Review: Intelligence and Information Policy for National Security

by Jan Goldman and Susan Maret

Intelligence and Information Policy for National Security. Lanham, MD: Rowman and Littlefield, 2016 / 654 pp.
ISBN 78-1-4422-6015-3 (hardback) / ISBN978-1-4422-6016-0 (paper) / ISBN 978-1-4422-6017-7 (ebook)
https://rowman.com/ISBN/9781442260177/Intelligence-and-Information-Policy-for-National-Security-Key-Terms-and-Concepts

Reviewed by Gary T. Marx | References

Mark Twain observed that "the dictionary is the only place where success comes before work." This extensive collection of terms fits well with his observation. It is a most useful, effortless introduction to topics of great interest to practitioners and scholars of intelligence analysis and information protection, discovery and communication and the issues should be of importance to all citizens valuing a democratic and just society.

Two questions: How do you review a dictionary and what are the ideal characteristics for such a reviewer? Two answers: with great difficulty and someone with a short attention span. Since I like challenges and am not above peripatectism, doing this review was appealing. My kind of book—imagine reading a few pages each day and never forgetting the plot or a character, having to figure out the argument, summarize findings or offer trenchant criticisms.

The book belongs in libraries as a basic reference. For those interested in intelligence and related issues it offers a feast for grazing and mining the unknown, unseen or camouflaged data veins within the labyrinthian confines of the multitudinous intelligence and security establishments. It is a veritable "who's who, who's what and what's where" for key terms and concepts and also an invaluable historical record (if in short hand form). The book is part of the Security and Professional Intelligence Education Series edited by Goldman for those interested and/or working in intelligence as it relates to national security.

Jan Goldman is an experienced intelligence analyst who now teaches intelligence and national security at Southern New Hampshire University. Susan Maret teaches courses on secrecy and freedom of information at San Jose State University.

The volume has its origin in Goldman's early work as a federal intelligence analyst. He kept a notebook with definitions to help policy makers or "customers" understand intelligence reports. That eventually resulted in his 2006 publication, Words of Intelligence: An Intelligence Professionals Lexicon for Domestic and Foreign Threats The current volume builds on Goldman's book and Maret's On Their Own Terms: A Lexicon with an Emphasis on Information-Related Terms Produced by the U.S. Government (2006, 3rd edition).

Goldman stresses how important it is for the users of intelligence to understand specialized language offered by their intelligence analysts, who strictly speaking, are not operational intelligence agents. The former know the distinction between analysis (what you know) and assessment (what you believe). The disastrous consequences of failing to make that distinction can be seen in the supposed presence of weapons of mass destruction in Iraq.

When words mean different things to those working together, we can be in trouble. Shared, certified, explicit and codified definitions offer a counter to Humpty Dumpty's subjective, solitary, culturally imperialistic definitions. The words included here come from unclassified or declassified policies, memorandum, training materials, FOIA documents, NGOs, other dictionaries, court records, journalists (both mainstream and alternative), academics and the authors' deep understanding of the fields.

Susan Maret's useful introduction offers a context for the terms and notes the evolving nature of this bureaucratic language. In drawing on the work of Raymond Williams, she notes how certain "keywords" are important signifiers of historical change. Such words serve as "mile markers" that help us see culture and society. This volume provides a documentary record of the culture(s) that creates the words that drive information,and more broadly national security policies. Maret notes how codified terms for national security can be seen to involve a number of "languages"—rational, cultural, secrecy and (reflective of much in the current volume) an anticipatory, evolving language.

Maret put it best, the book "is a guide to the origins and contexts of the words and ideas that drive institutional actions as products of national security information policies. Above all, this guide demonstrates the pivotal, dynamic role language and discourse have in shaping the policies that intersect national security and information."

The audience for the book is varied. This is primarily a reference book for practitioners and scholars, although it also offers material for the satirist and those partial to a Kafkaesque view of bureaucracy. The book seeks to advance understanding of how information and intelligence are used, protected and understood in national security policy. There

are some entries that broaden definitions of national security beyond the military, terrorism and international relations (e.g., to disasters and public health).

Providing common written terms can improve practitioner communication (whether for policy or particular operations, and within, or between, agencies). Specialized words can help define a group and serve solidarity. They can also be useful in education, training, meeting legal requirements, avoiding liability, and creating standards for evaluation and public understanding. For journalists, students, and scholars (categories that need not be opposed) interested in intelligence and FOIA issues it can be something of a Rosetta Stone, helping decipher bureaucratic language, defining new terms and upping their literacy level (not to mention helping them to appear "wise" in knowing the esoteric meanings and language of insiders). In conjunction with references to original sources a dictionary such as this can help trace the development (or genealogy in Foucault's terms) of intelligence ideas and practices.

Comparing dictionaries (or simple definitions in laws and policy documents) across time periods, countries and institutions can highlight cultural differences and social change. Data-analytic software for mining content analysis would find much to analyze here. Looking at changes in the meaning of words and their appearance and disappearance offers an archaeology of the social and mental life of intelligence and security issues. For example, the largest category of terms in this volume begin with "Cyber-" and there is nothing on intercepting telegraph messages or carrier pigeons and no warnings from 1929 that "gentlemen don't read each other's mail."

The organizing principle for the dictionary is simple - start with the letter A (Able Danger a classified U.S. Army data mining initiative) and end with Z (Zombie - a computer program that is installed on a system to cause it to attack other systems) with hundreds of entries in between. The terms run the gamut from everyday words to the largest category—obscure bureaucratic language that only a lifer could appreciate. To more fully give the flavor and fulsomeness of the book, I offer a sampling of terms organized in the following categories: less well known terms associated with spying and surveillance; familiar words with unfamiliar meanings; new terms; terms involving openness and freedom of information; terms identifying sources of error and calling for hubris; The entries below are taken directly from the book; my occasional comments are shown in brackets.

There are terms reflecting common sense understandings (particularly for those who watch the news and enjoy spy and crime fiction). Consider: backstopping, blowback, casing, commercial fronts, crywolf syndrome, defector in place, dead drop, decoy, disinformation, false flag, feint, laundering, legend, malware, mole hunting and misinformation. phishing, tradecraft identity, trap and trace, trash cover, trojan horse.

There are less well known terms familiar to scholars of the dark side arts including spy tools, and references to well-known historical events (Cuban Missile Crisis, Professor Kent Sherman, a major theorist of intelligence). Among the former are BEHAVIORAL DETECTION ANALYSIS PROGRAM (BDA), CARNIVORE and ECHELON, MAGIC LANTERN as well as some less well known shown below.

Some Less Well-Known Terms

ACSS ACTIVE CELL SITE STIMULATORS Also known as a stingray, triggerfish or dirtbag. A tool that mimics cell phone towers in order to reveal cell phone data.

ALPR AUTOMATED LICENSE PLATE RECOGNITION High speed cameras that can capture up to 1880 plates per minute (even if a car is going over 120 miles an hour).

BLACK SITE 1 Classified, secret facilities where defense and/or intelligence activities are conducted....`4. The Chicago Police Department operates an off-the-books interrogation compound, rendering Americans unable to be found by family or attorneys while locked inside what lawyer say is the domestic equivalent of a CIA black site.

BLACK WIDOW To sift through it all, the agency has the world's largest collection of data-eating supercomputers. Its newest, code-named "Black Widow," is a colossal $17.5 million Cray computer made up of sixteen tall cabinets crammed with thousands of processors. It is able to achieve speeds of hundreds of teraflops—hundreds of trillions of operations a second—and the NSA predicts that it will soon break the petaflop barrier, plowing through phone calls, e-mails, and other data at more than a quadrillion operation a second. [Here the term black is used in a very different way than black as in dark, hidden and possibly nefarious. **COVERT OPERATION** 1. Military or political activities undertaken in a manner that disguises the identity of the perpetrators. 2. Operations that are so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. These differ from clandestine operations in that emphasis is placed on concealment of identity or sponsor rather than concealment of the operation."

COVERT PRODUCTS Covert products require exceptional coordination, integration, and oversight. The operations are planned and conducted in such a manner that the responsible agency or government is not evident, and if uncovered, the sponsor can plausibly disclaim any involvement. Gray and black products are employed in covert operations.

DOX, DOXING Dox generally has a negative connotation—not only because it's seen to violate someone's privacy, but also because it's often used as a kind of retaliation mechanism in online discussions. [Sure, but this doesn't tell the

reader what it is. Using Internet resources to research and communicate private information about an identifiable person. A term apparently drawn from "document"].

DRY CLEANING Any technique used to elude surveillance.

EDUCING INFORMATION (EI) From a technical perspective EI encompasses "elicitations (engaging with a source in such a manner that he or she reveals information without being aware of giving away anything of value): "strategic briefing" (systematically covering topics and areas with a voluntary source who consents to a formal interview), and "interrogation" (interaction and conversation with a source who appears initially unwilling to provide information. [Given my interest in deception as a form of soft surveillance (Marx 2017), I was very glad to encounter the reference here to Fein's (2006) work on the topic].

NATIONAL VEHICLE LOCATION SERVICE (NVLS) NVLS is a national data-sharing initiative started by Vigilant Solutions in 2008. [The data comes from law enforcement and "commercial LPR, or 'private' data harvested by Vigilant [next entry].

LAW ENFORCEMENT ARCHIVAL AND REPORTING NETWORK (LEARN) Vigilant Solutions proprietary online portal.... Vigilant claims to have the nation's largest repository of license-plate images with nearly 2 billion records...

MEDIA SANITIZATION The action taken to render data written on media unrecovered by both ordinary and extra ordinary measures. [A rather different meaning than seen in 2017 efforts to control media written by the media.]

NEXT GENERATION IDENTIFICATION (NGI) Developed over multiple years.... advancements in technology and the changing business needs of IAFIS's [Integrated Automated Fingerprint Identity System) customers necessitated the next generation identification services. To further advance biometric identification services, the CJIS Division, with guidance from the user community, established the vision for the Next Generation Identification. See **INTERSTATE PHOTO SYSTM FACIAL RECOGNITION PILOT; NATIONAL PALM PRINT SYSTEM, RAP BACKSERVICE**. [This is a nice example of the new surveillance as it applies to identification. Such surveillance has become ever more data inclusive, precise and easily searchable. Data bases for identification via scent and gait may soon join improvements in facial recognition. New facial images may eventually be available from drones that look like flies and hover like hummingbirds, "snakebots" capable of slithering under doors and cyborg beetles that can portage cameras and other smart sensors. Hudson (2016)]

PLUMBING A term referring to the development of assets or services supporting the clandestine operations of CIA field stations—such as safehouses, unaccountable funds, investigative persons, surveillance teams.

SHEEPDIPPING The utilization of a military instrument (e.g., an airplane or officer in clandestine operations, usually in a civilian capacity .... The term is also applied to the placement of individuals in organizations or groups in which they can become active in order to establish credentials so that they can be used to collect information of intelligence interest on similar groups.

STEGANOGRAPHY The art, science, and practice of communicating in a way that hides the existence of the communication. STELLAR WIND Is a highly classified and strictly compartmentalized program of electronic surveillance within the United States that President Bush directed the Department of Defense to undertake on October 4, 2001.

TEMPEST TRANSIENT ELECTROMAGNETIC PULSE SURVEILLANCE TECHNOLOGY Tempest is the unclassified short name referring to investigation and studies of compromising emanations. [those that are not intended]

TERRORISM INFORMATION PREVENTION SYSTEM (OPERATION TIPS) An idea proposed as a Citizen Corps program that would create a national information-sharing system for specific industry groups to report suspicious, publicly observable activity that could be related to terrorism. The idea was based on programs such as Highway Watch and Coast Watch, which allow truckers and ship captains to report dangerous conditions along their routes.... However, there was resistance to the idea, and the plan was scrapped.

TERRORIST IDENTITIES DATAMART ENVIRONMENT (TIDE) 1. TIDE is that knowledge bank and supports the USG's various terrorist screening or "watchlists" .... As of December 2013 TIDE contained about 1.1 million persons, most containing multiple minor spelling variations of their names.

THREAT SCORE Perhaps the most controversial and revealing technology is the threat scoring software Beware. Fresno is one of the first (police) departments in the nation to test the program. As officers respond to calls, Beware automatically runs the address. The searches return the names of resident and scans them against a range of publicly available data to generate a color-coded threat level for each person or address: green, yellow or red. Exactly how Beware calculates threat scores is something that its maker Intrado, considers a trade secret, so it is unclear how much weight is given to a misdemeanor, felony or threatening comment on Facebook. However, the programs flags issues and provides a report to the user.

YANKEE WHITE A rigorous, special security investigation and background check for military personnel working with the President.

Transcending Usual Definitions

Then there are uncommon definitions that transcend usual meanings:

BIGOT a narrow, select group of people with access to the reports of a particularly sensitive agent or espionage operation [I assume that is an acronym, but it is not spelled out.]

BOLO Be on the lookout

BOOTLEGGING informal agreements by intelligence officers to share data outside established formal channels; seen as a practice between analysts to share data bypassing more formal channels of communication. SEE **STOVEPIPE WARNING**.

DEMONSTRATION Activity to divert a victim's strength and attention from the real or primary operation.

PIANO Clandestine radio

New Terms

Then there are terms or usages I was unfamiliar whose acquaintance I was pleased to make:

AGNOTOLOGY Attributed to linguist Ian Boa, the study of ignorance. [This comes from agnoia, "want of perception or knowledge" and agnosia , "a state of ignorance or not knowing." These are the opposite of gnosis which means knowledge.]

BORDER VIOLENCE INTELLIGENCE CELL (BVIC) Provides intelligence support for ICE weapons-smuggling investigations along Mexican border. This is located within the Crime-Terror Nexus Unit and works closely with partners at EPIC. [One of plethora of units that generally stay out of the public eye. A couple of others are below.]

CONFUSION AGENT An individual dispatched by his sponsor to confound the intelligence or counterintelligence apparatus of another country rather than to collect and transmit information.

CONTROLLED INFORMATION 1. Information conveyed to an adversary in a deception operation. 2. Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign actions advantageous to U.S. interests and objectives.

DANGLE A person controlled by one intelligence service who is made to appear as a lucrative and exploitable target to an opposing intelligence service.

DISRUPTIVE TECHNOLOGY OFFICE Incorporated into IARPA (Intelligence Advanced Research Projects Activity), is a project that provides funds to agencies for R&D activities....

eGUARDIAN In 2007, eGuardian was developed to help meet the challenges of collecting and sharing terrorism-related activities among law enforcement agencies across various jurisdictions. The eGuardian system is a sensitive but unclassified (SBU) information-sharing platform hosted by the FBI's Criminal Justice Information Series, (CSIS) Division as a service on the Law Enforcement Enterprise Portal (LEEP.)

EL PASO INTELLIGENCE CENTER (EPIC) A cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. Its primary concern is drug trafficking; however, intelligence on other crimes is also managed by EPIC. [Not to be confused with EPIC The Electronic Privacy Information Center, a group also concerned with intelligence issues.]

EPIDEMIC INTELLIGENCE SERVICE (EIS) A part of the Centers for Disease Control established in 1951. Following the start of the Korea War as an early warning system against biological warfare. The EIS is composed of medical doctors, researchers, and scientists who serve two-year assignments, and it has expanded into a surveillance and response unit for all types of epidemics, including chronic illness and injuries.

FOREIGN INSTRUMENTEAL SIGNALS INTELLIGENCE (FISINT) Intelligence information derived from electromagnetic emissions associated with testing and operation deployment of foreign aerospace, surface and subsurface systems.

FOREIGN DENIAL AND DECEPTION COMMITTEE (FDDC) Chaired by the National Intelligence Officer for Science and Technology, advises and assists the DNI on foreign activities s that thwart U.S. intelligence through denial and deception (D and D), promotes the effective use of IC resources to counter foreign D and D, and serves as one of four DNI Production Committees.

EXFORMATION Explicitly discarded information.

EYEWASH False entries made in files, usually to protect the security of a source, after indicating that a particular target has rejected a pitch, when in fact the offer was accepted.

FATIDIC relating to predicting fates; prophecies.

ONEIROMANCY The practice of predicting the future of interpreting dreams (not encouraged as a methodology for intelligence analysis). From Greek oneiros (dream.)

FIG LEAF An event or activity of seemingly minor consequence used for the justification of a larger or more important segment of an action.

GHOST DETAINEES The various detention facilities operated by the 800th MP Brigade have routinely held persons brought to them by Other Government Agencies (OGAs) without accounting for them, knowing their identities, or even the reasons for their detention. GHOST PLANE CIA planes ...used in rendering.

GREEN DOOR Slang term for the metaphorical locked door behind which intelligence personnel are said to hide their codewords, secrets and important information not shared with consumers who need and should get it.

LASER INTELLIGENCE (LASINT) Technical and geo-location intelligence derived from laser systems.

MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT) Technically derived intelligence data other than imagery and signals intelligence that locates, identifies, or describes distinctive characteristic of targets.

NATIONAL VEHICLE LOCATION SERVICE (NVLS) NVLS is a national data-sharing initiative started by Vigilant Solutions in 2008. [The data comes from law enforcement and "commercial LPR, or 'private' data harvested by Vigilant [next entry]

LAW ENFORCEMENT ARCHIVAL AND REPORTING NETWORK (LEARN) Vigilant Solutions proprietary online portal.... Vigilant claims to have the nation's largest repository of license-plate images with nearly 2 billion records..."

Open Government

Given an adversarial world overflowing with internecine conflicts, the need for extra ordinary powers to gain intelligence on external and internal threats often requires skullduggery and "grey and black products", although perhaps not to the degree popularly believed, or as put forth by entrepreneurs with self-serving tools and ideologies. The irony of course is that like any powerful tool what protects (e.g., fire) can also harm. This comes through clearly in that, along with the many concepts on the dark side the book offers, there are also entries on classification, leaks, open government and freedom of information issues.

FREEDOM OF INFORMATION ACT (FOIA) Legislation enacted in 1966 with (subsequent amendments) that require federal government agencies to release information requested by a person who submits a formal request. However some categories of information are exempt from disclosure.

FREEDOM OF INFOMATION EXEMTPTIONS The Freedom of Information Act lists 9 categories of information that are exempt from disclosure: documents classified for national security reasons, internal rules and practices, documents exempted by statute, trade secrets, inter and intra-agency specific materials (executive privilege), personal and medical records, records compiled for law enforcement purposes, information used in regulating financial institutions (bank examination reports) and geological information about oil wells and water resources.

LEAKS 1. A Disclosure of classified information or unauthorized disclosure established under EO 10501... According to Steven Hess, [1984] there are six types of leaks: ego leak (giving information primarily to satisfy a sense of self); goodwill leak (information offered to "accumulate credit" as a play for a future favor); policy leak (a straightforward pitch for or against a proposal using some document or insider information as the lure to get more attention than might be otherwise justified... animus leak (used to settle grudges; information is released in order to cause embarrassment to another person); trial balloon leak (revealing a proposal that is under consideration in order to assess assets and liabilities); and the whistleblower leak.

SHADES OF SECRECY COLLATERAL INFORMATION National Security Information classified Top Secret, Secret, or Confidential that is not in the Sensitive Compartmentalized Information or other Special Access Category.

BORN CLASSIFIED Information that is considered a government secret as soon as it comes into existence. Under the information control provisions of the 1946 Atomic Energy Act, practically all information related to nuclear weapons and nuclear energy is "born classified;" no government act is necessary to classify the information. Moreover, the information, defined as Restricted Data, remains secret until the government affirmatively determines that it may be published.

CONTROLLED UNCLASSIFED INFORMATION At present, executive departments and agencies employ ad hoc agency-specific policies, procedures and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patch work has resulted in inconsistent markings and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues. To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of government wide practice.

CIA RECORDS SEARCH TOOL (CREST) Since 2000, CIA has installed and maintained an electronic full-text searchable system... The CREST system is the publically accessible repository of the subset of CIA records reviewed under the 25-year program in electronic format (manually released records are accessioned directly into the National Archives in their original format). Over 11 million pages have been released in electronic format and reside on the CREST databases from which researchers have printed about 1.1 million pages.

FEDERAL ADVSORY COMMMITTE ACT (FACA) The Federal Advisory Committee Act was enacted in 1972 to ensure that advice by the Advisory Committee formed over the years is objective and accessible to the public.

OPEN GOVERNMENT DIRECTIVE In the Memorandum on Transparency and Open Government, issued on January 21, 2009, the president instructed the Director of the Office of Management and Budget (OMB) to issue an Open Government Directive. This memorandum requires executive departments and agencies to take the following steps toward the goal of creating a more open government. 1. publish government information online; 2 improve the quality of government information; 3. create and institutionalize a culture of open government; 4. create an enabling policy framework for open government.

OPEN GOVERNMENT NATIONAL ACTION PLAN In September 2011, the United States released its first Open Government National Action Plan, setting a series of ambitious goals to create a more open government.

DECLASSIFICATION 1. The authorized change in the status of information from classified to declassified.... Classification levels are Top Secret, Secret, and Confidential; declassification "downgrades" these levels in portions of a record-document or the entire material. [There are of course other stops on the train. Consider additional terms such as SBU (sensitive but unclassified), (Need-to-know), YEO (your eyes only), restricted, confidential and my favorite, the Do Not File memo. Calling brother Orwell on the language hotline.]

DECLASSIFICATION GUIDE Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified. Also a guide providing classification and declassification instructions specifically for information that is 25 years old or older and of permanent historical value.

The formal certainty with which such concepts become ingrained within doctrine and practice rarely acknowledge, let alone reflect, on the first question of any good policy or rule, "says who, and why?" Classification issues involve choices and discretion. Decisions here differ from deciding if a shape is square or round or bike is red or white. Discretion is central but it must be carried out within public standards and reviews.

Good Writing

Not surprisingly, some of the most readable and spirited passages come from journalists and scholars outside the fence looking in. Consider:

DIGITAL ASSASSINATION A willful act by someone who wishes to do harm through the internet. It unfolds as a deliberate campaign to spread harmful lies that the assassin has concocted about you or as an attempt to take a fact about you grossly out of context or embellish it, making an ordinary shortcoming seem ghastly. Words are then forged into swords to be thrust into the gut. Digital assassination is most effective when others—as knowing conspirators or unknowing parrots—are incited by social media to trust swords of their own. The result is multiple slices and stabs, leaving a permanent, searchable Internet record that continues to harm your brand, fan base, business, or reputation among friends, customers, investors or other media on a 24/7 basis. (Torrenzano and Davis 2011)

CLIENTITUS. Overly sympathetic analysis of events in the target state; an unrealistic attempt to understand the motivations and values of the target country's leaders or major groups from the perspective of the target. [Or as put by Warren Christopher, former secretary of state, "..a malady characterized by undue deference to the potential reactions of other countries."

CLASSIFICATION PRIESTHOOD National Classification elite is a kind of secret society, closed to the uninitiated. It is a sect marked by a vigorous internal discipline, highly developed rituals, a strict hierarchy, and a consistent philosophy. Central to the philosophy is the principle of compartmentalization. (Hilgarten, Bell and O'Connor 1982)

Such entries contrast with the colorless bureaucratic jargon seen in most of the entries which has very little meaning for the non-specialist. Consider: A-Space (ANALYTIC SPACE) An ODNI project to develop a common collaborative workspace ...for collaboration tools accredited to the HUMINT Control System and Gamma Information Handling (HCS/G) level. [For further information we are told "See I-SPACE." I did and it wasn't much help—being defined as "U.S. Intelligence Community (IC) social networking and collaboration service hosted on JWICS..."]

Calls for Comment

Then there are terms that are noteworthy and call for comment:

AGGREVIED PERSON A person who is the target of an electronic surveillance or any other person whose communications activities were subject to electronic surveillance [This leads me to ask, "aggrieved from whose point of view?"]

COLLATERAL EFFECT Unintentional or incidental effects including, but not limited to, injury or damage to persons or objects that would not be lawful military targets under the circumstance ruling at the time...Such effects are not unlawful as long as they are not excessive in light of the overall military advantage anticipated from the activity [Is there a logician in the house? If they are "not unlawful" does that mean they are "lawful." What criteria apply in determining "excessive"?]

COOPERATIVE DETAINEE A detainee who has established a pattern of answering all questions truthfully and unconditionally and, in fact, answers all questions truthfully and unconditionally [a little redundancy now and then can be emphatic, but why here?]

FACT An event or action that has occurred and has been verified by 2 independent sources. [Holding apart the deep philosophical issues around what a fact "is," one might ask, "why not 1 independent and 3 dependent sources or adding some more adjectives such as 1 super reliable but dependent sources and 2 independent pretty good sources?"]

FAMILY JEWELS Slang term for a 692-page internal CIA report drawn up by order of Director of Central Intelligence James Schlessinger in 1974 so he would not face unpleasant surprises. The report contained details of all CIA operations since 1947 that were or might have been considered illegal, embarrassing, or unwise. [This was leaked to reporter Seymour Hersh and led to the Hughes-Ryan legislation and Congressional inquiries. It is nice example of leaders with the courage to critically look inward such as Schlessinger and of the importance of transparency, whatever its sources.]

FAULT TREE Graphical tool used to illustrate the range, probability, and interaction of causal occurrences that lead to a final outcome. [In a context of intel failures perhaps this has a double meaning.]

EXTRAORDINARY RENDITION and "irregular" rendition. [These are matter-of-factly described with no reference to the legal or moral issues raised.]

If Some Knowledge is Good Is More Better?

As Socrates and the evolution of science suggest, there are times that, "the more we know the less we know." In that regard, it is good to encounter anti-hubris concepts warning of error sources and limitations. In a world filled with unknowns reflecting not only complexity, but constant change and often deception, the intelligence analyst needs cross checking, independent reviewers, humility and more skepticism than the average person. That of course also holds for the scholar. Some concepts appreciating that need:

CREEPING NORMALCY 1. The methodical increment of a country's military capability so that its more capable posture is unnoticeable and accepted over time by outside observers.... 2. The way a major change can be accepted as normally if it happens slowly, in unnoticed increments although it would be regarded as objectionable if it took place all at once or within a short time period. .... The lesson to be learned is that people should make themselves aware of gradual change lest they suffer a catastrophic loss.

DISSENT CHANNEL The State Department has a strong interest in facilitating open, creative, and uncensored dialogue on substantive foreign policy issues within the professional foreign affairs community, and a responsibility to foster an atmosphere supportive of such dialogue, including the opportunity to offer alternative or dissenting opinions without fear of penalty. The Dissent Channel was created to allow its users the opportunity to bring dissenting or alternative views on substantive foreign policy issues, when such views cannot be communicated in a full and timely manner through regular operating channels or procedures, to the attention of the Secretary of State and other senior State Department officials in a manner which protects the author form any penalty, reprisal or recrimination. [The same logic underlies legislation protecting whistle blowers and channels for anonymous communication. To the extent that there is awareness of the above the need for transparency to reveal cover ups is lessened. Structure matters. Beyond creating channels that can bypass the chain of command, decentralized forms of organization with fewer levels from top to bottom of hierarchy are more conducive to open and honest flows of information.]

HUGGER-MUGGER, CIRCULAR INTELLIGENCE These refer to information that is reported as an unconfirmed factor or assessment that is subsequently repeated in another agency or analyst's assessment as a true report. [One of a number of entries dealing with intelligence mistakes.]

PARADOX OF COLLECTION As additional information is collected, the analyst becomes inundated with intelligence leading to ambiguity and uncertainty and thus making the person more ignorant. By collecting more intelligence, the analyst is exposed to more variables that can lead to more uncertainty.

PARADOX OF EXPERTISE The more a person becomes an expert in a particular area or field of study, the more likely that person will miss exchanges that would normally be detected by those with less knowledge or experience. The strengths of expertise can also be weaknesses, as reflected in the saying "He kept missing the forest for the trees." [One might also add "to a person with a screwdriver everything looks like a screw."]

Some Modest Limitations

Nowadays, the respectable reviewer can't get away with just doing a book report, rather, readers expect something critical. I can't help much there. I liked the book and enjoyed dipping into it over several months. I do however have a few minor criticisms. Beyond some general comments, we are not told with much specificity what the criteria were for including items. Nor is there any commentary on specific entries. Given the authors' experience and knowledge, it would have been helpful to have their take and additional context for some of the statements, perhaps offered in footnotes. As with other dictionaries, this one generally does not use quotation marks. Dictionaries are the sources which require other writers to use such marks. But in this case some statements are taken from books and articles and it is not always clear if the quotes are direct, or reflect the author's paraphrasing or emendations.

But more significantly, the book needs an index, although its length is no doubt a factor against an index. The alphabetical organization offers a kind of mock index with its logical order (indeed a 640-page index!), but the topics are so rich, and there is so much crisscrossing among the concepts that relying on the first letter of the first word in a multi-worded term is not particularly helpful. Organization by topics (e.g., information, intelligence and counter-intelligence, cyber threats, classification and declassification, covert means, legislation, congressional and commission reports, major historical events, to mention only a few possibilities) would be helpful. Absent that, symbols indicating the kind of topic would be helpful. A glossary spelling out the many undefined acronyms (in particular those contained within a definition) would also be helpful.

While there is something to be said for the serendipity of wide exposure, I waded through more than 3000 definitions in 640 pages to find ones directly connecting with my research interests. Perhaps that is the price a responsible reviewer must pay, but not so the reader.

A dictionary represents a discretionary codification and can provide a shared standard for meaning across readers/listeners. But it can only take us so far. For any given term, there can be chasms between the intent of the initial definer and subsequent interpretations by users (not helped when more than one meaning is present), nor can it separate serious statements from those intended as humor. Nor is it necessarily a guide to behavior. But the terms in official statements matter as important factors in the environment ("structure") within which behavior occurs, whether to guide it or as something to work around. The definition (even if disregarded by those within an agency) is important because it represents a kind of official, front-stage presentation. It is an exercise in advertising or impression management in Goffman's (1956) terms.

Children in a spelling bee asked to also define the word they are given have no need to probe the origins or uses of the term. But that is not so for the critical scholar who is aware of the social construction of names, their definitions and formats. A dictionary along with other linguistic forms such as the lexicon, glossary, thesaurus and encyclopedia and more distantly the novel, comic book, letter, diary, newspaper and magazine were all at some point invented.

A dictionary, like a bridge, is constructed. When the creator is a transmitting editor, we need to ask questions about the social locations and interests of those from whom the words are taken. That also holds for the compilers (quasi-authors?) who build on other's or offer their own definitions. As Susan Maret suggests in her introduction, a sociology of knowledge analysis (Mannheim 1972) regarding its construction is needed. How were the words and sources for the definitions chosen? To what extent do the words reflect the social, political and psychological location and experiences of the creator of the dictionary?

To its credit and the envy of researchers elsewhere, the United States goes further than most countries in making so much information about its intelligence organizations available—and online at that. Yet in writing about secrecy, particularly when it involves professionals at dissimulation and hiding, the reader wonders what was left out? Are some of these "unclassified" terms themselves examples of disinformation and misinformation? What other terms are only defined in classified documents?—(the outsider's "unknown unknowns" or those that are suspected or imagined). Terms reflecting popular culture terms such as "do not file, files", "terminate with extreme prejudice, "wet" or "black bag jobs" are not included, although other popular terms are such as back channel, brush contact and bug (to grab some from the B entries). How deep is the iceberg? Do unclassified dictionaries based on unclassified documents tilt toward the more,

rather than the less, savory aspects of the intelligence craft? Is there a kind of word laundering and euphemism creation that takes place? This alerts us to the dangers of confusing formal written policies with informal, off the books actions about which the outside researcher asking questions is politely told, "you don't want to know."

Yet, with this volume the reader who does want to know, can indeed learn things only available to insiders, whether because of secrecy, compartmentalization or the vastness, opaqueness and dynamism of the topics. The learning comes not so much from the single entry success noted by Twain, but from subsequent exploration of discrete elements that may combine into a mosaic—collecting the bread crumbs in order to create a loaf (or at least part of one). Pursuing the URL threads (and subsequent threads) the book offers was a pleasant and productive diversion from completing this review. The book is a valuable research tool in the endless quest for knowledge regarding how we can best be protected both by, and from, those with power.

References

Fein, Robert A. 2006. "Intelligence Science Board Study on Educing Information Phase 1 Report." In *Intelligence Science Board. Educing Information—Interrogation Science and Art: Foundations for the Future*. National Defense Intelligence College. Accessed July 17, 2017. http://www1.umn.edu/humanrts/OathBetrayed/Intelligence%20Science%20Board%202006.pdf

Goffman, Erving. 1956. The Presentation of Self in Everyday Life. New York: Doubleday.

Goldman, Jan. 2011. Words of Intelligence: An Intelligence Professionals Lexicon for Domestic and Foreign Threats. Lanham, MD: Scarecrow Press.

Hess, Stephen. 1984 The Government Press Connection: Press Officers and Their Offices. Washington DC: Brookings Institution.

Hilgarten, Stephen, Bell, Richard C., and Rory O'Connor.1982. Nukespeak. New York: Penguin.

Hudson, Mathew 2016. "What Surveillance Will Look Like in the Future" *The Atlantic Magazine*, November 2016.

Mannheim, Karl. 1972. Ideology and Utopia. London: Routledge.

Maret, Susan. 2015. On Their Own Terms: A Lexicon with an Emphasis on Information-Related Terms Produced by the U.S. Government. 4th revised edition. Federation of American Scientists. Accessed July 17, 2017. http://www.fas.org/sgp/library/maret.pdf

Marx, Gary T. 2017. Windows Into the Soul: Surveillance and Society in an Age of High Technology. Chicago: University of Chicago Press.

Torrenzano, Richard, and Mark Davis. 2011. Digital Assassination: Protecting Your Reputation, Brand, or Business against Online Attacks. New York: St. Martins Press.HR>

Gary T. Marx home page | Top