From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 20 • NUMBER 2 • $15 SINGLE COPY PRICE Fall/Winter 2013 ©2013, AFIO

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
Web: www.afio.com, E-mail: afio@afio.com

Guide to the Study of Intelligence

Perspectives on Intelligence Collection

by Robert M. Clark, PhD

INTRODUCTION

Intelligence is collected in many ways – from spies, eavesdropping, technical sources, and openly available materials. The various means are traditionally described as "intelligence disciplines" or, in shorthand, "INTs." The term "INT," however, has also been applied to a few specialized analysis disciplines, resulting in some confusion: is a concept having an "INT" suffix a collection INT, or an analytic method?

How you view the intelligence collection INTs depends on where you sit. Collectors have a specific view of the collection function, structure and process. And for them, it makes sense. It follows the US intelligence community organization. Analysts, to do their jobs most effectively, need to take a different perspective, one that is not closely tied to the existing functional or structural divisions. Let's examine those views, starting with function.

FUNCTIONAL VIEW: THE COLLECTOR'S AND ANALYST'S PERSPECTIVES

The traditional and easiest to understand view of collection divides the sources up by following the existing organizational structure. For the U.S., this results in the breakout shown in Figure 1. For a collection manager, Figure 1 is the simplest and most logical way to view the functions performed by collection. So we have large collection organizations such as the National Geospatial-Intelligence Agency (NGA) responsible for imagery (IMINT) collection, and the National Security Agency (NSA) responsible for signals intelligence (SIGINT). These are the *stovepipes* that intelligence professionals know well. Though they make collaboration difficult, stovepipes serve a number of essential purposes.

Collectors sometimes refer to these as "cylinders of excellence", which provides a clue as to how the divisions developed historically and a reason to functionally view them through that lens. Each stovepipe has built a critical mass of expertise, an elite force that its members consider to be the best in the world at what they do. Another reason that the stovepipe structure works well for collectors is that it identifies the *functional managers* of the major collection INTs. Functional managers have the job of protecting equities. They must plan for collection and define the areas of responsibility for the various INTs.

Primarily, functional managers must ensure that the entire collection process is effectively and efficiently managed, and they must argue their case for budget dollars each year.

As Figure 1 is the simplest and most logical way to view the functions performed by collection, there is

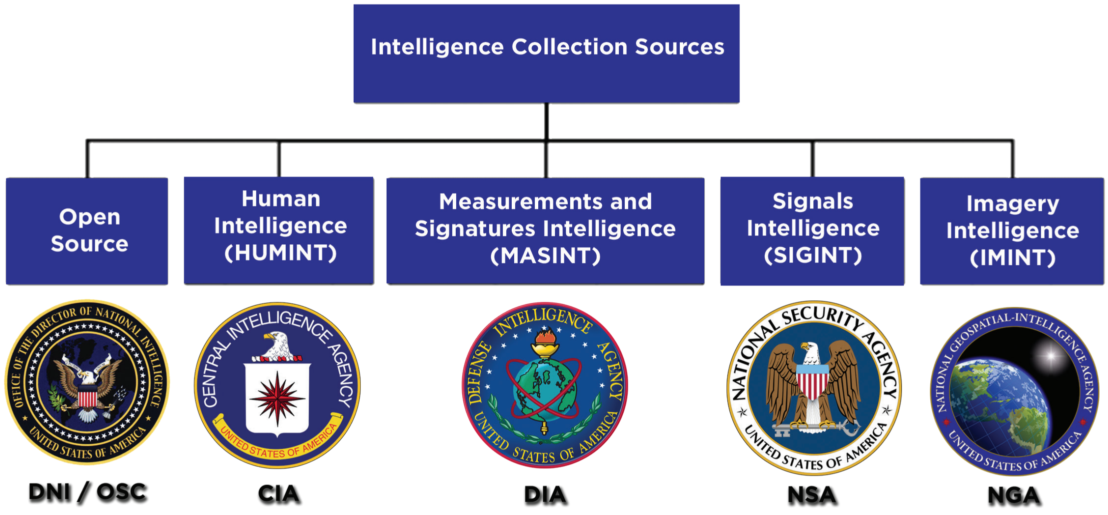

Intelligence Collection Sources
Open Source
Human Intelligence (HUMINT)
Measurements and Signatures Intelligence (MASINT)
Signals Intelligence (SIGINT)
Imagery Intelligence (IMINT)
DNI / OSC
CIA
DIA
NSA
NGA

Figure 1: Collector's Functional View of Intelligence Collection

another way to view collection functionally, shown in Figure 2. It's important to understand the difference, because it shapes how analysts can best collaborate with collectors and deal with customers.

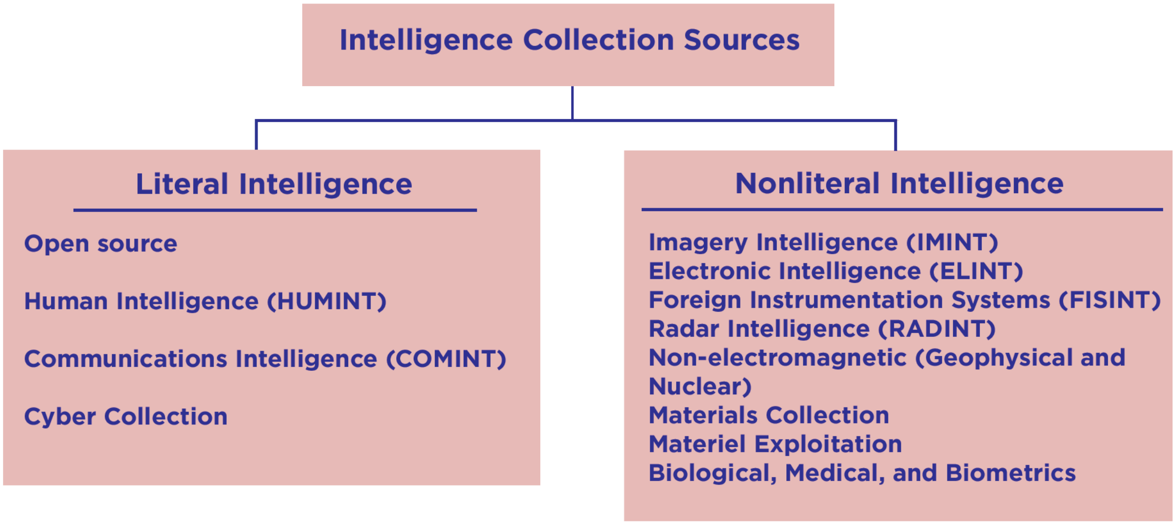

Intelligence Collection Sources
Literal Intelligence
Open source
Human Intelligence (HUMINT)
Communications Intelligence (COMINT)
Cyber Collection
Nonliteral Intelligence
Imagery Intelligence (IMINT)
Electronic Intelligence (ELINT)
Foreign Instrumentation Systems (FISINT)
Radar Intelligence (RADINT)
Non-electromagnetic (Geophysical and Nuclear)
Materials Collection
Materiel Exploitation
Biological, Medical, and Biometrics

Figure 2: Analyst's Functional View of Intelligence Collection

One type of collection produces *literal* information. It's the form that we use for everyday communication. Analysts understand how literal intelligence is collected and used. It requires no special exploitation after the processing step (usually just language translation) to be understood. It literally speaks for itself.

Nonliteral information, in contrast, usually requires expertise in special processing and exploitation in order for analysts to make use of it. Most customers don't understand it. British author Michael Herman also has written that there are two basic types of collection. He describes the types on the left as "Access to human thought processes" and the types on the right as "Observations and measurements of things."[1]

There are at least a few reasons for thinking this way about collection as an analyst. First, analysts request the types of collection that they need, without a focus on where the collection actually comes from or which specific organization it resides in. Though Figure 1 identifies the functional manager for each type of collection, it doesn't accurately describe where collection actually occurs. DIA and the military services collect more HUMINT than CIA does, and the State Department is a key HUMINT provider (although diplomatic reports are not officially termed "intelligence"). NSA collects MASINT signals. All the organizations in Figure 1, and several others, collect open source.

Both literal and non-literal collection are essential, of course. But, a second reason analysts use this functional delineation is that the two have to be judged differently. For example, literal intelligence can help determine intent and do predictive analysis, while non-literal collection usually cannot. A weakness of literal collection, though, is that people are less reliable than the scientific measurements collected non-literally. People may be misinformed or lie. During World War II, General Rommel lied to Berlin about being short of supplies. The British, intercepting Rommel's communications, mistakenly believed him and attacked. Saddam Hussein's generals routinely lied to him about their capabilities, and he in turn lied to them about having weapons of mass destruction (WMD).

Third, when making an assessment, analysts have to be wary of literal and non-literal specific biases. In literal collection, they must rely on translators. For non-literal, they must rely on the processor or exploiter's judgment. Customers sometimes receive and tend to act on raw literal collection, because they can readily grasp it. That is not necessarily a good thing, because they are not trained analysts. But this functional view helps them see where they may be able to give input and where they may not challenge the collection. Interpreting a hyperspectral image or an ELINT recording isn't usually within a customer's skill set.

[1] Michael Herman, *Intelligence Services in the Information Age* (New York: Frank Cass Publishers, 2001), 82.

TWO VIEWS OF THE PROCESS:

The Intelligence collection process is typically portrayed as a one cycle loop: question in, answer out. Figure 3 illustrates what the inside of a stovepipe looks like. It makes a nice picture but does not convey what is actually happening. Instead, collection is a highly iterative and continuous process. Collectors jump around a lot in the diagram of Figure 3.

Collectors often refer to the 'front end' and 'back end' of the process, as indicated. And Figure 3 also illustrates what they mean. In this view, the "cycle" divides into three distinct stages: Requirements and Tasking are the "front end." Collection is the middle action. And processing, exploitation and dissemination are referred to as the "back end". In an ideal system, you'd then identify the gaps in knowledge, revise the requirements, and the process begins anew.

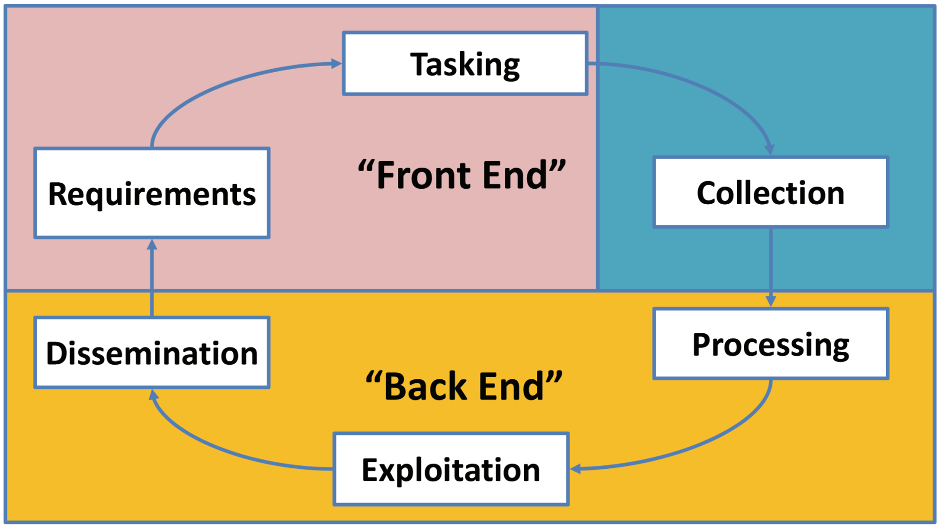


Figure 3: Collector's Process View

It's easy to think of it as a straight line process with a beginning and an end, rather than a cycle. That's how it works in practice. How you get from dissemination to requirements is almost an unknown for collectors. That's because they typically have no control over that step. Someone else has to do it. Usually, that's the job of an analyst.

There's another way to think about both collection structure and process, as shown in Figure 4, that is more useful for analysts. This view treats collection as many separate stovepipes, each having a specialized variant of the process shown in Figure 3, and each producing a different type of intelligence product – therefore, having a different function. It also has two distinctly different products:

Much of collection is high volume, with automated processing and of a mass of material which then is disseminated widely. In the field, you get a lot of open source, IMINT and SIGINT without having to ask for it.

The other kind is often called targeted collection; I often describe it as "boutique" collection. Think of the contrast between a mass-market store such as Wal-Mart and a boutique such as Tiffany's that caters to a select customer set. Targeted collection is usually expensive, produced in small quantity for a few customers. It requires extensive processing and exploitation.

The collection INTs shown in blue are targeted. Those shown in gold-orange are usually mass collection, but sometimes are targeted. ELINT is an example: it can be either (operational ELINT is mass collection; technical ELINT is targeted). Cyber collection often is targeted, but much of it is mass collection.

Why is this important for analysts? Because they handle collection requests quite differently, depending on which type they are dealing with. Mass collection typically has a formal requirements structure. Imagery collection, for example, may have massive target decks.[2] Getting your target into those decks means navigating a formal requirements structure. In contrast, targeted collection tends to be focused on a single event, facility, or individual. Think here of the hunt for Osama bin Laden or of collection against a North Korean ballistic missile test. Analysts tend to become much more directly involved in targeted collection than in mass collection.

It's also valuable for both analysts and collectors to view collection structurally as Figure 4 (see next page) shows it, because the cultures are different within each box shown in the figure. ELINT, FISINT, and COMINT are lumped within the category "SIGINT" in Figure 1. But these three INTs have distinctly different cultures, different technical

[2] A target deck is a list of existing intelligence targeting requests and the target related data.

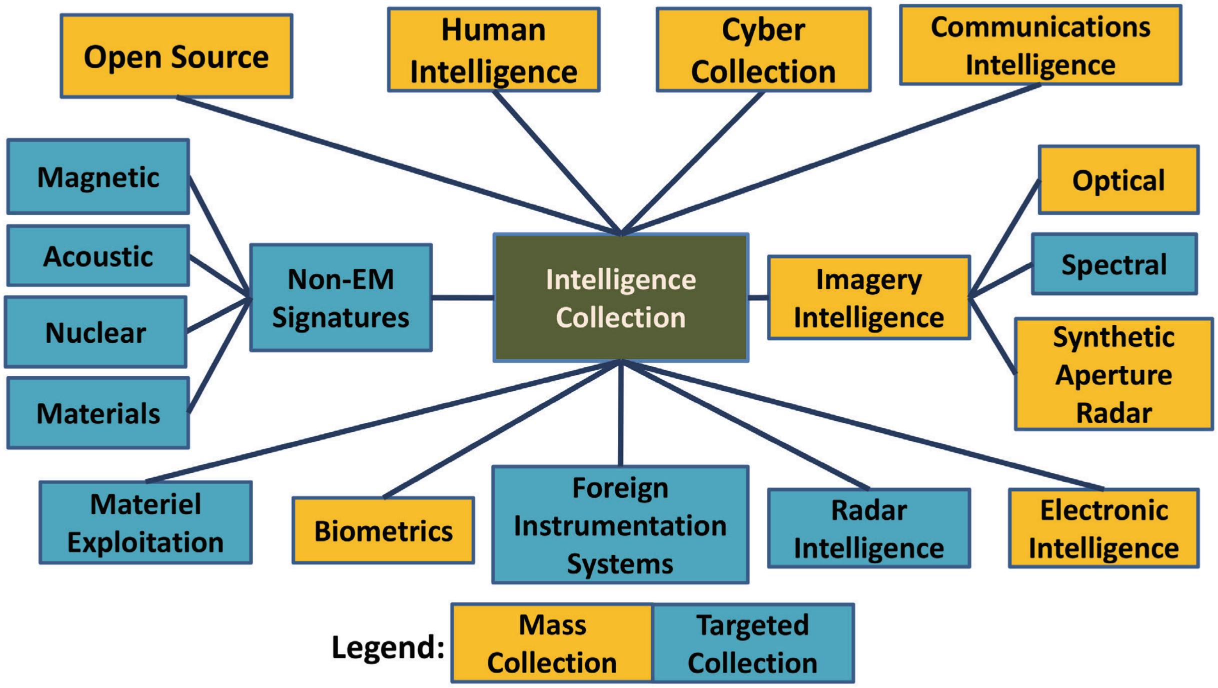


Figure 4: Analyst's Process View

disciplines, and different security compartmentation practices. The same is true for the three subcategories of IMINT shown in Figure 4. When working with collectors in all of these disciplines, it's essential to realize that fact and to understand that they cannot be treated simply as "SIGINT collectors" or "imagery analysts."

BOUNDARY ISSUES AND THE "NAME GAME"

> *General Michael Hayden, former Director of the National Security Agency and Central Intelligence Agency, has said that when he was an ROTC instructor he would quote this line from Confucius to his new students: "The rectification of names is the most important business of government. If names are not correct, language will not be in accordance with the truth of things."*[3]

We often deal with boundaries (areas of responsibility) in the intelligence community by choosing names for collection or analysis that emphasize the importance of our mission. After all, we prefer to work for an elite and respected organization and we want to believe that what we're doing is of value for national security. Also, we like to go into budget negotiations with a strong negotiating position. So, violating Confucius' edict, we choose names and their definitions that suit our bureaucratic purposes. For example, most of the intelligence community refers to the pilotless aircraft used in reconnaissance as an unmanned aerial vehicle (UAV). In U.S. Air Force circles, it's an article of faith to call it a remotely piloted vehicle (RPV), emphasizing the need for a pilot somewhere in the loop.

In intelligence, the misuse of names often results in confusion for all parties – collectors, analysts, and customers. It also results in the naming of many things as "INTs" that have little to do with collection. Following are some of the resulting boundary issues and competing terms that are associated with them.

All Source versus Single Source versus Multi-INT Analysis

National intelligence collection organizations perform what is called *single source analysis*. NSA, NGA, and OSC, for example, all do single source analysis: their job is to process, exploit, and analyze material collected from COMINT, IMINT, and open source, respectively. They often make use of material from other INTs, and refer to such material as *collateral intelligence*. So if an imagery analyst makes use of COMINT, she would refer to the COMINT as 'collateral.' And a COMINT analyst making use of imagery would call the imagery 'collateral.'

[3] Michael Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly*, Spring, 2011, accessed 28 June 2013 at *http://www.masonbay.com/clients/dev2/chertoff-html/articles-the-future-of-things-cyber.php*.

A number of national agencies and military service units are charged with producing *all source* analysis. For example, CIA, DIA, DHS, and the State Department all have the responsibility to provide all source analysis at the national level.

Supposedly, a boundary exists between these two analysis types. It is a boundary that is often ignored. Single source analysis groups want to produce all-source intelligence, and because intelligence is shared among collection organizations, they usually are able to do so. Michael Herman observed that "The single-source agencies now are not pure collectors of 'raw intelligence'; they are also institutionalized analysts, selectors, and interpreters"; and on the distinction between the two, that it is "intellectually artificial to chop up into parts what is in reality a continuous search for the truth."[4]

There are good reasons to encourage, rather than discourage, the proclivity of single-source analysts to do all-source analysis (which, playing the name game, they prefer to call "multi-INT fusion"). If it can be done effectively, the single-source analyst can pick up some of the workload of producing intelligence, so that the heavily loaded all-source analyst gets some help. And the whole idea of competitive analysis is built around the idea of a fresh and different perspective looking at the raw material. A different set of eyes on the material can often surface something important.

On the other hand, the single-source analyst simply doesn't have the same breadth of access to sources, and usually doesn't have the same depth of experience or expertise in dealing with the topic, nor the close access to the customer that the all-source analyst has. So the single source analyst producing all-source intelligence can provide a poor assessment (which the customer might just use). Another pitfall is that the single-source analyst can fail to do his/her primary job on the single source because of a focus on the all-source problem.

Operational Information versus Intelligence

In the course of combat operations, friendly units are constantly observing the enemy actions visually and also using imagery and electronic means. This could be considered intelligence collection, or simply operational information. Depending on which side you sit organizationally, you're likely to have different names for it. A few examples:

- A Predator video could be considered either intelligence or operational information. If the video is used for on-the-spot targeting, it logically would be operational information. If it is retained and analyzed for future use, it more likely is intelligence. But intelligence officers are prone to call the product "movement intelligence" or MOVEINT, while operational staff simply call it full motion video (FMV), avoiding the word "intelligence."
- ELINT intercepts that are used to geolocate enemy radars are referred to as Operational ELINT (or OPELINT) in intelligence circles. But the US military uses the term Electronic Support Measures (ESM) for OPELINT that is used to support electronic and physical attacks on a target. The term ESM was coined specifically to keep the product out of intelligence budgets and away from intelligence management.
- A battlefield radar detects opposing forces' aircraft and helicopter movements. This usually would be considered operational information. But the product might have intelligence value, and would then be referred to as "radar intelligence" or RADINT.

As the examples suggest, there may be boundaries, but they are fuzzy ones. The difference becomes important primarily when the US goes through its annual funding exercise. A collection system that provides operational information goes into the Defense budget and requires different approvals than one that is deemed for intelligence use in the National Intelligence Program budget.

NAMING NEW COLLECTION METHODS

When a new collection method becomes important for customers, and it doesn't fit cleanly into the existing structure, we often see a battle of names for it. Following are a few that have developed over the last ten years, including some that are still being argued.

GEOINT, AGI, and imagery-derived MASINT

Figure 1 shows NGA as the functional manager

[4] Michael Herman, *Intelligence Services in the Information Age*, Routledge, London: 2001, p. 192-93.

for IMINT. Most taxonomies replace IMINT with the term geospatial intelligence, or GEOINT. According to NGA doctrine, GEOINT is the product of integrating imagery, imagery intelligence, and geospatial information. But since geospatial information also is collected via open source, SIGINT, HUMINT, and MASINT, the GEOINT product would seem to result from either all-source analysis or multi-INT fusion, depending on your preferred terminology. GEOINT arguably is not a collection INT – no collection system collects GEOINT.

NGA has defined a special type of GEOINT called Advanced Geospatial Intelligence (AGI). The definition calls AGI "technical, geospatial, and intelligence information derived through interpretation or analysis using advanced processing of all data collected by imagery or imagery-related collection systems." Presumably, this refers to infrared, spectral, and radar imagery. DIA, with functional responsibility for MASINT, prefers to call it "imagery-derived MASINT."

Cyber Collection

Perhaps one of the most important sources of raw intelligence today, cyber collection does not fit cleanly into any of the traditional five INTs. It has some aspects of open source (since it relies heavily on the Web). It arguably is a type of SIGINT, since it can require intercepting internet communications. But how do you characterize placing a Trojan or worm on a victim computer, downloading the hard drive, and activating the victim's video camera? Such a process does not involve intercepting a deliberately transmitted signal. And how to characterize a HUMINT operation that downloads files from a single computer, one that never connects to the internet?

The result of these complexities is another naming contest. Those in the SIGINT business have coined the term "SIGINT at rest" to argue that cyber collection is a SIGINT activity. Those who find that terminology somewhat strained, especially when applied to standalone computers, argue that "HUMINT-enabled" cyber collection is more appropriate.

Identity Intelligence

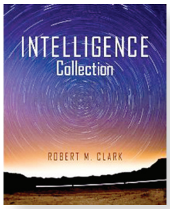
Biometrics has become an important source of intelligence as the focus of much collection, especially in Iraq and Afghanistan, has been on identifying and tracking individuals. The result has been the creation of a new "INT", called *identity intelligence.* While biometrics is about collection, and logically a type of MASINT, the term 'identity intelligence' would seem to describe the product of all-source analysis, much like GEOINT.

CONCLUSION

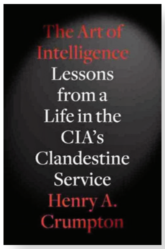
The U.S. Intelligence Community has developed, over time, an incredibly complex system for collecting and processing raw intelligence. It is effective, far from perfect, but the best in the world in providing intelligence to support a broad range of customers. It succeeds despite the challenges of collaborating across the stovepipes and the tensions created by budget competition. Collectors and analysts are best served when each understands the other's perspectives of function and process. Sound assessments depend on this understanding.

READINGS FOR INSTRUCTORS

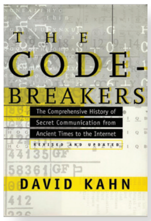
Robert M. Clark, *Intelligence Collection* (Washington D.C.: Sage/CQ Press, 2014) (available in August 2013). Takes a systems approach to collection, explaining the structure, function, and process of all of the INTs listed in Figure 2.



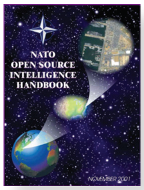
Henry A. Crumpton, *The Art of Intelligence* (New York: Penguin Press, 2012) This is perhaps the best available explanation in print of how a clandestine service actually functions.



David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1996) A classic, this is the standard reference on cryptology and its history.


THE
CODE-
BREAKERS
The Comprehensive History of
Secret Communication from
Ancient Times to the Internet
DAVID KAHN

United States. Commission on the Roles and Capabilities of the United States Intelligence Community. "IC21: The Intelligence Community in the 21st Century. Washington, DC: GPO, 1996." Accessed at *http://www.access.gpo.gov/congress/house/intel/ic21/index.html*. Though 17 years old, this report provides a good summary of the major INTs.



NATO Open Source Intelligence Handbook, 2001, accessed at *http://www.oss.net/dynamaster/file_archive/030201/ca5f* *b66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20 Handbook%20v1.2%20-%20Jan%202002.pdf.* This book, along with, the *NATO Open Source Intelligence Reader* and the *NATO Intelligence Exploitation of the Internet*, provides a comprehensive view of open source collection.

Robert M. Clark currently is an independent consultant for the US Intelligence Community. He is also a faculty member of the Intelligence and Security Academy and a professor of intelligence studies at the University of Maryland University College.

Dr. Clark served in the United States Air Force as an electronics warfare officer and intelligence officer, reaching the rank of lieutenant colonel. At CIA, he was a senior analyst and group chief responsible for managing analytic methodologies. He subsequently was President and CEO of the Scientific and Technical Analysis Corporation, directing intelligence collection and analysis support efforts and the creation of new collection and analysis methodologies.

As a consultant, Dr. Clark helped develop the DNI's Intelligence Community Officers' Course and served as a faculty member from 2001-2008. From 2008-2009 he was the course director of the DNI's Introduction to the Intelligence Community course.

Clark holds an SB from MIT, a PhD in electrical engineering from the University of Illinois, and a JD from George Washington University. He is a presidential interchange executive, a member of the Virginia state bar, and a patent attorney.

Dr. Clark's *Intelligence Analysis: A Target-centric Approach* is now in its fourth edition. His second book, *The Technical Collection of Intelligence*, was published in 2010. His third book, *Intelligence Collection*, is due to be published in 2013.

ECOCIDE

Easter Island is the "clearest example of a society that destroyed itself by overexploiting its own resources." Once tree clearing started, it didn't stop until the whole forest was gone. Diamond called this self-destructive behavior "ecocide" and warned that Easter Island's fate could one day be our own.

And that has become the lesson of Easter Island — that we don't dare abuse the plants and animals around us, because if we do, we will, all of us, go down together.

— Jared Diamond, author *Collapse*