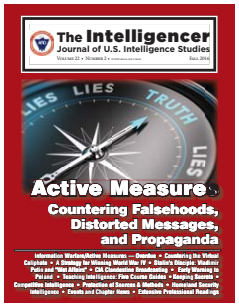

From AFIO's **The Intelligencer**
Journal of U.S. Intelligence Studies
Volume 22 • Number 2 • $15 single copy price **Fall 2016**

Association of Former Intelligence Officers
7700 Leesburg Pike Ste 324, Falls Church, VA 22043.
Web: www.afio.com. Email: afio@afio.com

The Protection of Intelligence Sources and Methods

Dr. Robert M. Clark

I have grown to love secrecy ... the commonest thing is delightful if one only hides it.

— Oscar Wilde

To the new initiate, the US Intelligence Community's system of security protections is a confusing maze, and its compartmentation system for protecting highly sensitive information is sometimes overwhelming. The protection system is loosely called the compartmentation system. It is a system that is sometimes misused, frustrating to understand, but it all really makes sense. To understand why it makes sense, one must go back to the system's origins. It helps to understand how the system evolved, and what it is protecting. Also, it has a lot of colorful history.

The system of protecting sources and methods can be better understood by answering one key question: *If this information were revealed to an opponent, how much damage would we suffer?* The answer to this question determines the nature of the protection. To understand how we have answered that question over the years, let's start with some history.

Historical Development

Until about 1960, the US (and British Commonwealth) control systems for protecting sources, methods, and the intelligence product was as described below. Most other countries had similar systems for protection of their intelligence resources.

HUMINT

The clandestine collection of intelligence through human sources (HUMINT) goes back at least to biblical times, when the Israelites spied out the land of Canaan. This first attempt, incidentally, was a disaster (its direct result was 40 more years of Israelite wandering in the wilderness) for reasons familiar to any intelligence analyst: unreliable sources.

HUMINT was developed to a fine art by Sir Francis Walsingham, Queen Elizabeth I's skilled spymaster, who established many of the basic principles of a clandestine service.[1] The two levels of protection that exist today date from his time (at least). The distinction is between the *product* of HUMINT and the *sources and methods*, and the key to the distinction is need-to-know.

The highest level of protection is placed on information that might allow someone to determine the identity of the source (the agent). Loss of this information usually results in someone being imprisoned or killed, loses the source permanently, and discourages others from volunteering to become agents. Therefore, a high level of protection of the source is necessary. The protection for this information was called the BIGOT list.[2] The term "BIGOT" is not used here in a pejorative sense, but merely in the sense of narrow, or restricted in access. The term originated when the allies were preparing for the Normandy invasion during World War II. Everyone with knowledge of the invasion plans, codenamed Operation Overlord, received security clearances and was listed on what was known as the BIGOT list – BIGOT being short for "British Invasion of German Occupied Territory."

Many such lists have been created since to protect HUMINT sources. Each list contains the names of individuals who need to know, for example, the true name of a specific agent. The lists are tightly controlled, but are not a formal control system.

The lower level of protection is on the content of information provided by a source. Such information, if lost, only reveals what you know, but not how you know it. This level of information is included in HUMINT reports that are sent to the intelligence analysis community. It is typically classified SECRET or below, though TOP SECRET reports are used to protect especially sensitive information. Codewords are not normally used.

The US State Department produces HUMINT reporting, though the department eschews the use of the term HUMINT (officially, Foreign Service officers do not engage in intelligence activities). So diplomatic reporting may be classified, but State also uses terms such as Limited Dissemination (LIMDIS), Exclu-

1. Allen Dulles (1977), *The Craft of intelligence*, Greenwood Press edition, p. 18.
2. U.S. Senate. Final Report, *Book I: Foreign and Military Intelligence*, Final Report of the Select Committee to Study Governmental Operations, 94th Congress, 2nd session, Report no. 94-755, April 26, 1976.

sive Dissemination (EXDIS) and No Dissemination (NODIS) markings to protect sources and methods.[3]

COMINT

Communications Intelligence (COMINT) – the interception and analysis of communications – predates the use of radio. Any follower of old Western movies is familiar with the frequently repeated scene where a US Cavalry scout deciphers Indian smoke signals. Military units were deciphering messages sent by their opponent's flag signaling systems immediately after the systems were invented. COMINT began to expand markedly after radio was introduced. The Russians lost their first major battle of World War I, at Tannenberg, primarily because the Germans intercepted Russian high frequency radio communications and thereby knew the exact deployment of Russian field armies. COMINT during World War I included both radio intercept and the tapping of telephone lines laid by armies in the field; it expanded after World War I to include information obtained from wiretaps and hidden microphones (bugs). Encryption came into wide use to protect against COMINT, and cryptanalysis came into wide use as countries attempted to break each other's diplomatic codes and encrypted military communications. (Encryption and cryptanalysis, of course, predate both electronic communications and COMINT).

The original protection of COMINT information was basically the same as for the BIGOT system used in HUMINT: lists of persons approved for access. This approach was found to be unsatisfactory as a result of the Pearl Harbor surprise attack. US cryptanalysts had broken the codes that provided warning of the attack, but compartmentation contributed to keeping the information from those who could have benefited.

It was clear that a BIGOT system would not work for COMINT; too many people had to have the COMINT product. Though the loss of COMINT information would not directly cost human lives, it could cause loss of the source (the opponent would develop a new encryption system). COMINT organizations would lose valuable information if a compromise occurred, and it was expensive to break new encryption systems.

The result was the beginning of the COMINT compartmentation system during World War II. Under this system, only cleared and briefed people (usually senior government officials and military commanders) had access to the product information.

The codeword system has evolved into the present Special Intelligence (SI) control system, which uses two classes of compartments and associated security systems.

- One class protects the sources and methods: access is usually granted only to SIGINT collectors and processors. It functions much like the BIGOT list. A large number of compartments exist in this set.
- The second class protects the product, and access is granted to a wide range of people.

The SI control system's extensive use of SIGINT-only compartments leads to some amusing exchanges. In one case, a senior US military officer found out that his National Security Agency (NSA) contact was providing sensitive material to the Government Communications Headquarters (GCHQ, the British SIGINT organization). In response to his question "How can you give it to the British, but not to me?" the NSA man replied "Well, they're SIGINT, you're not."

IMINT

Imagery Intelligence (IMINT) originally was called Photographic Intelligence (PHOTINT), and was conducted by reconnaissance aircraft. Aerial photography matured as an intelligence discipline during World War II, and photo interpreters (PIs) became common in all military services. There were no special controls on imagery, because the information needed to be made available quickly to field commanders. Very little protection of sources and methods was needed anyway, because when a reconnaissance aircraft flew overhead, it was obvious to the enemy that you were taking their pictures. Most aerial photography was classified secret or below.

The term IMINT became standard during the Cold War because it included, in addition to standard photography, infrared photography, multispectral imagery, and radar imagery. With the 1996 establishment of the National Imagery and Mapping Agency (NIMA), the geospatial intelligence concept was born, combining imagery with geographical information. When NIMA changed its name to the National Geospatial-Intelligence Agency (NGA) in 2003, GEOINT became a standard intelligence discipline similar to SIGINT and HUMINT.

3. Office of the Director of National Intelligence [ODNI], *Intelligence Community Classification and Control Markings Implementation Manual*, Vol. 4, Ed. 2, 31 May 2011, *https://www.fas.org/sgp/othergov/intel/capco_imp.pdf*.

ELINT

Electronic Intelligence, or ELINT, is a SIGINT sub-discipline. It refers primarily to the collection and processing of the signals emitted by radars. It dates back to the first use of radars in combat. Like IMINT, ELINT was not tightly protected during World War II, and most ELINT today continues to be classified secret or below. Little protection of sources and methods was needed because, when an opponent uses radar, he has to assume that you will intercept it; and denying ELINT collection is very difficult.

FISINT

Foreign Instrumentation Signals Intelligence (FISINT) refers to the collection and processing of signals collected from a missile, aircraft, or satellite platform – primarily telemetry. Telemetry signals give status and performance characteristics of the platform. Telemetry signals are useful for predicting the performance of weapons systems that are in testing phase, and for assessing the operations of satellites. In FISINT, our ability to break out the telemetry channels and determine the meaning of each channel signal is the important method to protect. FISINT therefore resembles COMINT – the processing part needs a very high level of protection.

Open Source

Little or no special protection is given to the open source "INT," and since the source material is unclassified, it seems difficult to justify any protection. However, the techniques for exploiting open source material, and the specific material of interest for exploitation, can tell an opponent much about an intelligence service's targets. For this reason, NSA has for years marked its translations of open source as "Official Use Only." A restrictive marking also allows a government to ignore copyright laws while limiting use of the material. Corporations make use of similar restrictive markings on material that is translated or reproduced for in-house use, for the same reasons – concealment of interest and avoidance of copyright problems.

A more serious reason for protecting open source exploitation methods is that, if your opponent knows what your target materials are, it is easier for him to carry off a successful deception. The US has long been aware that many intelligence services translate and avidly read *Aviation Week and Space Technology* (AW&ST). Within the intelligence community, *Aviation Week* was often referred to as "aviation leak." When the Defense Department wishes to mislead or deceive another country about US capabilities and intentions, *AW&ST* is the natural place to attempt to "plant" the misleading story.

The Modern Compartmentation System

Since about 1960, an extensive new control system has developed for protecting sensitive intelligence information. It had its origins in the US decision to conduct peacetime photoreconnaissance over the USSR using the U-2. Because such flights violated international law, the consequences of their exposure were expected to be severe (and in fact, their exposure subsequent to the U-2 shootdown did cause severe consequences). Therefore, the compartmentation on both the sources and methods and on the imagery product (since the product revealed the fact of such reconnaissance) was very tight.

Clearly, the US was not protecting the "fact of" reconnaissance from the Soviets; they were well aware of the overflights. So long as the US did not publicize the overflights, however, the Soviets found it expedient not to do so themselves – at least, until they could shoot one of the U-2s down.

By the time of the 1960 U-2 shoot down and the termination of all aircraft reconnaissance overflights over the USSR, the US was already building the first reconnaissance satellites. Satellite reconnaissance, however, posed several unique security concerns.

- By necessity, satellites overfly many international boundaries. The USSR launch of Sputnik I established the principle that satellites could legally overfly other countries. In the 1960s, however, it was not clear whether satellites could legally conduct reconnaissance during such overflights, and the right of another country to shoot down a "spy satellite" over its territory was in dispute.
- If a US airplane deliberately overflies a hostile country's territory, the opponent can assume its mission was intelligence collection. In contrast, an opponent could not easily determine whether a satellite was an intelligence collector.
- Satellites are very expensive to build, launch, and support. The more opponents know about a reconnaissance satellite, the easier it is for them to counter its mission. The high cost of any disclosure of sources and methods argued for a stringent security system.

The Kampiles case illustrates the importance of protecting the details of satellite reconnaissance. The

US lost a significant advantage in intelligence collection when former CIA employee William Kampiles, who had resigned after failing to qualify as an overseas operations officer, sold the technical manual for the new KH-11 satellite to the Soviets for $3,000 in 1977. The KH-11 was the first imagery satellite that could transmit its images to earth in near real time. Because it did not downlink directly to a ground station, the Soviets did not intercept any signals from the satellite, leading them to believe that it was a system failure. Therefore, they took no security measures when the satellite passed overhead. The National Reconnaissance Office (NRO) collected valuable imagery of new Soviet weapons systems being tested in the open until the Soviets realized that the satellite was a new system that transmitted its imagery away from the earth to a relay satellite in higher orbit. The surprise factor was lost. Knowing its capabilities, the Soviets took measures to conceal sensitive activities and deny the US valuable intelligence.[4]

The Sensitive Compartmented Information (SCI) protection system, which originated in US peacetime aircraft and satellite reconnaissance, provides two levels of protection, much like the COMINT control system. An extensive set of compartments was developed to protect collection sources and methods, and another set was developed to protect the product.

Since the 1960s, a number of separate compartmentation systems have evolved within the SCI system. Three examples illustrate the nature of these compartments.

The BYEMAN and RESERVE Systems

After the NRO was created in 1960, it adopted a compartmentation system to protect its system development process as well as its operations. Under the BYEMAN compartmentation system, an extensive set of sub-compartments, with codewords assigned to each, was created to protect specific systems and studies. Persons having access to the system development for a specific overhead system might not, for example, be permitted access to the operations part, and would not automatically be permitted to know anything about other overhead systems.

A number of efforts were made to shrink the number of compartments within the BYEMAN system. Criticisms of the NRO security system came from both outside and inside the organization. An NRO inspector general report noted that there are "numerous examples of over classification and use" of the BYEMAN compartment. The NRO security system, the report noted, is often used as the excuse to bypass or mitigate established procedures and controls. A special panel review (the Jeremiah Panel review) noted that the practice of using the NRO security system as something more than a security compartment existed within the NRO. It also noted the perception by many outsiders that the NRO uses its security system selectively and arbitrarily to restrict what is seen as legitimate access to NRO information.[5]

The BYEMAN control system was retired on 20 May 2005; the system became unwieldy, as more and more defense officials needed knowledge of satellite systems and their capabilities. However, the principles of compartmentation were retained and sensitive operational details and system vulnerabilities continued to be protected from general knowledge. The most sensitive of such material is now protected in compartments within a new NRO control system called RESERVE.[6]

The HUMINT Control System

A formal compartmentation system now exists for the control of human source intelligence, entitled the HUMINT Control System (HCS). HCS covers both source identity and sensitive reporting.

The GEOINT Control System

The National Geospatial-Intelligence Agency (NGA) uses the KLONDIKE control system as an SCI control system to protect sensitive geospatial intelligence (GEOINT).[7]

A Note on Codewords

Those whose job involves working with the military or intelligence communities soon learn about codewords. They are endemic to both, and most of them, in the military at least, have little or nothing to do with intelligence.

But the intelligence compartmentation system does rely heavily on codewords in protecting sources

4. Defense Security Service Security Research Center, *Recent Espionage Cases, 1975-1999,* (Monterey, CA: Defense Department, 1999), 41; George C. Wilson, "Soviets learned of spy satellite from U.S. manual," *Washington Post*, November 23, 1978 at *http://www.jonathanpollard.org/7890/112378.htm*.

5. Report of the Jeremiah Panel on Defining the Future of the NRO for the 21st Century, Chapter IX, Security, 26 August 1996 (Unclassified Extract).

6. ODNI, *Intelligence Community Classification and Control Markings Implementation Manual*, Vol. 4, Ed. 2, 31 May 2011, 146, *https://www.fas.org/sgp/othergov/intel/capco_imp.pdf*.

7. Ibid.

and methods. Today, codewords are an essential part of the intelligence information management process. Codewords and compartmentation, though, are two separate things. Compartmentation is the system for controlling access to classified information. Codewords are short names used to identify the control systems.

Codewords, in both military and intelligence, serve several purposes, though not all of the purposes served are legitimate. If properly chosen, they are useful in protecting programs from hostile intelligence efforts. This is, in fact, their main legitimate purpose.

- Codewords are a convenient way to define something – a concept, a collection program, a software project – in a brief word. They allow quick identification of security access to a specific compartment.
- Codewords are more easily remembered, especially at budget time. A project with a code name acquires special stature, especially if the code name is protected by compartmentation.
- Codewords, when protected by compartmentation, can shield programs from scrutiny, especially from auditors and budget-cutters.

Codewords have been used in industry for years, and the computer industry is particularly fond of them. Apple Computer executives have consistently followed the prudent course of choosing codewords that "evoke inappropriate images."[8] Names like "Lisa" provide no clue as to the project nature, and "Macintosh" provides only a slight clue; whereas, when your current product is named iPhone 6, a codename such as iPhone 7 could tell a great deal to an industrial spy.

Fortunately for intelligence analysts, a powerful temptation exists for military officers to choose codewords that have some meaning, often ones that represent an insider joke. The Germans during World War II were particularly vulnerable to this temptation:

> *One of the more inappropriate codewords was the one the Germans chose during World War II for their air raid of 14-15 November 1940, which devastated the British city of Coventry. The name, "Moonlight Sonata," correctly suggested to British Intelligence that the raid would be conducted at night, near the time of the full moon.*[9]

The British did not act effectively on the intelligence, and Coventry suffered; but that is another story. Intelligence has its limits, and it does not make operational decisions.

> *Another time, the Germans chose the nickname "Freya" for a new aircraft detection system. The name provoked R.V. Jones, while waiting for photography of the new system, to do some research on mythology. Freya, the Nordic goddess of Beauty, Love, and Fertility, had a prized necklace called Brisingamen. Its guardian, the watchman of the gods, was Heimdal; and Heimdal could see one hundred miles in every direction, day or night. Jones cautiously (but correctly) reported that the system was probably a radar, and gave an estimate of its range performance based on the nickname.*[10]

The US still uses codewords that evoke appropriate images. In the days leading up to the Gulf War, the US adopted the codeword "Desert Shield" for its preparations – evoking a fairly clear image of a defensive deployment in the Saudi Arabian desert; and once the opponent understands the meaning of this codeword, then the codeword "Desert Storm" conveys a very clear image of what is to happen next.

In contrast, the Russians and British have been able to resist the temptation to assign nicknames or codewords that have meaning, and even in some cases to choose codewords that were carefully designed to mislead intelligence analysts. A famous example is the British use of "tank" during World War I for machines that, when enclosed in canvas for transport to the front, looked like fuel storage receptacles of the same name. The Russians learned this lesson well, and they consistently rely on neutral codewords, heavily oriented to names of natural objects – rivers and bodies of water, rocks or minerals. It once seemed that every third Soviet program was nicknamed "Almaz" (Russian for "diamond"). The use of the same codeword for different programs, in fact, makes the intelligence analyst's life much more difficult because separating fragments of information into the proper program becomes harder. The British tend to rely more on names of man-made objects; for example, "window" was the British codename in World War II for reflecting chaff that is dropped from aircraft to confuse enemy radar. In contrast to the US codeword approach to Gulf War preparations, the British adopted the unevocative codeword GRANBY for its RAF deployment to the theatre; a Defense Ministry computer randomly selected GRANBY .[11]

8. John A. Barry, *Technobabble* (Cambridge, MA: MIT Press, 1992), 142.
9. N. E. Evans, "Air Intelligence and the Coventry Raid," RUSI/RMAS Research Centre Bulletin 121 (3), September 1976.
10. Alfred Price, *Instruments of Darkness: The History of Electronic Warfare, 1939-1945* (London: William Kimber, 2006) 78.
11. Mark Urban, *UK Eyes Alpha* (London, Faber and Faber Ltd., 1996), 155.

All countries, however, tend to fall into the consistency trap in assigning codenames, as the British and Russian examples above suggest. NATO designators for Soviet aircraft always began with "B" if the aircraft was a bomber and "F" if it was a fighter; one-syllable names indicated propeller-driven, two syllables indicated a jet. Thus BEAR would be a prop-driven bomber, FOXBAT a jet fighter. For a long time, one could tell that a program originated in the US Air Force, and which USAF group originated it, by the first word of the two-word nicknames that USAF selected. Codenames such as "HAVE xxxx" or "PAVE xxxx or "RIVET xxxx" were part of a series, for example, and conveyed specific information about the associated program. (The "xxxx" refers to a specific program name, e.g. RIVET JOINT, RIVET BRASS.) Codenames such as "CLASSIC xxxx," "SENIOR xxxx," or "COMPASS xxxx" had similar patterns. The temptation to choose codewords in such series is understandable, since a codename that fits into a familiar pattern has more legitimacy with budgeteers. However, such patterns are a gift to hostile intelligence analysts. Over time, this has become less of a problem, as many codewords (especially within the US Intelligence Community) now are randomly generated.

In Conclusion...

The US compartmentation system has frustrated, amazed, and confused most of us on occasion. Furthermore, the continuing proliferation of special compartments seems counter to the stated missions of the Director of National Intelligence (DNI): to lead intelligence integration and forge an Intelligence Community that delivers the most insightful intelligence possible. But one of the DNI goals is to "drive responsible and *secure* information-sharing"[12] [emphasis added]. For all of its flaws, the compartmentation system continues to serve us well in that regard.

Robert M. Clark, Ph.D., J.D., is a consultant for the US Intelligence Community, a faculty member of the Intelligence and Security Academy, and adjunct professor of intelligence studies at the University of Maryland University College and Johns Hopkins University. Dr. Clark served in the United States Air Force as an electronics warfare officer and intelligence officer. At CIA, he was a senior analyst and group chief managing analytic methodologies. He subsequently was President and CEO of the Scientific and Technical Analysis Corporation. Dr. Clark has published three books: *Intelligence Analysis: A Target-centric Approach*, now in its fourth edition; *The Technical Collection of Intelligence*, published in 2010; and *Intelligence Collection*, published in 2013. He is co-author of *Target-Centric Network Modeling*, and co-editor of *The 5 Disciplines of Intelligence Collection*, both published in 2015.

12. DNI Mission, Vision, and Goals, *http://www.dni.gov/index.php/about/mission*.