.

Richardson, Doug, “An Illustrated Guide to the Techniques and Equipment of Electronic Warfare,” New York: Simon & Schuster, 1988.

Richelson, Jeffrey T., “A Century of Spies: Intelligence in the Twentieth Century,” Oxford University Press, 1997. A history of modern intelligence from the early days of the British Secret Service to present times including spies, agencies, and technological developments including aerial surveillance and ground station operations.

Richelson, Jeffrey T., "Foreign Intelligence Organizations," listed as out of print, 1988.

Richelson, Jeffrey T.; Evans, Michael L. (assisting), "The National Security Agency Declassified: A National Security Archive Electronic Briefing Book."

Richelson, Jeffrey T., "Sword and Shield: The Soviet Intelligence and Security Apparatus," Cambridge, Ma.: Ballinger, 1986.

Richelson, Jeffrey T., "The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries," London: Allen & Unwin, 1985.

Richelson, Jeffrey T., "The U.S. Intelligence Community," Boulder, Co.: Westview Press, 1999, 544 pages.

Richelson, Jeffrey T., "The U.S. Intelligence Community, 1947-1989," Boulder, Co.: Westview Press, 1990. A comprehensive portrait of about two dozen U.S. intelligence-gathering organizations and the internal relationships and evolution of federal agencies including the FBI, the CIA, and military intelligence agencies. A related document, "The U.S. Intelligence Community: Organization, Operations and Management, 1847-1989" is available on microfiche, reproducing over 15,000 pages of documents from key intelligence organizations.

Saferstein, Richard, "Criminalistics: An Introduction to Forensic Science," Englewood Cliffs: Prentice-Hall, 1997, 638 pages. Introductory text to the forensic sciences.

"Science at its Best | Security at its Worst: A Report on Security Problems at the U.S. Department of Energy," A Special Investigative Panel, President's Foreign Intelligence Advisory Board (PFIAB), June 1999. A report on an inquiry requested by President Clinton on 18 March 1999 regarding "The security threat at the Department of Energy's weapons labs and the adequacy of the measures that have been taken to address it...." including counterintelligence security threat and its evolution over the last two decades.

Shane, Scott, "Mixing business with spying; secret information is passed routinely to U.S.," Baltimore Sun, 1 Nov. 1996.

Shulsky, Abram N., "Silent Warfare: Understanding the World of Intelligence," New York: Brassey's, 1993. A text that has been recommended for college courses on intelligence.

Smith, Walter Bedel, "Proposed Survey of Communications Intelligence Activities," Report to the Secretary of State and the Secretary of Defense by a Special Committee, 1951.

Swanson, Charles R.; Chamelin, Neil C.; Terriro, Leonard "Criminal Investigation," New York: Random House, 1981. Comprehensive text (used by some of the civil service programs) with practical introductory information on criminal investigation. Provides a framework for a variety of types of investigative activities. Includes illustrations and case studies.

Taylor, L.B., Jr., "Electronic Surveillance," New York: Franklin Watts/Impact Books, 1987, 128 pages. A former NASA employee, Taylor highlights key aspects of electronic surveillance in a style suitable for teen readers and adults looking for an illustrated introduction to the field.

"U.S. Government Manual," Washington, D.C. The official handbook of the U.S. federal government which describes offices and programs within the federal government, including top personnel and agency addresses and phone numbers. It is available for purchase for about $36 through the Superintendent of Documents or can be found in public libraries.

Wark, Wesley, "Canada and the Intelligence Revolution," IIHSG 1996 annual conference presentation. Concepts relating to the Information Age and the Intelligence Revolution and Canada's experience and role in the intelligence community.

Weber, Ralph, "Spymasters: Ten CIA Case Officers in Their Own Words," Wilmington, Del.: SR Books, 1999. A collection of interviews of almost a dozen CIA officials covering a range of topics from the early days of the NSC and the CIA to more recent events.

Westerfield, H. Bradford (editor), “Inside CIA’s Private World,” London: Yale University Press, 1995.

Yost, Graham, “Spy-Tech: The Fascinating Tools of the Espionage Trade–What, How, and Who Uses Them,” New York: Facts on File, 1985.

Zegart, Amy B., “Flawed by Design: The Evolution of the CIA, JCS, and NSC,” Stanford: Stanford University Press, 1999, 342 pages. A critical analysis and discussion of the origins, development, and functions of the nation’s primary intelligence agencies.

Articles

Aviation Week and Space Technology Editors, “Electronic Countermeasures: Special Report,” 21 Feb. 1972, pp. 38-107.

Aviation Week and Space Technology Editors, “Special Report on Electronic Warfare,” 27 Jan. 1975, pp. 41-144.

Clark, Robert M., “Scientific and Technical Intelligence Analysis,” *Studies in Intelligence*, V.19(1), Spring 1975, pp. 39-48.

Dumaine, Brian, "Corporate Spies Snoop to Conquer," *Fortune*, 7 Nov. 1988, pp. 68-76.

“Electronic Surveillance and Civil Liberties,” Congress of the United States, Washington, D.C., Office of Technology Assessment, 1985.

“Federal Government Information Technology: Management, Security, and Congressional Oversight,” Congress of the United States, Washington D.C., Office of Technology Assessment Report Brief, 1986.

Hermann, Robert J., “Advancing Technology: Collateral Effects on Intelligence,” *American Intelligence Journal*, V.15(2), 1994, pp. 8-11. Hermann advocates a look at management of national systems and supports the exploitation of open-source intelligence and other information sources.

Hunter, Robert W., “Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case,” Annapolis, Md.: U.S. Naval Institute, 1999. The recounting of years of Soviet espionage within the U.S. Navy. Hunter is a former FBI foreign counterintelligence agent involved in the case.

Maiolog, Joseph A., “I believe the Hun is cheating: British Admiralty Technical Intelligence and the German Navy,” *Intelligence and National Security*, February 1996, V.11(1), pp. 32-58.

Woodward, Bob, “Messages of Activitists Intercepted,” *Washington Post*, 13 Oct. 1975, pp. A1, A14.

Journals and Bulletins

This is just a small selection, as there are approximately 200 intelligence journals published regularly or semi-regularly in English alone.

“AFIO Intelligence Notes,” a weekly publication of the Association of Former Intelligence Officers. Includes news, reviews, and relevant Web information. Available by paper subscription, email subscription, and Web download.

“Africa Intelligence,” online by-subscription politcal/economic news journal published by Indigo Publications. http://www.indigo-net.com/

“American Intelligence Journal,” published by the National Military Intelligence Association, includes personal recollections and articles by leaders in the intelligence field. http://www.nmia.org/AIJ.htm

“Bulletin of the Atomic Scientist,” an analytic and often critical professional journal that includes articles about the intelligence community analysts. http://www.bullatomsci.org/

“Competia Online,” is an online by-subscription resource for news and articles on tools, analysis techniques, and strategic planning for corporate intelligence.

“Competitive Intelligence Magazine,” quarterly journal from SCIP with news and tutorial information on competitive intelligence (primarily business).

“Competitive Intelligence Review,” quarterly journal from SCIP and John Wiley & Sons, Inc. with practical research and analysis information on competitive intelligence (primarily business).

“CovertAction Quarterly,” http://www.mediafilter.org/caq/

“Defense Intelligence Journal.”

“Director of Central Intelligence Annual Report for the United States Intelligence Community,” an annual report of the accomplishments, priorities, and issues of concern to the CIA.

“Economic/Commercial Interests and Intelligence Services, Commentary No. 59,” *Canadian Security Intelligence Service*, July 1995. Written by a strategic analyst, this focuses on protecting and pursuing a nation’s economic/commercial interests.

“Inside Fraud,” U.K.-based professional bulletin on business fraud, its detection and management. Published by Maxima Partnering Ltd., London.

“Intelligence and National Security,” (I&NS) academically oriented journal.

“Intelligence Newsletter,” bimonthly journal of business intelligence, community watch, threat assessment, technology, people, etc. Aimed at the needs of diplomats, officials, security companies, and academic researchers. Indigo Publications (founded in 1981), Paris, France.

“Intelligencer,” the journal of the Association of Former Intelligence Officers.

“International Journal of Intelligence and Counterintelligence,” (IJI&C) academically oriented journal.

Justice Department’s Office of Information and Privacy, “FOIA Update,” is a newsletter published quarterly which contains information and guidance for federal agencies regarding the Freedom of Information Act. Selected portions are available online. http://www.usdoj.gov/oip/foi-upd.html

“Morning Intelligence Summary,” an internal document produced by the INR each day for the Secretary of State, no matter where the Secretary may be stationed.

“National Intelligence Daily,” NID is a CIA secret bulletin which ceased publication in 1998 due to alleged press leaks. Its successor since 1998 has been the “Senior Executives Intelligence Brief (SEIB)” which has a more carefully monitored distribution.

“National Military Intelligence Association (NMIA) Newsletter,” lists news, activities synopses, upcoming events, book reviews and other information of interest to members. Available in hard copy, Adobe PDF format (from 1999), and through email subscription.
http://www.nmia.org/

“National Security.”

“National Security Law Report,” publication of the Standing Committee which is distributed eight times yearly to attorneys, government officials, and scholars. http://www.abanet.org/natsecurity/nslr/

“Naval Intelligence Professionals Quarterly.”

“On Watch: Profiles from the National Security Agency’s Past 40 Years,” Fort Meade, Md.: The National Cryptologic School, 1986.

“Orbis,” scholarly articles on theory and practice.

“Periscope,” a journal of the Association of Former Intelligence Officers.

“Senior Executives Intelligence Brief (SEIB)” the CIA secret bulletin that replaced the “National Intelligence Daily” in 1998 in order to provide greater security from unauthorized distribution.

“Studies in Intelligence,” CIA publication which can be accesssed through the CIA Electronic Document Release Center online.

“Surveillant,” Military Intelligence Book Center email newsletter. Ceased publication.

“Weekly Defense Monitor,” published by the Center for Defense Information, it includes information on world conflicts, the CIA, the NSA, arms agreements, weapons production, etc. from an independent public perspective. http://www.cdi.org/

“World Intelligence Review,” Heldred publication which went out of print in 1997. Back issues may be available. It was descended from Foreign Intelligence Literary Scene.

“Your Right to Federal Records: Questions and Answers on the Freedom of Information Act and the Privacy Act,” Washington, D.C.: U.S. General Services Administration and U.S. Department of Justice, November 1996.

10.c. Conferences and Workshops

Each chapter has a section listing conferences, workshops, and sometimes contests which are held with relation to the technologies discussed in each chapter. In addition, there are some meetings of general interest listed below.

Many of these conferences are held annually at approximately the same time each year, so even if the conference listed here is outdated, it may help you figure out the schedule for upcoming events. It is common for international conferences to be held in a different city each year, so contact the organizers for current locations. Many organizations announce upcoming conferences on the Web and some of them archive the conference proceedings for purchase or free download.

The following conferences are listed in the order of the calendar month in which they are usually held.

“The Digital Detective Workshop™,” New York, 18 Feb. 2000 and 6 Mar. 2000 (corporate) and 7 Mar. 2000 (government). The workshop covers acquisition tools and techniques for digital evidence. http://www.codexdatasystems.com/ddw.html

“Impact 2000: National Security Institute Forum,” 15th annual forum discusses emerging threats to corporate and government information, Falls Church, Va., 3-5 Apr. 2000.

“Business Intelligence and Law Symposium II,” sponsored by the Association of Former Intelligence Officers, Washington, D.C., 19 May 2000.

“Competitive Technical Intelligence Symposium,” San Francisco, Ca., 8-9 June 2000.

“AFCEA/FCW GovTechNet 2000,” Washington, D.C., 15-17 June 2000.

“IIHSG Annual Conference,” 6th annual International Intelligence History Study Group conference, Paderborn, Germany, 23-25 June 2000.

“InfowarCon,” military operations, infrastructure protection, terrorism and espionage topics, Washington, D.C., 11-14 Sept. 2000.

“NASIRE Annual Conference,” represents the concerns of Chief Information Officers (CIOs), Baltimore, Md., 24-27 Sept. 2000. http://www.nasire.org

“ConSec ‘99,” Austin, Texas, 4-8 Oct. 2000.

“AFIO National Convention,” sponsored by the Association of Former Intelligence Officers, hosted by the Director NSA, Fort Meade, Maryland, 5-6 Oct. 2000.

“Information Systems Security Expo,” Crystal City, Virginia, 19 Oct. 1999.

“Counterintelligence 2000 Symposium,” Fort Myer, Va., 25 Oct. 2000.

“SCIP European Conference and Exhibit,” annual conference of the Society for Competitive Intelligence Professionals, London, U.K., 25-27 Oct. 2000.

“Defense Intelligence Status 2000 Symposium,” sponsored by NMIA, Fort Myer, Va., 26 Oct. 2000.

“AFCEA,” Washington, D.C., 27-28 Oct. 2000.

“Conference of the Association for Crime Scene Reconstruction,” College, Park, Georgia, 27-29 Oct. 2000. http://www.acsr.com/

“Competitive Finanacial Intelligence Symposium,” sponsored by SCIP, New York City, 10-11 Nov. 2000.

10.d. Online Sites

Here are a few Web sites of particular interest or relevance to this topic. In most cases, commercial sites are not included unless they have a particularly good educational focus or set of illustrations. The selected sites are generally well-maintained and up to date and are likely to remain at the same URL for some time. In the case of sites that change, keywords in the descriptions below can be used to try to relocate the site on a Web search engine (it is more likely that the site has been moved rather than deleted).

Army Counterintelligence Discussion Group List. Initiated early in 1999 for active and former counterintelligence agents. Private, moderated list. Members must be approved. Covers counterintelligence trends, training, news, history, and current events.

Canadian Forces Intelligence Branch Association (CFIBA). This professional organization provides the Intelligence Note Book online, which provides an introduction to intelligence. It also hosts a Virtual Museum with information about Norse records dating back thousands of years and an illustrated history of Canadian contributions to the World Wars. There is also an annotated bibliography of suggested readings. http://www.intbranch.org

Center for Army Lessons Learned. A site with some interesting illustrated lesson-style articles that have arisen out of the real-world experiences of army personnel. While not directly related to the use of technology and surveillance devices, there are references to technological advances and their place within the overall frameworks of peacekeeping and armed conflicts. There is also access to Periscope, an online source for intelligence data and defense news, which is available to authorized users. http://call.army.mil/

CIA Electronic Document Release Center. A searchable archive of CIA documents that have been released or declassified under the Freedom of Information Act. Includes documents released since 1996. http://www.foia.ucia.gov/

Crime & Clues. This site includes links to forensics and crime investigation sites and provides a series of articles by various authors on crime scene protection, processing, and investigation. There is also signup for a crime scene investigation discussion list. http://crimeandclues.com

Cryptome. An online resource with articles and excerpts of communications regarding international surveillance and political developments. Includes information on wiretaps, ECHELON, cipher activities, Internet security, and more. http://cryptome.org/ http://www.jya.com/

Duncan Campbell IPTV Reports. This is an extensive, illustrated, news and investigative journalism site that covers global intelligence activities, including projects within the U.S. that have been haphazardly researched by others. While there is no way for anyone outside the secret services to authenticate much of the information, this site appears to be a better source of 'informed speculation' than many others on the Web. http://www.iptvreports.mcmail.com/

Granite Island Group Technical Surveillance Counter Measures. An extensive list of links to statutes and documents on intelligence and surveillance including the complete text of some of the more relevant Presidential Executive Orders. Maintained by James M. Atkinson, Communications Engineer. http://www.tscm.com/reference.html

Intelligence Online. "Intelligence Online: Global Strategic Intelligence" is a bimonthly online by-subscription journal of business intelligence, community watch, threat assessment, technology, people, etc., aimed at the needs of diplomats, officials, security companies, and academic researchers. It is a searchable, online version of the print journal Intelligence Newsletter. http://www.indigo-net.com/

Intelligence Resource Program. This resource site, with charts, articles, and links is compiled by the Federation of American Scientists. It includes an extensive complication of news reports (dating back to 1992), some with analyses, and programs, intelligence operations, documents, congressional material, and more. http://www.fas.org/irp/index.html

International Intelligence History Study Group Newsletter. The IIHSG publishes an abridged version of their print publication on their Web site. As this is focused on intelligence activities, it is of broad general interest to surveillance. http://intelligence-history.wiso.uni-erlangen.de/newsletter.htm

Law Reform Commission Publications. The Australian Law Reform site provides a series of papers on various aspects of law, including several on surveillance, e.g., "What is Surveillance? Paper 12 (1997)." http://www.legalaid.nsw.gov.au/nswlrc.nsf/pages/index

The Literature of Intelligence. "A Bibliography of Materials, with Essays, Reviews, and Comments." J. Ransom Clark, J.D., a Faculty Dean at Muskingum College and former member of the CIA, has produced this extensive resource to fill what he considers to be a need for a "central, civilian-controlled entity for the collection, preparation, and dissemination of national-level foreign intelligence." The bibliography is well-organized, annotated, and cross-referenced according to topics. It includes search capabilities. http://intellit.muskingum.edu/

The National Security Archive. This is the world's largest resource of its kind, a nonprofit, nongovernmental library, archive, and research resource founded in 1985. It includes information on international affairs, declassified U.S. documents obtained through the Freedom of Information Act and from a public-interest law firm. It also indexes and publishes documents in books, microfiche, and electronic formats. It is supported by public revenues and private foundations. The physical archive is located on the seventh floor of the George Washington University's Gelman Library in Washington, D.C. http://www.gwu.edu/~nsarchiv

U.S. Senate Republican Policy Committee. This site has some political and legal interpretations of some of the intelligence-related Acts (e.g., the Foreign Intelligence Surveillance Act) and critiques of White House and Department of Justice interpretations and implementation of those Acts that are of interest. http://rpc.senate.gov/releases/1999/fr080699.htm

Vernon Loeb's IntelligenCIA Column. A biweekly column by the Washington Post reporter who specializes in intelligence topics. Available only in the online edition of the Nation section of the Post. http://www.washingtonpost.com/

10.e. Media Resources

A small selection of media resources is listed in each chapter, mainly popular feature films and video series. The media resources are not complete or comprehensive compared to other sections in this book, but are included to guide the reader to some visual representations and scenarios, both real and imagined, that provide a little extra insight into the field. They're included because some aspects of surveillance technology are hard to describe and illustrate in print.

The listed resources vary in quality from middle-of-the-road movies to science fiction thrillers and serious documentaries. They aren't necessarily included because they were good movies, but rather because they show devices and their use in a new or interesting way (e.g., Sliver isn't a five-star film, but the technology depicted in the film is representative of several important social and technological aspects of visual surveillance). Since the quality of the listed resources is uneven, short annotations are sometimes included in the description to alert the viewer. The author has viewed most of the media resources included, but not all of them. Some were included on the recommendation of colleagues and a few are based on publishers' descriptions.

"Elizabeth," feature film biography of Elizabeth I, the wily Queen of England who firmly held her crown longer than most historic rulers, in part because of her use of the intelligence services of Sir Francis, Earl of Walsingham (not covered in detail, but the movie provides some background). The story is fictionalized and Hollywoodized, but gives a feel for the period and the fact that 'spying' has been around for a long time. Polygram, Cate Blanchett and Joseph Fiennes, 1998, 118 minutes.

"The German Historical Museum," includes exhibits of interest and has been instrumental in establishing the Allied Museum for Berlin in which the Allied presence can be documented and preserved. The Allied Museum provides information on secret intelligence services.

"The Imperial War Museum" in London, England, has a permanent exhibit called the "Secret War Exhibition" which includes espionage history.

"The Nordic Museum" in Stockholm, Sweden showed a special exhibition until 1 Sept. 2000 regarding espionage in and for Sweden. It includes the prehistory of modern expionage and the conflicts between neutrality and espionage activities. The tools of espionage, such as cameras, listening bugs, and cryptographic equipment are featured. This exhibition has ended, but it may be possible to ask curators about access to parts of the exhibit and archival information regarding the exhibit.

"Operation Solo," a July 1999 broadcast of the *History Channel*, based on the John Barron book "Operation SOLO: The FBI's Man in the Kremlin," produced by Towers Productions, Inc. This covers a FBI counterintelligence operation from the early 1950s. The accuracy of some of the ideas presented in the program has been questioned, particularly the portrayal of J. Edgar Hoover, and the assertion that no communist connections to King were found. In general, however, this program is considered to be of interest.

"The Oral History of the Office of Strategic Services," is a project to systematically interview the small number of living representatives of the original employees of the Office of Strategic Services (OSS) which was the predecessor to the U.S. Central Intelligence Agency (CIA). Sponsored by the CIA Center for the Study of Intelligence; initiated and directed by Christof Mauch. Unpublished memoirs of interviewees were also solicited as part of the project. It is archived in the Special Collections Division of the Lauinger Library at Georgetown University. Interview transcripts are also archived with the Library of Congress.

"Red Files," a four-part Public Broadcast Service documentary series that provides a look at the Soviet Union/U.S. Cold War rivalries. The episodes are titled "Secret Victories of the KGB," "Soviet Sports Wars," "Secret Society Moon Mission," and "Soviet Propaganda." There is a Web-based companion site to the series which includes story scripts, synopses, stores, and video clips.
http://www.pbs.org/redfilesRed

"The Rote Kapelle: 50 Years After," a documentary film written and directed by Yelena Letskaya, TROYKA Company, 55 minutes. Based on formerly classified documents in the KGB archives, this film includes interviews with former GRU resident agents and portions of German documentary images. The consultant is Professor Youri Zorya, who discovered some Nürnberg Trial (Nuremberg Trial) documents.

11. Glossary

Each chapter has a short glossary including terms, acronyms, and common abbreviations relevant to the chapter topic. For longer explanations, the reader is encouraged to consult more compreshensive dictionaries and encyclopedias.

Titles, product names, organizations, and specific military designations are capitalized; common generic and colloquial terms and phrases are not.

ACS/I	Assistant Chief of Staff/Intelligence
AFIC	Air Force Inteligence Command. Evolved from Electronic Security Command (ESC).
AFSA	Armed Forces Security Agency. Established in 1949 within the U.S. Department of Defense.
AIA	Air Intelligence Agency
AISC	Army Intelligence and Security Command

AITAC	Army Intelligence and Threat Analysis Center
ALoR	acceptable level of risk. An authoritative and carefully considered assessment that a system or activity meets certain minimum stated or accepted security requirements. Aspects that typically factor into ALoR include capabilities, vulnerabilities, potential threats, the possible consequences of those threats, and countermeasures options.
AMSIC	Army Missile and Space Intelligence Center
anomaly detection	The systems and processes used to assess deviant or unscheduled activities or presences which may indicate anomalous activities or unauthorized access. This interpretation assumes a baseline norm from which deviations are assumed to indicate some type of intrusion.
ASIM	Automated Security-Incident Measurement. A Department of Defense network access and traffic monitor.
BIR	Bureau of Intelligence and Research, better known as INR
breach	A successful disruption or intrusion that could indicate or result in penetration or vulnerable exposure of a system.
BS/I	Bachelor of Science degree with specialization in intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
CBRN	Chemical, Biological, Radiological, and Nuclear
CCMP	Civilian Career Managment Program
CDTD	Critical Defense Technology Division
CERT	Computer Emergency Response Team
CFIBA	Canadian Forces Intelligence Branch Association
CI	counterintelligence, competitive intelligence
CIFMP	Civilian Intelligence Force Management Program
CIM	Communications Identification Methodology
CIPMS	Civilian Intelligence Personnel Management System
CIR	Civilian Intelligence Reserve. A NIC-administered pilot program that was rolled into the Global Expertise Reserve.
CIS	Combat Intelligence System
CM	countermeasure(s)
CMRT	Consequence Management Response Team. An interagency response team which provides coordination and interagency communication for USG-Host Nation responses to CBRN events.
CSS	Central Security Service
CSSPAB	Computer Systems Security and Privacy Advisory Board
CIA	Central Intelligence Agency
countermeasures	Actions and systems intended to prevent, detect, or respond to a security threat.
CTC	Counterterrorist Center
CIWE	Center for Information Warfare Excellence
DCI	Director, Central Intelligence (Director of the CIA)
DCIM	Distinguished Career Intelligence Medal. Awarded by the Central Intelligence Agency (CIA).
DIA	Defense Intelligence Agency
DIC	Defense Intelligence College
DII	Defense Information Infrastructure. The phrase for the information assets of the U.S. Department of Defense.

DSS	Diplomatic Security Service
DSTC	Diplomatic Security Training Center
EAP	Emergency Action Plan
ECM	Electronic Countermeasures
espionage	This translates roughly to “spyage,” the act of spying upon.
ferret	*n.* someone who provokes a response or illumination of a situation, not usually through confrontation but rather through subterfuge or calculated actions
FOIA	Freedom of Information Act
FTD	(Air Force) Foreign Technology Division
GDIP	General Defense Intelligence Program
GIITS	General Imagery Intelligence Training System
GITC	General Intelligence Training Council
GITS	General Intelligence Training System
HDBT	hard and deeply buried target
ICAC	(Canadian) Intelligence Collection and Analysis Centre
IIS	Intelligence Information System
In-Q-It	A venture-capital firm established by the CIA in 1999 to fund promising Internet/ computer-related technological developments. *In* (intelligence) *Q* (Major Boothroyd, aka “Q” the fictional British secret service agent who created gadgets for Agent 007) *It* (information technology).
INSCOM	Intelligence and Security Command, within the U.S. Army
intelligence	The product resulting from the collection, analysis, integration, evaluation, and interpretion, within a given context, of a body of information, of which the information may variously include, but not be limited to, images, data, statistics, facts, objects, schedules, and figures.
ISRC	Intelligence, Surveillance, and Reconnaissance Cell
ITAB	Intelligence Training Advisory Board
JIVA	Joint Intelligence Virtual Architecture
JWICS	Joint Worldwide Intelligence Communications System. A computerized system which includes videoconferencing intended to facilitate communication among intelligence community agents.
misinformation	An important concept in investigations and covert acitivities, misinformation is the spreading of rumors, falsities, fraudulent claims or documents and the general creation of a deceptive persona or situation. When misinformation is used to discredit individuals or organizations, it can be potentially more lethal and devastating than any bomb.
MSD	Mobile Security Division. U.S. diplomatic protection division, the mobile arm of the DSS.
NAVSECGRU	Naval Security Group
NCS	National Crytopologic School
NFIB	National Foreign Intelligence Board
NIE	National Intelligence Estimates
NOIC	Navy Operational Intelligence Center
NSA	National Security Agency
NSC	National Security Council
NSG	Naval Security Group

NSTISS	National Security Telecommunications and Information Systems Security
NTIC	Naval Technical Intelligence Center
OIPR	Office of Intelligence Policy and Review, which is under the direction of the Counsel for Intelligence Policy, advises the Attorney General on national security activities and approves certain intelligence-gathering activities.
OOTW	Operations Other Than War
OPSEC	Operation Security. Securing an operation from discovery, infiltration, and intervention or compromise.
OSAC	Overseas Security Advisory Council
OSTP	Office of Science and Technology Policy
PFIAB	President's Foreign Intelligence Advisory Board
RSO	Regional Security Officer
SASO	Stability and Sustainment Operations
SC&DI	Surveillance, Control and Driver Information system
SCIP	Society of Competitive Intelligence Professionals
secret agent	colloquial term for individuals officially engaged in covert or clandestine surveillance or other intelligence-gathering activities
SIF	Securities Issues Forum
SIRVES	SIGINT Requirements Validation and Evaluation Subcommittee
SORS	SIGINT Overhead Reconnaissance Subcommittee
spoof	*n.* a trick, masquerade, decoy, or use of an imposter to control or divert actions or events.
spook	*n.* a secret agent, spy, operative, or other (usually human) undercover, clandestine or covert agent.
spy	an agent (human, animal, robot) that overtly/clandestinely acquires secrets, information, or unauthorized entry to a facility, event, or nation
STIC	Science and Technology Information Center
sting operation	deliberate, planned, covert or clandestine manipulation of a situation to create an illusion intended to trap or entrap an individual or group
STOA	Scientific and Technological Options Assessment
TENCAP	Tactical Exploitation of National Space Systems Capabilities. A program for improving "combat-readiness and effectiveness of the U.S. Air Force through more effective military use of national space system capabilities."
TIARA	Tactical Intelligence and Related Activities
TRC	Terrorism Research Center
TSCM	Technical Surveillance Countermeasures. A TSCM survey is professional detection and reporting of the presence of technical surveillance devices, hazards, and security weaknesses.
UGIP	Undergraduate Intelligence Program. A Joint Military Intelligence College program for enlisted service members.
undercover	*adj.* concealed; covert or clandestine person, object, or operation
USCID	Unified and Specified Command Intelligence Directorates
USSS	United States Secret Service