



Open Source Intelligence (OSINT) Analyst

Overtly Passive / Covertly Active

Surveillance / Reconnaissance

Observation / Exploration

Eye / Spy

PREFACE



This desk/pocket smartbook contains information to assist you, the open source intelligence analyst, in carrying out your research responsibilities in a manner that first of all adhere to intelligence oversight and follow the guidelines of AR 381-10, Executive Order 12333, and unit standard operating procedures (SOP). The second is to practice and implement effective operational security (OPSEC) measures during data and information collection activities online. A fine line exists between collection and acquisition, and examples will be pointed out throughout the handbook. This handout is not written specifically for the military active or passive OSINT Analyst but rather as an all-purpose guide for anyone doing research. The one big advantage for the passive OSINT Analyst is that it does not require interaction with the mark. Therefore, it poses little risk since it does not alert the target to the presence of the analyst. If a technique violates Intelligence Oversight and OPSEC, then common sense must take center stage. For those in the civilian community (law enforcement, journalists, researchers, etc.), you are bound by a different set of rules and have more latitude.

One important thing to keep in mind is that when threats are mentioned the majority tend to think they are military in nature. We think of Iran, North Korea, and other countries with a military capability. That is not the case. Threats can be the lone wolf types, a disgruntled worker, someone calling in a bomb threat to a hospital, etc. But guess what? It is all about the research and how one goes about obtaining the information. But don't get too wrapped up around the internet; it's also about talking to people. People talk to other people, individuals have thoughts and ideas that have not made their way into the digital world and it requires interaction with those folks.

This handout is written in an easy to read format that can be understood by anyone. It can be used as a teaching guide, or to supplement and/or complement current OSINT instruction. It does not address classified network techniques however all techniques mentioned here will have some functionality in those worlds.

Being an OSINT analyst is no different than being a journalist. The only difference is that the analyst is guided by strict legal guidelines whereas the journalist is free to roam the prairie. The research techniques are the same, whether online (or offline), interviewing, attending trade shows, listening to the *radio or watching television. So does that make the journalist an analyst? Absolutely! He/she have to validate and vet their sources just like the OSINT analyst. So you have an advantage over the journalist. You can passively use their material but they cannot use yours. However, a strong word of caution! While the primary mission of journalists is to inform they still carry some influence. (see [News Media Analysis](#))

*According to the UN, an estimated 44,000 radio stations broadcast to at least five billion people, representing 70 percent of the population worldwide.

<http://www.aljazeera.com/news/2016/02/radio-world-media-primary-source-information-2016-160213130238088.html>

The phrase “Do Not Send a Spy Where a Schoolboy Can Go” which was coined by Robert Steele, aptly applies to the above. Let others do the hard work for you in the open source world. You are that schoolboy/girl. Which leads to another often mentioned line “open sources may account for as much as 80 percent of the intelligence database”. Some even claim the percentage to be much higher.

Several years ago, Major General Marks, former U.S. Army Intelligence Center Commander, said that every soldier is a sensor, basically a collector of information. How right he is. Well, guess what? You don’t have to be a soldier to collect information. As a member of the various open source intelligence teams (DEA, DHS, Fusion Centers, FBI, etc.) you are constantly in the midst of information, so in essence, just like a soldier, you are also a sensor. Sometimes we depend too much on sensitive non releasable information, and when we do get it we then have problems with distribution and sharing. Open source is your answer. You can share it and disseminate in practically any form without revealing sensitive sources. At times open sources will be the only source of information. If information has to be obtained surreptitiously, open sources are sure to drive the collection effort and point the collector in the right direction. Open source will never replace sensitive operations but it can be used to supplement/complement, and even confirm or deny current holdings. Open source drives the sensitive collection effort and works nicely in the unclassified environment.

We must also change our way of OSINT thinking and how it interacts with the classical “INTs”. For too long the thought was that OSINT drove the collection effort and filled in the gaps in the classified holdings, which in fact it remains true to this day. However, the classified holdings can also fill in the gaps of open source intelligence and also drive the OSINT collection effort. On the other hand, is a catch-22 created? Does my unclassified information now become classified because the OSINT collection effort is driven by a classified requirement or a classified sentence filled in a gap in the OSINT report? I can see where it would have little or no effect in the active environment but what about the passive phase? And remember, open source is complimentary, not competitive with the other intelligence disciplines.

This mini handbook only nicks the surface and is not the answer for the OSINT Analyst, whether military or civilian, but is rather a guide to get you going quickly. In many illustrations, like in searching techniques, you have to use your imagination for the right syntax or Boolean logic to get to your destination quickly.

To do your job effectively beware and be aware. Become familiar with Executive Order 12333, AR 381-10, DOD Regulation 5240.1-R, Intelligence Oversight and OPSEC.

Three Days of the Condor
I work for the CIA. I am not a spy. I just read books.

In the 1975 film Three Days of the Condor, Robert Redford plays the role of CIA open source analyst Joe Turner (code name “Condor”), who inadvertently uncovers, through

publicly available sources, a rogue operation designed to ensure U.S. control of Middle Eastern oil fields. Turner's job is to analyze foreign books, newspapers, and journals to develop insights for his CIA bosses. A few days after filing a particularly intriguing report with CIA headquarters, Turner returns to his New York City office to find that his colleagues have all been murdered. The film centers on Turner's quest to solve the mystery while avoid being killed by CIA operatives who are involved in the plot. During one scene, CIA bureaucrats question Turner's handler during a meeting.

CIA official: "This Condor isn't the man his file says he is." "So where did he learn evasive moves"?

Handler: "He reads."

CIA official: "What the hell does that mean?"

Handler: "It means, Sir, that he reads everything."

Turner is an unlikely hero who uses open sources and his superior reasoning and creativity to uncover, and later foil, a CIA conspiracy. Decades later, far from Hollywood, a handful of officials, policy makers, and corporate executives have endeavored to craft a rather different depiction of the ideal open source practitioner. This practitioner is an intelligence agency analyst, contractor, or even an ordinary citizen who uses open sources and overcomes bureaucratic obstacles to help thwart defined external threats to U.S. national security.

No More Secrets by Hamilton Bean

The very first open source intelligence section can probably be traced back to 1867, when Chief of the General Staff Helmuth von Moltke established a specialized agency, a geographic and statistical branch, to collect what would today be called "open-source intelligence" about other countries. It had a good run for 24 years until it was abolished in 1894 and its functions distributed elsewhere.

Source: Foreign Affairs, The Rise of Intelligence, by David Kahn, September/October 2006 Issue

Table of Contents



OPSEC	
OSINT Definition	
Gray/Grey Literature	
Ephemeral Literature	
OSINT Tradecraft	
The Other INTs	
OSINT Intelligence Cycle	
OSINT Support to the "INTs"	
Who Has the Best Links?	
Web Layers	
Searching Strategies	
Deep Web Research	
Source Reliability/Information Credibility	
	Online Translation Services
	Managing Information Overload
	Open Source Imagery
	OSINT Analyst Tools
	Virtual Private Network
	People Finder
	Inadvertent Achievement
	Private Search Engines
	OSINT Situational Awareness
	News Media Analysis
	OSINT Support to Counter Human Trafficking
	Declassified Sample of Actual OSINT Collection

OPSEC

One area that needs to be touched on up front is that about Operations Security (OPSEC). OPSEC is an analytic process used to deny the adversary information, generally unclassified, concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations. OPSEC does not replace other security disciplines, it supplements them.

As you do research you will leave electronic footprints for a webmaster to be able to track back to you. For example, you may get a requirement to do research on arms transfers from Colombia to Mexico via Central America. While this may seem innocent enough it can alert the criminal element that a certain department is interested in the subject. Make no mistake about it these individuals are not stupid. They know how to use the internet and have their own IT folks, or else they have bribed someone in a large organization to be watchful for certain keywords. Based on the traffic related to arms transfers the enemy can come up with their own requests for information. Examples include, but are not limited to where is the traffic originating; are there multiple locations requesting the same information; what are the geographic locations; why the sudden interest?

OPSEC is a process, but it is also a mindset. By educating oneself on OPSEC risks and methodologies, protecting sensitive information becomes second nature.

This example should give you an idea of simple indicators that when put together complete the missing pieces of the puzzle. We all like to brag, it is our nature. Consider the following:

At sports bar: I don't look forward to Friday, anyway, gotta go, have to be up and going by 4 a.m. See you Tuesday. How many other customers heard this?

Online: Can't say much or when but we're conducting a gang sweep. How many people was he/she communicating with?

Wife to neighbor: John is getting his riot gear together. You can bet the neighbor will tell her husband who may tell someone else.

Online: We are cleaning up that rat's nest on the south side. Same as above.

At sports bar: Come Friday all you'll hear is the clanging of cell doors. Same as above.

Customer at movie rental to sales clerk: Friday the 13th will be creepy for MS-13. Again, how many people overheard the comment?

You have probably been practicing OPSEC in your personal life without knowing it! When you are getting ready to go on a trip have you ever stopped the delivery of the newspaper so that they would not pile up outside; asked your neighbor to pick up your mail so the mailbox would not fill up; connected your porch lights and inside lights to a timer so they would go on at preset times; connected a radio to a timer so that it comes on at different times? Congratulations, you were practicing OPSEC.

OSINT Definition

Open Source Intelligence (OSINT): Open source intelligence refers to intelligence based on information gathered from open sources, i.e. information available to the general public. This includes newspapers, the internet, books, phone books, scientific journals, radio broadcasts, television, and others. Collection of information in OSINT format is a very different process in comparison to collection conducted by the other intelligence disciplines because, by definition, the information sources are publicly available versus covertly collected. (Note: There are many variations to the definition but overall the meaning is basically the same in that it is publicly available for anyone to use.)

An open source is any person or group that provides information without the expectation of privacy. The information, the relationship, or both is not protected against public disclosure.

Passive versus active collection: In the passive mode you simply observe while active demands interaction like asking questions, creating an account, joining a group, etc.

Consider the following: *“The Collection of foreign intelligence is accomplished in a variety of ways, not all of them either mysterious or secret. This is particularly true of overt intelligence, which is information derived from newspapers, books, learned and technical publications, official reports of government proceedings, radio and television. Even a novel or a play may contain useful information about the state of a nation.”*

Mr. Allan Dulles, first civilian director of the CIA

OSINT is more than information, it represents a careful sifting, selecting, analyzing and presenting of open source material on a timely basis, and the keyword is timely. OSINT is a valuable contributor to "all source" intelligence, supports the classical "INTs", helps drive the collection effort, and tells the "INTs" where to look, but most important where not to look and as a consequence saving precious resources and time. Intelligence is the product that results from collection, the processing of collected raw data, and analysis and interpretation of collected information. Collection is both the acquisition of information and the processing of that information into products tailored for use by various customers. Collection is conducted in response to customer requirements, with specific collection tasking given to collectors to gather the required information. The intelligence process involves developing raw information into finished intelligence for customers to use in decision-making and action. This is called the intelligence cycle which has five phases, each of which drives the next phase in the process.

Gray/Grey Literature

Gray Literature (a.k.a. Grey Literature) is open source material that usually is available through specialized access and may not enter normal channels or systems of publication, distribution, bibliographic control, or acquisition. Generally, the producers of gray literature make little effort to disseminate or popularize it beyond its intended audience. Gray Literature can include, but is not limited to, research reports, technical reports, economic reports, trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, dissertations and theses, trade literature, market surveys, and newsletters. This material cuts across scientific, political, socio-economic, and military disciplines.

Ephemeral Literature

Ephemeral is written or printed matter not meant to be retained or preserved. It is temporary. Ephemeral literature poses similar practical difficulties as Gray Literature and sometimes can be confused with it. The chief distinction is that Gray literature tends to include technical information whereas ephemeral can include virtually any topic. It includes working documents, such as drafts or preliminary versions, committee agendas, copies of invoices, and routine emails to schedule or confirm events. Other examples include advertisements, business cards, pamphlets, unpublished photographs, postcards, notices, fliers, posters, tickets, or self-published works. (Gray and Ephemeral literature are easy to dismiss because they are hard to get and use, but that would mean ignoring a tremendous amount of information. It's information that's more up-to-date and may be more concise and focused than public works.)

OSINT Tradecraft

An art and a science of creating lawful intelligence from publicly available data and information while shielding sources and methods, and without revealing intentions. (Note: The meaning of "lawful" indicates observing strict legal guidelines under Intelligence Oversight.)

The Other INTs

HUMINT – Human Intelligence. Intelligence derived from information collected and provided by human sources. Not much different from OSINT since a human can be considered as a source of open source information. However, the main difference is that a person trained in HUMINT goes about obtaining information in a more refined procedure. HUMINTers are highly trained individuals and best left for them to do the work. They know how to ask questions or leading questions. In a covert situation the source would only give information to the person conducting HUMINT operations and only after a trusting relationship had been established. The person providing information is always in constant danger especially if the information were to involve countries that are hostile to the United States.

IMINT – Imagery Intelligence. Intelligence derived from satellite and/or aerial photography. Google Earth, GeoEye, DigitalGlobe, and other commercial companies make imagery available for the typical citizen. In the classified world a satellite may be deployed over Iran or North Korea to photograph nuclear facilities but we don't want them to know when we are conducting the missions.

GEOINT – Geospatial intelligence. A combination of disciplines. Intelligence about the human activity on earth derived from the exploitation and analysis of imagery and geospatial information that describes, assesses, and visually depicts physical features and geographically referenced activities on the earth. It consists of imagery, imagery intelligence (IMINT) and geospatial information.

SIGINT – Signals Intelligence. Intelligence derived from interception of signals between people and/or machines. Although this encompasses a huge variety of emanations, it is principally concerned with COMINT: intercepted communications. When people talk on the phone or other means that give off a signal SIGINT is there to catch it. Two fax machines sending and receiving are also intercepted. Subsets include COMINT & ELINT.

MASINT – Measurements and Signatures Intelligence. Electronic version of all-source intelligence. Scientific and technical intelligence derived from specific technical sensors.

OSINT: Information they told everybody.

HUMINT: Information they only told us.

SIGINT: Something we heard when they didn't know we were listening.

GEOINT/MASINT: Something we saw in a specific area when they didn't know we were watching, smelling, touching or tasting.

IMINT: Something we saw when they did or didn't know we were watching.

Special Access Program (SAP): Information they REALLY don't know we know. That is until Edward Snowden and Hillary Clinton told them.

Foreign Material Exploitation (FME): Physical material we got our hands on.

“Big Brother is Watching You.”
– George Orwell, 1984

OSINT Intelligence Cycle

This cycle is provided simply to keep the OSINT Analyst focused and in no way replaces the traditional Intelligence cycle. The collection phase is probably the most brutal since the analyst is going to be dealing with massive amounts of information and may not have the luxury of time to study every piece of data and information.

Processing, exploitation and dissemination will suffer if the analyst does not keep a clear focus on the collection phase. Analytical tools like Analyst Notebook and Palantir will make it easier to keep track of the data/information but cannot predict like the analyst can; it still requires human interaction.



THE INTELLIGENCE CYCLE

Equally important to the components of strategic intelligence is an awareness of the strategic intelligence cycle and the debriefer's role within that cycle. The first step is the identification of intelligence gaps. Analysts translate these gaps into intelligence requirements - the second step. In the third step, the strategic debriefer fulfills those requirements. The fourth step involves preparation of an intelligence report. The fifth and last step is the preparation of an intelligence report evaluation by the originator of the requirement. These evaluations measure the quality of the information as well as the quality of the report writing.

The Intelligence Cycle is the process of developing raw information into finished intelligence for policymakers to use in decisionmaking and action. There are five steps which constitute the Intelligence Cycle.

1. Planning and Direction

... is management of the entire effort, from identifying the need for data to delivering an intelligence product to a consumer. It is the beginning and the end of the cycle—the beginning because it involves drawing up specific collection requirements and the end because finished intelligence, which supports policy decisions, generates new requirements. The whole process depends on guidance from public officials. Policymakers—the President, his aides, the National Security Council, and other major departments and agencies of government—initiate requests for intelligence.

2. Collection

... is the gathering of the raw information needed to produce finished intelligence. There are many sources of information, including open sources such as foreign broadcasts, newspapers, periodicals, and books. Open source reporting is integral to CIA's analytical capabilities. There are also secret sources of information. CIA operations officers collect such information from agents abroad and from defectors who provide information obtainable in no other way. Finally, technical collection—electronics and satellite photography—plays an indispensable role in modern intelligence, such as monitoring arms control agreements and providing direct support to military forces.

3. Processing

... involves converting the vast amount of information collected to a form usable by analysts. This is done through a variety of methods including decryption, language translations, and data reduction.

4. All-Source Analysis and Production

... is the conversion of basic information into finished intelligence. It includes integrating, evaluating, and analyzing all available data—which is often fragmented and even contradictory—and preparing intelligence products. Analysts, who are subject-matter specialists, consider the information's reliability, validity, and relevance. They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for the United States.

The CIA devotes the bulk of its resources to providing strategic intelligence to policymakers. It performs this important function by monitoring events, warning decisionmakers about threats to the United States, and forecasting developments. The subjects involved may concern different regions, problems, or personalities in various contexts—political, geographic, economic, military, scientific, or biographic. Current events, capabilities, and future trends are examined.

The CIA produces numerous written reports, which may be brief—one page or less—or lengthy studies. They may involve current intelligence, which is of immediate importance, or long-range assessments. The Agency presents some finished intelligence in oral briefings. The CIA also participates in the drafting and production of National Intelligence Estimates, which reflect the collective judgments of the Intelligence Community.

5. Dissemination

The last step, which logically feeds into the first, is the distribution of the finished intelligence to the consumers, the same policymakers whose needs initiated the intelligence requirements. Finished intelligence is provided daily to the President and key national security advisers. The policymakers, the recipients of finished intelligence, then make decisions based on the information, and these decisions may lead to the levying of more requirements, thus triggering the Intelligence Cycle.

Note: If you do a search on the intelligence cycle you will see that the Army, FBI, CIA, USMC, etc., and even other countries like the UK have slightly different versions. However, they are all basically the same with the intent of producing intelligence.



OSINT Support to the “INTs”

OSINT Support to HUMINT



How can OSINT possibly support HUMINT when both disciplines are almost the same? Well, let's not start a turf war with the HUMINTers. In each one the target is a human with information that both disciplines want to have. The only part that may be considered the same in both disciplines is the overt collection phase but that is where it ends. I guess the best way to put it is in this manner, if you are an OSINT Analyst (collector type) and you acquire information that is voluntarily made you need to stay within the passive collection lane. HUMINT folks, on the other hand, have specialized training and are in the business of trying to unearth new information that is not accessible by the public. A good rule of thumb when conducting OSINT research is to remain passive. Essentially this means you may passively follow an individual or organization's blog, microblogs, or social networking site without contacting any individual for any reason. Do not make contact even to answer a seemingly innocent request for information (RFI) or to merely provide helpful information. If you do, you are crossing over into the HUMINT dominion.

But consider that OSINT can often collect information that may be difficult or sometimes impossible to collect by HUMINT because of distance and time or some other unknown restriction. OSINT can deliver information which includes enemy plans and intentions, leadership, weapons systems, infrastructure or other areas that may be helpful to HUMINT in their collection effort.

Example of OSINT contributions to HUMINT: This is a made up scenario. Border patrol agents believe an individual they are holding possibly belongs to a gang. He was stopped at the San Luis Port of Entry because the officer inspecting the documents believes they are forgeries. The individual says his name is Pedro Borrego and claims to be 22 years old but appears to be more like 18 or 19. Initial questioning reveals that he was born in Tijuana and helped his father repair boots in a boot factory near Mercado de Artesanias. He has a single tattoo of a scorpion on his right arm which appears to be fresh because of red swelling. He had in his possession one suitcase with 3 changes of clothing. His business in the U.S. is strictly pleasure before returning home. Additional inspection of the documents reveal they are not forgeries, however, the tattoo and age suspicion do open up some concerns. OSINT can provide support in the following ways:

Tijuana newspapers with gang news.

Video and audio media of gang activities.

Phone/business directories that identify Mercado de Artesanias.

What other stores are located near Mercado de Artesanias?

What tattoo parlors are in the area and what is the favorite graphic?

What gangs have the scorpion tattoo as their logo?

What drug cartels use the scorpion logo? Drug distributors identify their products with symbols.

OSINT Support to SIGINT

Actual Example: Many years ago while stationed in East Germany (when we had an East Germany) our unit received a message from another unit in West Germany about an unidentified signal coming out of East Germany and could we investigate. Our unit did mostly open source collection and OSINT hadn't been coined yet as we know it today. We had a choice of launching an aerial recon mission or a ground recon but we decided going by air since it would be faster and it also happened to be within our area of flight operations. A ground recon would have been useless since the signal was coming out of a training area in a restricted zone. We were able to make it to the coordinates given to us and identify the equipment associated with the unidentified signal. This in turn provided a good update to the electronic order of battle.

Other ways our missions supported SIGINT was in foreign magazine translations. Some of our collectors were tasked with acquiring magazines, especially military, from different countries that were sold in East Germany. The focus, besides translations, was really on new, or old, military equipment. We studied the photos for recent modifications on known equipment and what they could possibly mean to the SIGINT field as far as new signals relating to the equipment. Occasionally magazines were the first source of new equipment being fielded.

Besides these examples there are countless means where OSINT supports SIGINT in ways we hardly ever think about.

OSINT Support to GEOINT/IMINT

Just as in the above example where OSINT provided support to SIGINT, the same was true when it came to IMINT in some of our operations. (GEOINT had not been coined at that time.) There were many areas where we could not go into because of restrictions so we had to rely on our maps to determine where a particular piece of equipment had gone into a restricted area and disappeared. You can guess what happened after that and who was notified to sweep the area, especially if it was a piece of equipment that had not been identified before.

The same holds true for reporters deployed around the world. They can help guide the collection effort without even realizing it. The major news organizations have personnel deployed throughout the globe and most of the time are first to report on significant events. The intelligence agencies do not necessarily go straight to a source and ask them to cover a certain area or event (???) but you can bet they are cemented to the tube, social media, 3 letter news sources, and others. The .mil intelligence agencies are no different; OSINT Analysts scour imagery for anything out of the ordinary like new construction, new equipment and in particular the terrain they operate in. With that information the analyst can help guide the IMINT collection effort. This is a good example of passive collection/acquisition. Let the information come to you then let the

appropriate discipline handle the rest. However, this does not mean the end of the OSINT collection phase, it is a continuous process.

OSINT Support to MASINT

This category is not as difficult as it may seem because it's all about touch, taste, and smell. It is technically derived intelligence data other than IMINT and SIGINT. MASINT encompasses all of the traditional INTs but does not fit neatly into any one specific INT. It includes areas like nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. So how can persistent OSINT help drive the MASINT collection effort?

Simple example: Farmers in a small village in Country X report that the water in a nearby stream they use for irrigation and personal use, at times turns a different color and other times it is foul smelling. Could there be a drug lab operating up stream? If it is a cocaine processing laboratory, then chemicals have to be used in the manufacture of cocaine or other drugs. The labs also need to be located near a water source both for the benefit of the workers and to discharge the used chemicals. Let's suppose that SIGINT cannot get much because of encrypted communications and/or strict radio silence. Let's also presume that IMINT may not be able to see through the heavy vegetation that is masking the operation. I know, I know, lots of presumptions and assumptions. This would then more than likely fall to MASINT and its sophisticated sensors to determine what is actually taking place especially if a most wanted drug lord is being hunted. Again, this would very much be a passive phase for the OSINT Analyst although the active collector could follow up with specific questions about the type of problems farmers are encountering. HUMINT could also play a very active role in this scenario.

Who Has the Best Links?

That would depend on who you ask. Some would claim Denny's; others would say Ihops; still others would say the Good Egg; and the independent one would claim their links are the best. It's all a matter of taste (pun intended). But I have purposely deviated to make a point. The links I am referring to are internet links and it seems like every day someone has created a list of supposedly great OSINT links. I no longer scour the internet looking for that one particular site to keep my handout updated; instead I take advantage of what others have put together. Hey, let someone else do the work, after all, that's what open source is all about, exploitation. Because if you stop and take the time to compare all those great links, you are going to discover that for the most part they all replicate each other to some extent. I go through their links and cull the dead ones from the functional ones, those that are no longer associated with the original page and the ones that lead to questionable sites (37% of the web is porn). What's left, I then distribute throughout my handout ([OSINT 2oolKit On The Go](#)) under the appropriate title. Then I wait for the next batch of great links. This is what I call real passive acquisition.

Web Layers

Everyone has heard of the web and the different layers that make it up. There is the surface web, that portion of web content that can be indexed by search tools, and is therefore easy to access. The surface web is where we find ourselves on any given day when doing just plain surfing or simple searching, and search engines like Google, Bing and Yahoo are the most commonly used. What you do on the surface web is basically clicking on links that take you to different areas without any problems. You are doing what the search engines' web crawlers have accomplished; looking for active links. For many casual users it is the only content they ever see but it is only a very small portion of total web content - 1% to 5% by some estimates.



Now let's dig a little deeper and go to the deep web. This layer contains content that search engines cannot find or index. For example, let's say you click on a link on the surface web and it takes you to a university homepage. Most times, anything beyond this homepage requires a password, special permissions, or paid subscription to access the entire site, especially if you are doing research; this is known as the deep web. This portion of web content cannot be indexed by search tools (web crawlers) and is therefore difficult to access. These sites have their own search engines or search boxes to go deeper into the content. Other reasons why content may not be searchable comprise: do not enter codes; dynamically generated content; Non-html formats; short-lived information; database content; or subscription-only access. Some site examples include Intelink, AKO, Open Source Center or places like Foreign Affairs and Foreign Policy sites (nowwww you get it). All these sites have their own search engines to find whatever.

And finally, there is the dark web. For this layer I will shy away from the terms invisible web and darknet. The dark web is a small area of the deep web that has been purposely concealed and cannot be accessed through your customary web browsers. For this you need the [TOR browser](#). The dark web is where anything may lurk. Want to buy a gun? Go to the dark web. Want to buy drugs? Go to the dark web? Illegal anything? The dark web. And unfortunately this is also the place where the illegal sale and distribution of human beings is taking place. Here's what Tor's data looks like as it flows around the world. <http://www.wired.com/2016/01/heres-what-tors-data-looks-like-as-it-flows-around-the-world/>

Searching Strategies

In my personal opinion, I think the search strategy is really about thinking and time management. We devote too much time doing research by not establishing a time frame and then when we are faced with a drop dead phase we end up doing more cutting and pasting and less on adding value (analysis) to the information because of time compression. This section is to show you good research techniques to cut down on

the time you spend online and spend more time with the brain offline. This should lead to more real-time intelligence and/or actionable intelligence. A good practice is to use multiple search engines. Sit back and enjoy the ride.

Why the research strategy? Because frequently when the analyst is faced with a deadline the analyst will get into the ready, fire, aim approach and the results are devastating information overload which equals quantity rather than quality, an endless number of resources, poor results, missed deadlines and a ruined use of time. The opposite is the ready, aim, fire approach and the analyst ends up with quality results, good time management, a better focus, targets the best sources of information which equals smaller resources. Taken altogether it keeps the analyst from straying, meets deadlines, is timely for the client (your commander) and very likely will produce timely and actionable intelligence.

Define the objective. What is it exactly the analyst is looking for? If researching Russian military order of battle, you need to specify whether it is artillery, armor, infantry, airborne, or some other field. What about the geographic deployment or the leadership of the unit? As you can see the objective is very important else you end up with results you were not exactly looking for. The same thing with a subject like gangs. Searching simply for gangs will very quickly overwhelm the analyst. Be specific; is it local gangs or international? Any gang in particular? Just like in Russian order of battle, are you researching leadership and/or geographical dispositions? What about gang graffiti and slang? So as you can see, defining the objective is more than just searching but it will narrow the concentration. Although the main topic is gangs, each sub area requires a different type of search.

Identify key words. This is a key step; do not ignore it. To do so is to waste precious time looking for anything rather than for something. Key words have a direct impact on search hits and will get you closer to your objective. Be sure to include logical and likely variations. These are some examples of word variations and slang.

A-bomb	marijuana and heroin smoked in cigarette.
a la canona	abrupt ("cold turkey") withdrawal from heroin.
Baby	minor heroin habit.
Belly habit	heroin addiction resulting in stomach symptoms.
Chasing the dragon	inhaling vapors of heroin or cocaine heated on tin foil
	House, haus, casa, maison



Everyone is familiar with the Navajo Code Talkers and how the Japanese were never able to break the code. Following are a few examples of words the Navajo communicated and their meanings. These should give you an idea of what keywords are and their meaning.

Names of Airplanes

Planes

Air Force

Dive Bomber	Chicken Hawk	Ships	Sea Force
Torpedo Plane	Swallow	Battleship	Whale
Observer	Owl	Aircraft	Bird Carrier
Fighter Plane	Humming Bird	Submarine	Iron Fish
Bomber Plane	Buzzard	Mine Sweeper	Beaver
Patrol Plane	Crow	Destroyer	Shark
Transport	Eagle	Transport	Man Carrier
Names of Ships		Cruiser	Small Whale

Select the right source. You have several choices when it comes to search engines. You can go with any of the basic search engines like Google, Bing or Yahoo, or if you prefer you can use meta-search engines that take advantage of the other search engines but you give up some flexibility with the meta-search engines. There are also databases and subject matter experts that may or may not require payment which brings up a very important point. Information should only be paid for once. Before paying for any information make sure that someone else hasn't already paid for it. The analyst does not have unlimited resources and needs to check with other analysts before committing to payment. Don't forget the librarians; they are experts in their field and come in very handy. Universities and government sites have a wide-ranging storehouse of data. Take advantage!

Search. Most people operate in the basic category, no thought required, and simple search terms. Just type terms in search box. Too many returns to digest. Results are suspect. They typically get a lot of hits, too many to peruse and of dubious relevance. Moderately skilled researchers normally use at least some Boolean operators and attempt to string together multiple keywords, or even conduct phrase searching. At least this method is more focused and somewhat productive. Advanced searching is where the analyst wants to begin from. In the advanced method the analyst uses Boolean operators and/or advanced syntax to refine results. Results are fewer, but rich in substantive content.

Let's do a basic search. Type in "drug cartels" into Google or your favorite search engine and see what the results are. Almost 1 million hits, and that's on a government computer that blocks many sites. Now try that on your computer at home. Over 4 million hits! The results should be an indicator of why good searching techniques are essential. You don't have the time to look at 1 to 4 million hits. But to be fair to researchers and analysts, we do sometimes get these silly requests. I have gotten my share of them over the years and it requires a bit of tact to get the consumer to spell out exactly what they are seeking without making them look awkward. The fact of the matter is that sometimes the consumer does not know exactly what they need and it is up to us to get into their head and dig it out and get them to talk about their requirements. A bit of caution – do not accept the "I'll know it when I see it" bullshit! I've had my share of that also. Pin 'em down and ask the right questions. But be tactful. So that's why it matters. What matters? The way you search! Time is important for the researcher and the

analyst and ultimately the consumer who has to make timely critical decisions so we want to be as efficient as possible. Unsound open source harvesting techniques can create large quantities of data that are extremely diverse and irrelevant. Given these large bumps in the information highway, sound research is a must to finding quality, tailored, complete and timely data. With fine-tuned research techniques you retrieve only what you want without all the distractions.

Depicted below are the main Boolean operators used in standard searching. There are more (e.g. you can group words or phrases in parenthesis), but these are the ones used the most. But don't just read about it; if you want to become proficient you must actually do some hands-on exercises. After while it becomes second nature and you will find yourself practicing good search techniques without even thinking about it. Try it, you'll like it. Brief descriptions are provided for each.

<p><i>AND (+) (default)</i>. Finds all specified words AND is the default. The search engine must find all keywords you list before it will return a URL. It will presume the AND connector for any series of words provided.</p>	<p>Peanut AND butter, (peanut butter AND jelly) Seven AND wonders AND world. You need to experiment with this one but it appears that using the word AND without the + symbol hits more accurate returns.</p>
<p><i>OR (must be capitalized)</i>. OR will find at least one, but only one, of the keywords you list before it will return a hit. You can list a series of words with the OR connector.</p>	<p>North OR South Korea Stuxnet virus OR worm</p>
<p><i>NOT (-) (to exclude)</i>. Excludes the specified word. NOT is an exclusion operator. In the example given, virus will return all types, except computer viruses, since you told the search engine not to include that keyword.</p>	<p>Motorcycle NOT -Honda Virus NOT -computer. Best to include NOT and the minus – symbol together as shown above. Results are more accurate. Google does not appear to recognize NOT when used by itself.</p>
<p>Mix It Up (AND, OR, NOT)</p>	<p>Credit card AND visa OR chase NOT -Mastercard</p>
<p><i>“keyword1 keyword2” (phrase)</i>. It tells the search engine to look for an exact match of what keyword string is provided within the quotes. You can insert one or several words – doesn't matter. The search engine will only return exact matches found, so typically this dramatically reduces your hit file, but returns rich content.</p>	<p>“Lord of the Rings” “peanut butter and jelly” "computer virus" -"trojan horse“</p>
<p><i>Truncation (*) e.g. patent*</i>. Includes all forms of a root word. The truncation character (*) is an asterisk. It essentially functions as a wild card and tells the search engine to give you any other variations of text following the root keyword, like in the example shown.</p>	<p>Patent, patents, patented, etc. Senate vote * to * unemployment extension Senate vote * to * fast and furious</p>
<p>Try a Truncation Exercise. Gives you multiple results on stories about different Senate votes with respect to Iraq. * Tells the search</p>	<p>Senate voted * to * Iraq bill Senate voted * funding * Iraq bill Senate voted * against * Iraq bill</p>

engine to treat the star as a placeholder for any unknown term(s), then finds the best matches.	Senate voted * security * Iraq bill gao * weapons * fast and furious
---	---

But first to see what the top level domains stand for.

.com	Originally stood for "commercial" to indicate a site used for commercial purposes, but it has since become the most well-known top-level Internet domain, and is now used for any kind of site.
.int	Used by "International" sites, usually NATO sites.
.edu	Used for educational institutions like universities.
.gov	Used for US Government sites.
.mil	Used for US Military sites.
.net	Originally intended for sites related to the Internet itself, but now used for a wide variety of sites.
.org	Originally intended for non-commercial "organizations", but now used for a wide variety of sites.
Country Code Examples az Azerbaijan cg Congo bo Bolivia co Colombia cx Christmas Island ru Russia	See below for searching examples.

.aero	Aviation
.asia	Asia
.biz	Business Organizations
.cat	Catalan language and culture
.coop	Co-Operative Organizations
.info	Open TLD
.jobs	Jobs
.mobi	Mobile devices
.museum	Museums
.name	Personal
.pro	Credentialed professionals and related entities
.tel	Publishing of contact data
.travel	Travelling

Advanced Search: Tell Google Where to Go.

Site: Narrows search to specific website (domain).

Drug Cartels	1 million hits	
"Drug Cartels"	718 thousand hits	
site:com "Drug Cartels"	1.7 million	
site:org "Drug Cartels"	133k hits	
site:net "Drug Cartels"	72k hits	
site:edu "Drug Cartels"	16k hits	
site:cnn.com "Drug Cartels"	3.4k hits	
site:ru "Drug Cartels"	(country code Russia)	6700 hits
site:hn "Drug Cartels"	(country code Honduras)	56 results

By the time you get this guide the above results may have changed considerably but at least you'll get an idea of how to modify the searches and at the same time you'll get an idea of how chaotic the web is. But don't give up, by the time you get to the end of this section you should be able to string together good searching techniques.

Note: All searches were through a government network which is known to block sites; therefore the results are less than what would be retrieved on an unblocked computer.

Inurl: Searches URLs of web pages.

inurl:history of Drug Cartels 9610 hits

<https://www.timetoast.com/timelines/history-of-the-colombian-drug-cartels> *(note the words without quotation marks appear in the URL of the web page)*

inurl:"history of Drug Cartels" 7 hits

<https://prezi.com/1qxmngxko498/history-of-drug-cartels-in-latin-america/> *(note the number of hits when words are in quotation marks)*

inurl:"history of Drug Cartels" "zetas" "sinaloa" 2 hits

<https://prezi.com/q3errtxnrgwd/history-of-drug-cartels-in-mexico/> (note what happens by adding Zetas and Sinaloa in quotation marks; the hits are less and very specific)

Intitle: Restricts search to web page titles. Useful for specific topics.

intitle:Russian Military 4.4 million returns

<http://www.cfr.org/russian-federation/russian-military/p33758> (note that Russian Military appears in the title of documents and not necessarily in order. Helps when you know certain words appear in a document you may be trying to retrieve)

intitle:"Russian Military" 151K returns

<http://www.dw.com/en/russian-military-helicopters-stationed-near-turkey/a-18902803>
(note the quotation marks cut down on the returns and Russian Military appears exactly in the title)

intitle:farc Bombings 5050 returns
<http://www.aljazeera.com/news/2015/04/colombia-resume-bombing-farc-rebels-attack-150415222246990.html> (note same as above)

intitle:"farc Bombings" 41 hits
<http://www.bbc.com/news/world-latin-america-32330380> (note same as above)

intitle:"mexican mafia" california 6570 hits
<http://www.nbclosangeles.com/news/local/Mexican-Mafia-Member-Orders-Truce-15-Arrested-For-Federal-Racketeering-308273981.html> (note Mexican mafia appears in title and California in text of document)

intitle:"mexican mafia in california" 5 hits
<http://www.knoxvilledailysun.com/news/2011/july/mexican-mafia-busted-in-california.html> (note exact words appear in title)

intitle:"mexican mafia in california" "orange county" 4 hits
<http://www.cnn.com/2011/CRIME/07/13/california.mexican.mafia/> (note orange county appears in text of document)

Intext: Searches for specified text in body.

intext:Guatemala 577 million hits
intext:"methamphetamine" 7.5 million hits
intext:"Sinaloa" 37.2 million hits
intext:"Cartel" 88.3 million hits

(Use your imagination to cut down on the returns. At this point you should have a good working knowledge of how to do that)

Filetype: Specifies extension ppt (powerpoint), doc (document), pdf (document), xls (excel), etc.

Human Trafficking in Mexico filetype:pdf
Intext:"Human Trafficking in Mexico" filetype:txt
"Human Trafficking Crisis" filetype:pdf
Let's mix it up some and see what we have learned so far.

Example: site.gov "human trafficking in mexico" filetype:pdf 5 hits
What we did in this example was to go strictly to a government site, with the exact title in a .pdf file.
Let's try another. site:.org "web hacking" filetype:ppt 21 hits

In this example we went strictly to an organization for specific web hacking in a powerpoint presentation.

Mix it up some more. These are just examples of how a good OSINT Analyst can go after information. In these examples I am going after government and military sites. Notice the symbol (|) separating the .gov and .mil sites. You can change the sites and filetype extensions to anything you want. Text (txt) files and excel (xls) files are excellent sources of information. You will also notice I have several variations of the information I'm looking for. That guarantees more accurate hits and cuts down on information overload.

Remember the instructions above about defining the objective (what is it that the customer wants), identifying key words and building a word repository, selecting the right source, doing the search, and don't forget to document the search history.

```
site:.gov | .mil inurl:/FOUO/ filetype:pdf
site:.mil | .gov "FOUO" filetype:pdf
site:.mil | .gov FOUO filetype:pdf
site:.mil | .gov sigint filetype:pdf
site:.mil | .gov "fouo" sigint filetype:pdf
site:.mil | .gov "fouo" humint filetype:xls
site:.mil | .gov "fouo" imint filetype:xls 2015
site:.gov "fouo" humint 2015 filetype:xls
site:.mil | .gov "fouo" humint filetype:pdf
site:.mil | .gov //counterintelligence filetype:pdf 2015
site:.mil | .gov counterintelligence "fouo" 2014 filetype:pdf
site:.edu "fouo" humint filetype:pdf
site:.mil | .gov "fouo" counterintelligence 2014 filetype:pdf
site:.mil | .gov "secret" counterintelligence 2013 filetype:pdf
site:.mil | .gov counterintelligence "top secret" 2012 filetype:xls
site:.mil | .gov "lasd" "fouo" 2012 filetype:pdf
site:.mil | .gov "mexican mafia" "fouo" "los angeles" 2011 filetype:pdf
site:.mil | .gov "mexican mafia" "fouo" "los angeles" filetype:pdf | filetype:xls
site:.mil | .gov "mexican mafia" "fouo" "law enforcement sensitive" "los angeles"
filetype:pdf | xls
site:.gov "mexican mafia" "fouo" "law enforcement sensitive" "los angeles" filetype:pdf
site:.mil | site:.gov "mexican mafia" "los angeles" filetype:pdf
site:.mil | site:.gov "mexican mafia" "los angeles" 2012 filetype:doc
site:.edu | site:.mil | site:.gov "mexican mafia" "social media" "los angeles" 2012
filetype:pdf
CAUTION to Military Personnel, Government Employees, Government
Contractors! Do not download these files to your computer! I only use this and only
this as an example of what can be found on the internet with a properly put together
syntax. You can experiment with this syntax for even more documents but this is as
far as I go. site:.uk | .us "OSINT" top secret rel filetype:pdf.
```

Generally, information that is still classified is considered classified even if it is leaked or published as "unclassified." The unauthorized publication does not change the fact that the information is classified until officially declassified. Some organizations prohibit their employees from accessing unclassified versions of classified information, or from sharing it since that would be a security violation on the part of the individual. Be especially vigilant with what Wikileaks has released.

Link: Identifies who links to the host page. This comes in very handy when wanting to know what other sites link to your target site. Be sure to use several browsers and clean your cache often when investigating linking sites. Look for blogs that may be linked to the target site; they are a wealth of information.

Example: Link:www.cnn.com/

Info: Shows cache, pages that are similar to, or contain the term. Provides a variety of information about a site. After finding blogs that link to a target site you can then use the info script to gather additional information. Example: Info: <http://wikileaks.org/>

Another search engine I am getting used to and using alongside Google is [Qwant](#) which I consider almost, but not there yet, as good as Google. Once you try it I think you'll agree also.

11 Advanced Searches to Bookmark to Become a Google Power User.

<http://www.makeuseof.com/tag/11-advanced-searches-bookmark-become-google-power-user/>

Deep Web Research

Deep web research does not differ much from regular research other than going below the surface web, and there are special search engines for the deep web. For the surface web you have the general web search engines or web directory. The invisible web is what you cannot find using these types of tools. When searching the deep web think of using the word "database" in your query. Some sites are inaccessible because they are in an un-readable format or are held in databases that require some type of human interaction that search engines cannot do like typing in a password or entering a search query, etc.). In other words, it consists of content that search engines cannot crawl and categorize (index).

The following is a very short list of what may be considered deep web search engines. It is just a small sampling of what you can put together yourself. But if you really want to get a listing of what's out there and start building a repository, go to Google and type in "databases by subject" with or without quotation marks. Careful that you don't drown in the data! Remember what I said above about using the word database. Why are databases so worthy? Well, the information has already been found and skillfully

indexed, saving the researcher precious time. Try the following considerations to give you an idea.

"databases by subject" 2014 filetype:xls. Here I entered a year and a filetype extension. You can also search by site. Example: site:.gov "databases by subject" nuclear filetype:pdf. If you apply what I wrote above on searching techniques, you will have great success.

UC Riverside Library. Although it ceased to exist on December 15, 2014, it still provides great links to sources of information.

<http://library.ucr.edu/>

Wolfram|Alpha introduces a fundamentally new way to get knowledge and answers—not by searching the web, but by doing dynamic computations based on a vast collection of built-in data, algorithms, and methods.

<http://www.wolframalpha.com/>

Infoplease - <http://www.infoplease.com/>

Science.gov searches over 60 databases and over 2200 selected websites from 15 federal agencies, offering 200 million pages of authoritative U.S. government science information including research and development results. <http://www.science.gov/>

The WWW Virtual Library. Run by a loose confederation of volunteers, who compile pages of key links for particular areas in which they are expert. Even though it isn't the biggest index of the Web, the VL pages are widely recognised as being amongst the highest-quality guides to particular sections of the Web. <http://vlib.org/>

ZapMeta is a meta search engine; which means that the user can search listings from multiple search engines all in one place. <http://www.zapmeta.com/>

FindLaw. For legal professionals

<http://lp.findlaw.com/>

USA.Gov. Direct access to a wide variety of information and databases from the United States government, state governments, and local governments. This includes access to the Library of Congress, an A-Z government agency index, the Smithsonian, and much, much more.

<https://www.usa.gov/>

There are literally hundreds of thousands of US government and government-related Web sites online today, and it can be overwhelming (to say the least!) to find what you're looking for. This site goes through the top United States government sites that you need to know about; the sites that consistently offer the best user experience, helping you to find what you need quickly, easily, and efficiently.

<http://websearch.about.com/od/referencesearch/ss/The-Top-Twenty-Essential-US-Government-Web-Sites.htm>

Source Reliability/Information Credibility

"If it's on the internet it must be true." Remember that commercial? How do we vet sources? Anytime you access the internet you have to enter with a suspect mind. The internet does hold valuable resources that can be exploited but it is also abundant with misinformation, disinformation, individuals waiting to exploit you, and of course the sites you don't want your children exploring. For the most part it can be a gold mine of valuable information but just how can you determine the reliability and credibility of what you find?

We are constantly bombarded with information from local, state, federal, and of course global. We interpret information according to our biases, cultural, upbringing, and many

times according to whom we want to influence for our own ulterior motives or someone else's. Everyone has their own agendas and motives. Factual information can be made to sound false and false information made to sound factual. It is up to the listener or researcher to separate the good from the bad or to use the idiom of separating the wheat from the chaff. In other words, to select what is useful or valuable and reject what is useless or worthless.

Analysts are routinely put on the spot to give a briefing or update a particular situation with the latest information with very little time for preparation or in depth research. This is when it becomes critical that the information has been thoroughly researched to keep the requestor or ultimate user of the information from making a bad decision.

There are some questions that must be answered in order to define the reliability of a source like **who** created the information, is it an authoritative source, what else has the source published; **when** was the information created, what is the date and context of the information; **where** was it released, is it an authoritative site, is the information public or private, and where is it hosted; **what** does it contain, is it confirmed by other sources; and finally **why** was it posted or released?


Good reading on subject.

<http://verificationhandbook.com/downloads/verification.handbook.pdf>

<http://verificationhandbook.com/downloads/verification.handbook.2.pdf>

http://verificationhandbook.com/downloads/verification.handbook_additional.pdf

I'm certain everyone remembers Mr. Colin Powell before the United Nations making a case for attacking Saddam Hussein because he was storing chemical weapons in Iraq. The American people trusted Mr. Powell because there was no reason not to; he was a respected individual and we gave him an A1 rating. But Mr. Powell had also been misled by others. What about Rafid Ahmed Alwan al-Janabi, codenamed Curveball, who gave the false information? What kind of rating was he given? Obviously a very high one when in fact he should have received an F8. Here we are talking about people but the same applies to information on the web. Remember the 5 w's above: who, what, when, where, why.

Code	Rating	Description
A 	Reliable	No doubt of authenticity, trustworthiness or competency; has a history of complete reliability; usually demonstrates adherence to known professional standards and verification processes.
B	Usually Reliable	Minor doubt about authenticity, trustworthiness or competency; has a history of valid information most of the time; may not have a history of adherence to professionally accepted standards but generally identifies what is known about sources feeding any broadcast.
C	Fairly Reliable	Doubt about authenticity, trustworthiness or

		competency but has provided valid information in the past.
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness or competency but has provided valid information in the past.
E	Unreliable	Lacking in authenticity, trustworthiness or competency; history of invalid information.
F	Cannot Be Judged	No basis exists for evaluating the reliability of the source; new information source.



Code	Rating	Description
1	Confirmed	Confirmed by other independent sources; logical in itself; Consistent with other information on the subject.
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject.
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject.
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject.
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject.
6	Misinformation	Unintentionally false; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	Deception	Deliberately false; contradicted by other information on the subject; confirmed by other independent sources.
8	Cannot Be Judged	No basis exists for evaluating the validity of the information.

Online Translation Services

For the OSINT Analyst time is always a serious issue and fortunately machine translation can save the day. Translation software can decipher the content quickly and provide a quality output to the analyst in no time at all. It is reasonably inexpensive when compared to a professional service which normally charges on a per page basis which in the long term can be rather pricey. Another advantage to machine translation is confidentiality when certain sensitive information cannot be shared with a professional translator.

If you expect to get a literal translation from one language to another it is probably not going to happen. Several reasons for this are cultural, nuances, body language that cannot be seen, and unless you are a native speaker with the cultural background much is going to be missed. Even commercial software that is very expensive misses a lot

and is not known for accuracy on a consistent basis. You can get an idea from the output but the software will only do word for word translation and not comprehend the data which more than likely will have to be revised manually. The translation will also not look for things like the variation of a word or the way it is used or pronounced. It may mean different things in various areas of the country. What was the body language of the person speaking? Following are several translation sites that should provide good output when used together.

[Paralink](#) Translate a passage of text into numerous popular languages. Will even translate English text into Persian/Farsi.

[Google Translate](#). With 72 languages, they have the largest repository of the online translation services.

[Dictionary.com Translator](#). 53 translation languages, Icelandic and Maltese among them. The only downside is that there is a 300 character limit.

[Bing](#). 44 language repository with a user interface.

[Free Translation](#). Translates from 41 languages (Bengali among them!), but only into the big five (English, Spanish, Italian, French and Portuguese).

[BabelXI](#). Translates 36 languages.

[itranslate4.eu](#). Translates both in and out of 35 languages across many different search engines! Language repository includes unexpected languages such as Breton, Esperanto, Kazakh and Occitan.

[Babylon](#). Translates 30, including two different forms of Chinese. It is very similar to the capabilities of Worldlingo and imTranslator.

[SYSTRANet](#). It translates out of 15 languages.

[Babelfish](#). Translates 14 languages both ways. 300 character limit applies.

[Reverso](#). Limited language capacity (9 languages) with

the option to have translation read in the target language.

[Worldlingo](#) Personal service offering unlimited translation of text, documents, emails, and websites in 15 languages for \$4.95 a month

[imTranslator](#) The current version of PROMT-Online supports 55 languages or 2970 language combinations.

[Translation2](#)

[Online-Translator](#)

[Transl8it](#) Just type in SMS, text message, emoticon, smiley, slang, chat room net lingo or abbreviations and let transl8it! convert it to plain english to understand -- OR - type in your phrase in english and convert it to SMS TEXT lingo slang!

Managing Information Overload



Stay in the passive mode by making information come to you. OSINT Analysts tasked with research know the struggle of keeping up with the latest news, and going through the websites is a long and demanding process. RSS can cut down on the time spent perusing websites. What is RSS you ask? A quick and short description: RSS feeds give analysts a way of managing information overload by keeping up with blogs, news sites and other websites. RSS allows the content to come to the analyst without having to go to each site individually to view the latest updates. Anyone can

choose the sites they wish to subscribe to, and then get updates in one centralized location. The analysts benefit because the feeds are automatically fed to them based on the news they have programmed into the feeds. Many of us are wary of providing personal information on the web so the feeds make it very convenient to receive the latest without having to expose ourselves. Newsletter providers are known for requiring personal information in order to subscribe.

RSS makes web feeds available from a site like a blog, news outlets and other posts to subscribers in order to provide other people with a summary of the most recently added content. The new content is normally added to the very top of the other posts from previous days. This makes it easy for the reader to backtrack any related items. It appears that everyone involved with blogs and other similar postings use a standard format which makes it very convenient for those new to RSS feeds. The convenience to the OSINT Analyst is that he/she is passive rather than active and can be notified of new content without having to actively check for it: simpler than websites, media are automatically downloaded, unsubscribe by simply removing the feed from their aggregator, and finally RSS is a great way to collect information since the analyst is basically anonymous. Instead of checking all the websites you normally follow, you can just open an RSS reader app and see what's new on all of those sites together. You do not leave a trace of search terms but simply are the recipient of a site that interests you. Oh, and by the way, RSS stands for Rich Site Summary or Really Simple Syndication.

Look for the orange logo on websites, and when doing a search query be sure to add "RSS Feed". If the site has a feed the orange logo will appear somewhere on the page (normally at the very top or very bottom).



Following is a list of RSS aggregators with still functional links. Although some are no longer updated or supported they still provide a great service. The first 6 are either free or require a one-time fee. I personally like RSS Bandit (I did not say prefer). I have been using it for several years and have gotten very used to it and just know how to tweak it to answer my requirements. When it comes to handling information overload RSS is simply the answer.

NEWZPILE I definitely recommend this site for creating awesome RSS feeds on practically any subject you're tracking. Tracks "web buzz" of different topics in real time from a variety of sources including Twitter, YouTube, Google News, Flickr, and Google Blogsearch.

[Daily Top RSS Feeds](#)

[Selfoss](#) is another self-hosted RSS option that lets you follow sites and your favorite people on Twitter in one app. Like many of the other RSS apps so far, it simplifies the reading experience and has some basic features

that help you organize your feeds. [Inoreader's](#) "Discovery Mode" can help you find and follow specific topics and trending items.

[Feed Wrangler's](#) goal is to help you "wrangle" the news. It's a distraction-free reader—boasting perhaps the cleanest interface in this list—that makes managing feeds simple.

[NewsBlur](#) allows you to subscribe to different sites and organize your content into folders.

[Feedbin](#). Once you've subscribed to your favorite sites, you can use Feedbin's tagging system to organize your content into categories.

[Feedly](#) is designed to be a simple way to build your own newsfeed about your favorite topics.

[Active Web Reader](#) - Free aggregator. Supports RSS feed formats 0.9x, 1.x and 2.x. Requires Internet Explorer 6 or higher.

[Aggie](#) - A .NET based open source application for reading RSS feeds. Supports RSS versions 0.91, 0.92, 0.93, 0.94, 1.0, and 2.0.

[Awasu](#) - Free RSS client, allowing monitoring of a variety of news sites and weblogs. Using plugin architecture, can also be customized to monitor databases, email accounts, and other resources.

[CITA RSS Aggregator](#) - Free full function aggregator that can also deliver bittorrents. Can access feeds secured by user ID and password. Includes tool to remove adverts from feeds. Requires .NET Framework.

[Chaos Wallpaper](#) - A utility that rotates desktop wallpaper while displaying RSS or Atom feeds on the desktop.

[Composite](#) - A free desktop RSS/RDF aggregator application for .NET.

[CyberBuddy](#) - CyberBuddy is a freeware application that delivers

a variety of content to your desktop, including RSS News Feeds, via talking agent characters.

[Feed Notifier](#) - Feed Notifier is an application for Windows and Mac OS X that resides in the system tray or status bar and displays pop-up notifications on your desktop when new items arrive in your subscribed RSS or Atom feeds.

[FeedReader](#) - Open-source aggregator that supports RSS and Atom formats. Runs under Windows 95 and later versions.

[Fuzzy Duck RSS Reader](#) - Reads RDF, RSS and Atom formatted XML news feeds.

[GreatNews](#) - Supports all major RSS feed formats; integrates with Bloglines. Doesn't need .NET or Java runtime. [Windows 2000/XP/2003].

[News Interceptor](#) - Aggregator reads both RSS feeds and non-RSS based news sources.

[NewsPiper](#) - A freeware RSS feed and web news reader that can speak headlines.

[Newz Crawler](#) - Provides access to news content from several sources, including XML, RSS, Usenet, and the Web.

[Novobot](#) - A heavily featured desktop newsreader, that can also scrape non-RSS sites.

[QM nooze](#) - Very simple RSS/RDF reader with simple interface and small memory footprint. [Win 95/98/Me/NT/2000/XP]

[RSS Bandit](#) - A free desktop news aggregator for Windows built on the .NET Framework.

[RSS Captor](#) - A configurable RSS feed reader. Supports all versions of RSS and has an audible alert for new messages.

[RSS Popper](#) - A free news aggregator for Outlook. Allows reading of RSS/RDF/Atom feeds in Outlook.

[RssReader](#) - Free RSS reader is able to display any RSS news feed. Requires Microsoft .NET Framework 1.1.

[SharpReader](#) - Three-pane RSS Aggregator for the .NET framework.

[Vienna](#) - Vienna is an RSS/Atom reader for Mac OS X, packed with powerful features that help you make sense of the flood of information that is distributed via these formats today.

[Vox Lite](#) - Allows visitors to keep up-to-date with sources of information that support the RSS protocol. Requires .NET Framework 1.1.

[Web Reader](#) - You can follow your favorite sites, online newspapers, blog, forums, comments, video channels, photo albums, deal-of-the-day websites and more.

[blogbot for Outlook](#) - Blogbot for Outlook is an RSS/Atom/weblog aggregator that plugs into Microsoft Outlook 2000/XP/2003. It monitors subscriptions to Internet news feeds and delivers new posts to folders within Outlook.

[blogbot lite](#) - RSS/Atom news and weblog application integrated with Internet Explorer in a sidebar.

Open Source Imagery: A Picture Is Worth a Thousand Words

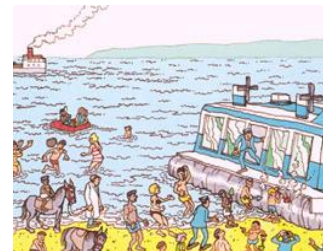


Imagery, no matter what type, is probably my passion when it comes to attempting to extracting information. Latest estimates say that approximately 1.8 billion photos (and I suppose those include XXX) are uploaded to the

internet every day, so that means I will never be without an interest. Perhaps I'm somewhat unfair because of a previous job. For approximately 3 years I averaged about 1 aerial recon mission per week and burned anywhere from 20 to 30 rolls of film (way before digital cameras), each with 30 frames. Multiply that and you get 600 to 900 frames per mission. But let me explain, we operated hand-held automatic cameras that could shoot 3 to 4 frames per second. The idea was to get pictures as close as possible to each other so that when developed we could place them under stereo glass and be able to see as much detail as possible. All photos were black and white, and I was not an imagery analyst; I was a 96B (now 35F) intelligence analyst.

(Source: http://en.wikipedia.org/wiki/A_picture_is_worth_a_thousand_words) The adage "A picture is worth a thousand words" refers to the idea that complex stories can be described with just a single still image, or that an image may be more influential than a substantial amount of text. It also aptly characterizes the goals of visualization where large amounts of data must be absorbed quickly.

Look at the picture to the right; so many things you can imagine are being said. The big brother could be threatening the little brother or he could be pleading with him to release the soccer ball. He could also be bribing him with money or a movie. Hard to tell what is being said but like a true analyst you have to make assumptions grounded on what you see. But this picture is too simple. Let's take a picture like a "Where's Waldo" as an example. A picture with so much detail as this has to be studied in sections. I do this by breaking it into quadrants and then depending on how much the photo can be accentuated without losing too much detail I further break those quadrants into quadrants also. In these examples the first quadrant is at the upper right hand corner.



This photo shows a group of foreign soldiers. It was in a magazine several years ago. Think of all the information that can be extracted from



this publicly available photo. A good example of passive collection versus active collection. Types of weapons, uniforms, training, hygiene, etc.

What about family photographs? Look at some family photos from years past and really study them. You will find minutiae that you had not noticed before. Is there any



information in the photos that you can use to your benefit? Perhaps there's a silverware set sitting on the kitchen table. You never paid much attention to it until now. You start wondering where it is and you always had your eye on it. Now is the time to start buttering up to your grandmother or aunt. What have you just accomplished? You have taken simple information from a photo and are now scheming to use it to your advantage. You now have information to support a planned operation of perhaps making sure that you are the one to inherit the silverware setting, or maybe just getting it as a gift.

Photo Surprises (discovering out of view information). The most apparent use for some of these software is to find out where an image was taken but if the GPS has been turned off on the camera or cell phone then it will be of no utility. However, this software will compare a photo to others on the web and you may find the information you seek. Perhaps someone else took the same photo with the GPS operational.

<http://metapicz.com/#landing> View metadata.

<http://regex.info/exif.cgi> Jeffrey's Exif Viewer. Searches the metadata and if a location is listed (GPS) it will bring up a map of the location.

<http://www.findexif.com/> Online photo EXIF metadata reader

<http://www.tineye.com/> Reverse image search engine. It finds out where an image came from, how it is being used, if modified versions of the image exist, or if there is a higher resolution version.



<http://fotoforensics.com/> This one works quite well with TinEye, Google and Reddit image searchers.



<http://www.imageforensic.org/> Image Forensic. You can verify if an image was manipulated.



<http://29a.ch/photo-forensics/> Forensically Beta

<http://imgops.com/> A metadata image tool.



<https://images.google.com/> Reverse image search

<http://karmadecay.com/> Reverse image search of Reddit.com (beta)



But very soon we may not have to struggle to find where a photograph was taken thanks to new software, called PlaNet, being developed by Google. Even with the GPS turned off, the software has awesome capabilities. The new technology can even determine the location of indoor images and pictures of specific things such as pets, food, and so on that have no location cues. Think of the possibilities for the military and law enforcement. <https://www.technologyreview.com/s/600889/google-unveils-neural-network-with-superhuman-ability-to-determine-the-location-of-almost/>

OSINT Analyst Tools

The only way to become skillful with these tools is to actually take them for a spin. Use real world events to get a feel for what you can do with them. Maltego and Foca are GR8 tools and can be used in conjunction with others. Some sites do require an account but what's stopping you from creating a phony profile (some of you must take into consideration common sense, OPSEC, and intelligence oversight)? Facebook alone boasts 83 million fake profiles and twitter has 20 million.

Go ahead and establish one; it can be for Facebook, twitter or whatever. Make it a fake one if you so desire. I would venture to say that many who do investigative research have fake accounts. These are two sites that can assist you in establishing a fake identity: <http://www.identitygenerator.com/> and <http://www.fakenamegenerator.com/> . However, to avoid leaving easily followed electronic footprints I recommend using a VPN service or the [TOR](#) software. Print a copy of what you filled out online via the print screen button on your keyboard. Don't forget to clear the browser's history. Now you can modify the printed hardcopy to your liking without doing it online and create an account. Be sure to retain a copy for your records, you may have to remember who you are at a later date because of some account verification. There is definitely no criminal intent by doing this, unless you **ARE** a criminal.

<http://whatcha.xyz/index.html> - You simply add the number you'd like to spy on, and ... That's it ! We'll do the rest!

<https://twitter.com/search-home> - See what's happening locally by entering zip code. Has additional functions.

<https://tagboard.com/> - Search engine with data about hashtags.

<http://hashtagify.me/> - Search engine with data about hashtags.

[Keotag](#) - lets you search multiple search engines, create social bookmark links around a topic or see who has used your brand as a tag.

[Tweetdeck](#) - The most powerful Twitter tool for real-time tracking, organizing, and engagement.

[Twazzup](#) - is a dashboard program that monitors Twitter, Twazzup will let you know whenever your keywords are mentioned in a [tweettools/#sthash.6QkBcVpz.dpuf](https://twitter.com/tweettools/#sthash.6QkBcVpz.dpuf)

[Twitterfall](#) - is a great way to keep up on conversations about an event, or an online chat, using hashtags. You can also use its geolocation panel to see discussions in a geographic area. - See more at: <http://www.socialbrite.org/2011/01/11/guide-to-free-social-media-monitoring-tools/#sthash.6QkBcVpz.dpuf>

[GeoChirp](#) - Helps you search for people Twittering for specific things in a specific area. It allows you to select an area on a map, choose a radius, and view tweets emanating from that location in real-time. You can include keywords in the search to see only those tweets that include a specific keyword.

[Tweetpaths](#) - Plots a Twitter users geotagged tweets on a map in real-time.

[Mentionmapp](#) - Provides a visualization of a Twitter user's tweets as determined by "mentions" of hashtags and other Twitter users. The lines connecting users are thicker or thinner depending on the strength of the connection.

[Trendsmapp](#) - Continuously tracks twitter trends and uses the location on users' Twitter profiles to map tweets to a geographic location.

[SpiderFoot](#) - Open Source Intelligence Automation Tool (OSINT). Please be careful with this one.

[Spokeo](#) - People search engine and free white pages finds phone, address, email, and photos. Find people by name, email, address, and phone for free.

[Foca](#) - FOCA 3.2 Great tool for gathering tool to find metadata and hidden information in the documents its scans. These documents may be on web pages, and can be downloaded and analyzed with FOCA.

[Shodan](#) - Search for computers based on software, geography, operating system, IP address and more

[Maltego](#) - Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure.

[Hoovers](#) - Search over 85 million companies within 900 industry segments; Hoover's Reports Easy-to-read reports on key competitors, financials, and executives

[Market Visual](#) - Search Professionals by Name, Company or Title
[LittleSis](#) - LittleSis is a free database of who-knows-who at the heights of business and government.
[Entity Cube](#) - EntityCube is a research prototype for exploring object-level search technologies, which automatically summarizes the Web for entities (such as people, locations and organizations) with a modest web presence.
[TinEye](#) - TinEye is a reverse image search engine built by Idée currently in beta. Give it an image and it will tell you where the image appears on the web.
[Social Mention](#) - Social Mention is a social media search engine that searches user-generated content such as blogs, comments, bookmarks, events, news, videos, and more
[Google Trends](#) – See what are the popular related topics people are searching for. This will help widen your search scope.

[Google Alerts](#) - Google Alerts are email updates of the latest relevant Google results (web, news, etc.) based on your queries.
[Addict-o-matic](#) – Nice little search aggregator. Allows you to enter a search term and build a page from search and social networking sites.
[PasteLert](#) - PasteLert is a simple system to search pastebin.com and set up alerts (like google alerts) for pastebin.com entries. This means you will automatically receive email whenever your term(s) is/are found in new pastebin entries!
[Whos Talkin](#) - social media search tool that allows users to search for conversations surrounding the topics that they care about most.
[TouchGraph SEO](#) – Java based tool for importing and visualizing various data types. Very simple but may have some utility.

Overtly Covert or Covertly Overt

The one thing to remember is that of covering your own tracks when conducting research. What if the person you're following has his/her own website and control their own server? Their IT person would very easily identify your IP address and be able to follow you back to a location even through an in between referrer link. Using software like [Tor](#) (The Onion Router) a free open-source Web surfing program that runs in the background and hides your surfing habits and location will help in covering your tracks; it accomplishes this by routing the user's data through a series of computers each one of which encrypts the data passing through it. According to a project overview the Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations. The drawback is that it slows down page views because of the numerous hops to hide your IP address. Another way to maintain anonymity is by way of a virtual private network (VPN). To prevent traces, you can use a VPN to hide your IP address. It's the same sort of connection used by many corporations to prevent security breaches using encrypted tunneling, but you can use it to route your connections through a remote server, often in a different country, and thus thwart trackers. Download the Tor manual at <http://www.makeuseof.com/pages/really-private-browsing-an-unofficial-users-guide-to-tor>



Virtual Private Network


What is a VPN Source: <http://www.proxpn.com/#how>
A VPN (virtual private network) is a network that can use the internet to provide secure connections between one or more devices for data exchange. A VPN can open a secure interconnection or "tunnel" between different devices and the data that passes

through the tunnel can be encrypted as a method of security so that the data passing through the tunnel cannot be read. Most often, VPNs are used to connect a company's main office with its satellite offices or its field agents. In some cases, people choose to connect their personal devices to a VPN service provider to secure their own connections (with the same kind of tunneling and encryption) to the general internet, keeping their banking details, credit card numbers, passwords, and other sensitive data from being intercepted, monitored, or recorded. This kind of VPN setup also affords the user an anonymous IP (internet protocol) address (used for determining a device's location), making them appear as if in a far away location. [proXPN](#) is an example of the latter scenario, just on a global scale.

Go to <http://www.makeuseof.com/pages/best-vpn-service-providers> for further information on VPNs.

Free and popular commercial VPN services include Tunnelbear (<http://www.tunnelbear.com>), browser extension for private browsing that allows you to choose a VPN server location from 15 countries, Strong (<http://strongvpn.com/>), [Private WiFi](#) (PRIVATE WiFi is VPN software that encrypts all your Internet communications) and [proXPN](#) (proXPN is a global virtual private network that creates a secure, encrypted tunnel through which all of your online data passes back and forth). I have to add one more pointer and that is that even when utilizing privacy software, make certain to clear your browser's history at the end of each research session.

Top VPN Services

 **ExpressVPN** 100+ VPN locations... and counting! You can choose from 100 cities in 78 countries. With unlimited speeds and unlimited server switches, you can connect from anywhere in the world. <https://www.expressvpn.com/>

PureVPN now offers "Virtual Router" feature within its Windows application. With this feature, you can convert your Windows-based desktop or laptop into a virtual router and use it to connect up to 10 devices. <https://www.purevpn.com/>

Use our free proxy to surf anonymously online, hide your IP address, secure your internet connection, hide your internet history, and protect your online identity. <https://www.hidemypass.com>



Other Privacy Tools

AMRDEC SAFE is designed to provide AMRDEC and its customers an alternative way to send files other than email. SAFE supports file sizes up to 2GB.



Our easy-to-use software lets you change your IP address anytime by routing your Internet traffic through private and secure servers worldwide. A small dropdown box will appear on your web browser toolbar (e.g. Internet Explorer / Firefox) with a list of several countries. Select one and your IP address will change so that you appear to be located in that country. <http://www.iprivacytools.com/>



Hotspot Shield VPN is the ultimate Internet security solution that secures your browsing session, detects and blocks malware, protects your privacy and allows you to **access blocked sites**. Hotspot Shield is available both as a **free VPN** and a paid Hotspot Shield Elite subscription. <http://www.hotspotshield.com/>



Hide your IP: Nobody will know where you are from; Encrypt internet data: Protect your Internet data with strong 256-bit encryption; Remove limits: Use any site you need without any limitations. <https://www.hideman.net/en>



Your online activities can reveal intimate details about you and the websites you visit. Anonymizer Universal ensures your identity remains anonymous and your personal information is protected and secure every time you're online. <https://www.anonymizer.com/>



Proxify is an anonymous proxy service which allows anyone to surf the Web privately and securely. Through Proxify, you can use websites but they cannot uniquely identify or track you. Proxify hides your IP address and our encrypted connection prevents monitoring of your network traffic. Once using Proxify, you can surf normally and forget that it is there, protecting you. <https://proxify.com/>



Online protection, simplified. Join over 3 million people who use our open source software to protect their identities and sensitive personal info from hackers and trackers. <https://disconnect.me/>



Many mice surf the web under the illusion that their actions are private and anonymous. Unfortunately, this is not the way it is. Every time you visit a site for a piece of cheese, you leave a calling card that reveals where you are coming from, what kind of computer you use, and other details. And many cats keep logs of all your visits, so that they can catch you! This service allows you to surf the web without revealing any personal information. It is fast, it is easy, and it is free! <http://anonymouse.org/anonwww.html>

Many web sites are harmful and attempt to log your IP address for improper use. Some spyware applications and web sites with harmful code sometimes need your personal IP address in order to do their dirty work. An anonymous proxy hides this information from the web sites you visit. Just type an address in the search window of the web page and you will see the page load. Any links you click from there will also be secure. There will also be a new form located at the top of the page. Use that form to continue to surf the web anonymously. <http://vectroproxy.com/>



CyberGhost

CyberGhost is a fast, simple and efficient way to protect your online privacy, surf anonymously and access blocked or censored content. It offers top-notch security and anonymity without being complicated to use or slowing down your internet connection. CyberGhost VPN hides your IP and replaces it with one of your choice. This way, you surf anonymously. "If you are looking for a free VPN service, CyberGhost VPN is by far the best one I've seen." PC Magazine.



https://www.cyberghostvpn.com/en_us

How does OkayFreedom VPN work? Upset when you can't view a video online? With our VPN-service OkayFreedom this problem is now history. But OkayFreedom VPN is also the right choice when you just want to prevent someone from following your traces on the internet. OkayFreedom VPN recognizes whether content, videos and entire websites are restricted in your country and automatically directs you over a server which enables you to view the content.



<https://www.okayfreedom.com/>



ZenMate is a next generation free vpn software which hides your IP and protects your privacy. With ZenMate installed you can surf anonymously, free from the snooping eyes of ISPs or government agencies. ZenMate is also free to use, so you can simply add it to your browser and in seconds be enjoying the web without any restrictions. <https://zenmate.com/free-vpn/>

People Finder

When searching for a person be sure to use several sites at the same time for better results. Some sites are very limited on information and using at least 3 will produce better outcomes. I like Pipl and it appears to have the better results of all the sites. Although there are several more sites those listed below are the ones I use and have gotten good results when using them simultaneously. One site may turn up a piece of information but not give you additional information that you are looking for. But that one piece of information can be used on another site and possibly retrieve what you need.

Several years ago I lost touch with a good friend. I had 3 pieces of information on him; I knew his name (obviously), his wife's name, and his approximate age. I used spokeo, peekyou and pipl for my searches. You can't imagine how many people have the same name to include wife with the same name. I was able to narrow him down to a particular city based on the approximate age but I still had to work through 3 individuals in the

same town. At least I had 3 addresses that I could look up on Google Earth and I had good luck on my very first try. From the overhead I went into street view and did a walk through on the street. I made it to one of the addresses and there in the front yard was an individual kneeling down planting flowers. I zoomed in and was lucky enough to see that the face had not been completely obscured from one angle. I had found my friend. So in this instance Google Earth also played a role. Other searches may not be as easy as this one but if you persist you will succeed. I have added one that is not particularly listed as a people finder but believe me it works great if you have the time to work through the results. It is vehicle purchase records database (<http://vin.place/>).

www.spokeo.com www.thatsthem.com www.zabasearch.com www.pipl.com http://vin.place/ www.peakyou.com www.411.com https://thatsthem.com/	http://www.whitepages.com/ www.veromi.net http://www.peoplefinders.com/ http://infospace.com/ (recommend using the results from https://www.mylife.com/ , and http://www.peakyou.com/)
--	--

Another way to find people is by way of email address if you have it. Facebook has over a billion users and chances are high that you may be able to locate that person via Facebook. Go to the search box and enter the email and if a profile exists it should pop up immediately. If a profile exists, more than likely a picture will be available. Take the photo and paste it into Google Images. You can do a reverse image search and if that person has used the same photo on other social profiles then you're in luck. This also works quite well if you receive an email from an unknown person and you want to know who it is before striking up a conversation.

Inadvertent Achievement

Now let's assume that quite by accident, and I do mean accident, you acquire information while surfing the internet at home that fits in with a work related assignment. Well you certainly don't want to send that information to your work email account or place it in a shared drive, but you also don't want to leave too many traceable electronic footprints when you do send it out. The best way to move the data between two separate devices is via the "[The Internet Clipboard](#)." The information is destroyed as soon as it is read and anyone visiting the same URL at a later time will not be able to see the message. The instructions are very simple and easy to follow. I would further recommend using a VPN and the incognito function on your browser for added security.

Private Search Engines

When it comes to browsing the Internet, privacy has been a constant concern, and this year is proving to be no different. In fact, could 2016 be the benchmark year for search engines that respect our privacy? <https://www.rocketmill.co.uk/what-does-the-growth-of-private-search-engines-mean-for-paid-search>

OSCOBO. No tracking, just searching. <https://oscobo.co.uk/>

Startpage. If you prefer Google's search results and just want more privacy, try Ixquick's Startpage. Startpage searches Google for you – when you submit a search, Startpage submits the search to Google and returns the results to you. All Google sees is a large amount of searches coming from Startpage's servers – they can't tie any searches to you or track your searches. <https://startpage.com/>

Ixquick is the main search engine from the company that runs Startpage. Unlike Startpage, Ixquick pulls results from a variety of sources instead of only Google – this can be a good or a bad thing, depending on how much you like Google's search results. <https://www.ixquick.com/>

Duckduckgo. The search engine that doesn't track you. Doesn't log any personally identifiable information. DuckDuckGo doesn't use cookies to identify you, and it discards user agents and IP addresses from its server logs. <https://duckduckgo.com/>

Privatelee, the most private and secure (https available) search engine. <https://privatelee.com/>

Grobe.it, combines the best results and functionality from the top search engines so you always get the best results. <https://grobe.it/>

Yippy will not collect personally identifiable information about you, like your name, telephone number, address or email address. However, it may collect anonymous information about your computer, like your IP address. It also uses cookies, but not to track your personal behavior. <http://yippy.com/>

Lukol. No IP tracking. No search term tracking. Your search, your privacy. Period. <http://www.lukol.com/>

Disconnect is part of a whole suite of software that is dedicated to keeping people's activities on the Internet private. All of Disconnect's products, including its search engine, follow four basic rules. First, they never collect any information about you without you saying so, which includes things like your computer's Internet address and (consequently) your location in the world. <https://search.disconnect.me/>

OSINT Situational Awareness

Simply put – knowing what is going on around you 24/7/52. Why is this so important? Remember what I said above about presenting information in a timely manner, and also about time management when doing research. But in the same breath I have to repeat the “beware and be aware” line. Be cognizant of everything that is going on around you and look for the threats that others may fail to recognize, but at the same time be wary of deception.

To be fair, even though we are constantly processing information not everyone can be a top-notch analyst, but everyone can be a collector. We are sensors; we are all the intelligence disciplines rolled into one. Your acquisitions, observations, collections and exploitation of open source information will create OSINT. To be sure, all your surroundings are constantly giving off information.

I have taken the acronym “OSINT” and broken it down into its individual letters for a simple reporting format.

OSINT – **O**bservation

This is the initial eyes-on and equates to investigation. What is it? What am I observing? Give a short description but don't get too detailed. The simpler the report, the more sense it makes to the OSINT Analyst. When a report gets too detailed the analyst will have a tendency to just skim it and possibly miss some key points. You may be on a critical mission and do not have the time to hang back so this one is very significant. You also may be in a baaaaad neighborhood. Gangbangers hanging on the corner and looking at you through the corner of their eyes. Not a good place to be in unless you're wearing a uniform. Ok, so let's take in the surroundings. What do I see?

Buildings – What's so special about this particular building? Could there be a meth lab operating inside? Could it be a distribution point for other drugs? What about a human trafficking shipping point. Do you hear people crying, or yelling? This is further discussed with the “senses” section below.

Vehicles – Type, make, model, year, etc. These give clues to the driver's occupation. Is the driver a user, distributor, seller, liaison, collector, etc. Why is a lone vehicle parked on the side of the road/street? This would be unusual, especially in a known gang neighborhood. Has the driver been kidnapped or is the driver doing business? What about a broken down vehicle with the hood raised? Obviously a vehicle on blocks with all wheels missing and the steering wheel spinning is a no-brainer.

Graffiti – The artist is proud of his/her work and will leave identifying signatures for others to see. Lots of color, plain black and white, or just want to send a message to others. Is the lettering artistic? You'd be surprised at how much intelligence simple graffiti sends out.

People in general – Are they watching from a distance? Do they avoid eye contact? Some may be too friendly and offering information. They could be acting as decoys and distracting you from doing business or covering for someone else doing business. Observe their body language; it is full of information. Their walk and dress will mimic the culture of the neighborhood they happen to be in to blend in and avoid being seen as someone who doesn't belong. The one thing that may give them away is the haircut and to cover this up they will wear a hoodie or oversized headgear.

Tattoos – MS13 gang members and others to be sure, are proud of their gang affiliations and will transmit that loyalty. Tattoos are a good source of information and all that it requires is good observation. You don't have to ask questions or even be in the vicinity of a gang member. A website is just as good and safer. Gang members have their own websites and are proud of what they post.

Gang Hand Signs – Hand signs were first used by Chinese Triads several hundred years ago. Black gang members introduced hand signs to the gang culture in the mid-1950s in Los Angeles. It is believed they copied their hand signs from family members who used secret hand signs in their fraternal societies and masonic groups. Hand signs are a powerful nonverbal form of communication much like the American sign-language. A quick flash of the hand is used as an announcement of gang affiliation or as a challenge or insult. These hand signs, which are quickly displayed with the fingers, hands and body, have very specific meanings to gang members. This nonverbal form of communication has been quickly accepted and adopted by gangs across the nation.

Posting is another form of nonverbal communication utilized by gang members. Posting is a system of postures, facial expressions and body motions to convey a message. When photographed the gangster may hold their chin up to display their feeling of defiance and arrogance or they may cross their arms and intently stare at someone to show their feeling of disapproval or as a challenge.

Another common gang indicator, mostly seen in the Midwest is that of right versus left. If the belt buckle or hat, for example, is tilted to the right or to the left, this may indicate possible gang affiliation. One pant leg or shirt sleeves may be rolled up or the member's hat may be tilted to the right or the left, would indicate which gang they affiliate with. When they get dressed, fold their arms or cross their legs, it will be done according to one side first, the other side second or one side on top and the other on the bottom.

oSINT – Senses

What do the 5 senses tell me? See, Hear, Smell, Taste, Feel. Observation and senses are not one and the same. What you sense may not be what you observe. You know – that gut feeling.

See – What are the significant features? If it's a building is it made out of concrete, cement, wood, etc? Why is this important? If it is determined that the building needs to be entered, then the right amount of firepower is applied to reduce the collateral damage. If terrorists (maybe even hostages) are hiding in the building, then it takes on a more important aspect. Are the intentions to take prisoners or to kill? What about hostages? Hostages need to be protected at all costs. You may recall that maximum firepower was applied to the house in which Uday and Qusay (Saddam's sons) were hiding in. Clearly the intention there was not to take any prisoners.

The windows also are clues as to inside activity. Frosted or clear? Have they been painted over to hide activity? The color of paint is also important. Light colors reflect heat while dark colors absorb. Are there fans mounted on the windows? If so, are they directing air to the inside or to the outside? When working with chemicals or other dangerous materials the air has to be directed to the outside to protect workers. One side of the building may have fans directing air into the building while on the other side

the fans may be directing airflow out. Report everything you see. It may not make sense to you but it will to the analyst. With human/drug/arms trafficking as a criminal enterprise and the heavy costs exacted on the innocents, the senses become a more meaningful tool.

A new vehicle with bald tires or an old vehicle with new tires is information waiting to be exploited. Why are there heavily worn tires on a new vehicle? This is an indicator of heavy usage. Why has an old vehicle been outfitted with heavy duty shock absorbers and new tires? Think heavy loads, like marijuana or even worse, a nuclear device. Have you ever wondered why sometimes at the Border Patrol checkpoints you are just waved through without a second thought on their part? You go home and complain to everyone that they are not doing their job. What good are they? They are in fact doing their job and doing it quite well. They are interpreting information from both the occupants and the vehicle. They are looking at the windshields for heavy dust, splattered bugs, cracks, condition of the headlights, etc. All indicators of where the vehicle has been. Even a water bottle with visible condensation on the inside is telling a story about the occupants. The occupants give off information in many ways too. Nervousness, too talkative, cracking jokes with the officer, deflecting by useless questions. Don't be too hard on the officers. They are in fact doing their duty.

A person lighting a cigarette at night can be seen from great distances. The lighted end of a cigarette, especially when taking a drag, can be seen from up to a mile on a clear night.

Hear – What type of sounds are emanating from the observed objective or from a distance? Is it an aircraft/vehicle engine? Human sounds like coughing, snoring, talking, crying, yelling, etc. Sounds can carry for long distances. Is there an argument taking place? Do you hear machinery like a lathe or something similar? A loud playing radio could be used to mask activities taking place. Electric generators have a very distinct sound. Be precise to what you hear even if you have to imitate the sound during a debriefing.

Smell - What about odors? Do you detect the smell of powder, fertilizer, ammonium, bleach, marijuana, cigarette smoke, etc.? Law enforcement agencies that conduct counterdrug operations will generally burn different drugs so that agents become familiar with the odors (true or not this is what I was told). Odors that were picked up in childhood remain in our memory banks forever and will give clues as to what the source may be. The odor of gasoline, diesel, oil, burnt powder and others are good examples of odors that give very distinct clues. They remain with us throughout our lives. After shave lotions, perfumes, deodorants. This may sound silly but can you capture the odor? Would you be able to describe it during a debriefing? It smelled like vanilla, no, wait, it was more like licorice. Clothing made of cotton has good absorbent capabilities, not only for liquids but odors as well. Remember the individual next to you who smoked all day? At the end of the day you could smell the cigarettes and cigarette smoke in your own clothing. What about spilled alcoholic beverages on clothing? The smell remains for a long time. If you do manage to somehow capture the odor/liquid be sure to put the

items in a sealed plastic bag to secure the odor/liquid. Cotton baby diapers have good absorbent capabilities and should be part of your kit.

Taste – There may be times when you actually have to taste the objects. Again, we did this in our childhood years and those tastes remain with us. Everyone has put a copper penny in their mouth. Have you forgotten the taste? Probably not! Alcohol, whether it be rubbing or drinking, has a certain taste along with odor, same thing with fuels and lubricants. Remember that unidentified liquid on the garage floor? You placed your finger in the liquid and took a small sample to taste. You wanted to see if it was brake fluid, power steering fluid or radiator coolant. If it tasted sweet, you knew right away it was coolant and you could also taste the difference between steering and brake fluid. An example is that of Afghan soldiers. Although they have the latest in sophisticated technology, they will taste a suspicious white powder to see if it tastes salty. This is an attribute of ammonium nitrate, which is a key ingredient in roadside bombs or IEDs. Sometimes the senses are a better indicator. Of course, just like with odors we have to be cautious with tasting certain objects. If in doubt, don't do it!

Feel – Unidentified objects can give lots of clues as to what it may be just by feel alone. Is it rubbery, soft, hard, scaly, or smooth? Gyroscopes for example if they are used in guidance systems have a very smooth surface because of the high tolerances that are required. They are built to exact specifications. On the other hand, there are certain weapons that do not require exact specifications if the intention is just to kill or maim. A piece of metal that is going to be used for shrapnel effects may be just rough in all respects. But along with feel, the shape and size gives indications as to the intended purpose. Could it be the front-end or tail-end of an IED/EFP?

OS|NT – Interpretation (Analysis)

Can you interpret? What is your initial gut feeling? This is very important for the analysts since they are not there to observe first hand. You may hold the missing idea or piece of the puzzle that drives the analysis. Once you have accomplished all of the above or as much as you can, try visualization interpretation. Do not look at the target while trying to interpret. Close your eyes and visualize, but only if you are out of harm's way. What else is there that I have missed? This takes a lot of practice and focus but it can be done. Do not let your mind drift but focus.

OSI|NT – Need to know/share

Need to know and need to share should not clash with each other. This isn't classified so there are no restrictions on the distribution, and besides you are not in a position to classify, declassify or determine who should get it. Everyone has a need to know and

share. Distribute as widely as possible. If it is determined that the information has to be restricted or protected in some way, shape or form then someone else will make that decision. Your job is to get it out as soon as possible.

OSINT – Timely

Timely, timely, timely. Cannot emphasize enough! Time of observation and timely distribution of information is extremely important. Hostages may have to be rescued or an ambush countered. Known terrorists, gang members or drug figures on a wanted list may be inside a building and cannot determine how much longer they will remain. Do not take action yourself but keep the target under observation.

Continuing with situational awareness: The following websites provide a wealth of open source information for researchers and analysts. This is just a sample listing to give you an idea of building your own sources that you can refer to in an instant.

Europe's World. Published twice yearly by the Friends of Europe think tank, Europe's World is the only independent Europe-wide policy journal. Europe's World has established itself as the premier platform for new thinking on political, economic and social issues. Our 100,000 readers – drawn from politics, business, the media, academia, think tanks and NGOs – are a powerful and influential audience who value Europe's World for its thought-provoking articles, Europe-wide outlook and lack of national or political bias. <http://europesworld.org/>

Oxford Analytica. A global analysis and advisory firm drawing on a macro expert network to advise clients on strategy and performance in complex markets. <https://dailybrief.oxan.com/>

National Defense. <http://www.nationaldefensemagazine.org/Pages/default.aspx>

Space War. <http://www.spacewar.com/>

DefenseTech. <http://www.defensetech.org/>

Reuters. <http://www.reuters.com/>

The National Interest. <http://www.nationalinterest.org/>

Center for Security Studies. <http://www.css.ethz.ch/en/>

Sputnik. An international multimedia service launched. Sputnik replaces the RIA Novosti news agency on an international stage (which remains active in Russia) and Voice of Russia. Sputnik intends to counter the "aggressive propaganda that is now being fed to the world". <http://sputniknews.com/>

Global Risk Map. <http://globalriskmap.nicta.com.au/>

China Defense Blog. This is the blog of China defense, where professional analysts and serious defense enthusiasts share findings on a rising military power. <http://china-defense.blogspot.com/>

SinoDefence. Chinese Space Programme and Aerospace Power. <http://sinodefence.com/>

38 North. A website devoted to analysis of North Korea. <http://38north.org/>

START. To advance science-based knowledge about the human causes and consequences of terrorism and serve as a leading resource for homeland security policymakers and practitioners. <http://www.start.umd.edu/>

The Diplomat. Know the Asia-Pacific area. <http://thediplomat.com/>

The Pulse of the Middle East. <http://www.al-monitor.com/pulse/home.html#>

Center for Security Studies. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing. It combines research and policy consultancy and, as such, functions as a bridge between academia and practice. The CSS also operates the ISN (<http://www.isn.ethz.ch/>) as a leading global open-source information platform in the field of international relations and security policy. <http://www.css.ethz.ch/en/>

Global Incident Map. <http://quakes.globalincidentmap.com/>

RAND Corporation. A nonprofit institution that helps improve policy and decision making through research and analysis. RAND has a proud tradition of making its research and analyses widely available to the public. More than 20,000 RAND publications are already accessible at no cost on our external website. The publications provide a rich resource for scholars and others interested in learning and writing about RAND's contributions to public policy. <http://www.rand.org/>

Foreign Military Studies Office. FMSO's Operational Environment Watch provides translated selections and analysis from a diverse range of foreign articles and other media that our analysts believe will give military and security experts an added dimension to their critical thinking about the Operational Environment. <http://fmso.leavenworth.army.mil/>

TradePub. Established in 1994 as the first online subscription services provided for B2B magazine publishers, TradePub.com has grown to be the most sophisticated repository of content for professionals in over 33 industry verticals, with extensive reach through 1000's of B2B partner sites worldwide. As the top destination for the latest research and publications, TradePub.com publishes curated resources on behalf of the world's largest and most influential companies. The TradePub.com research library is #1 resource for professionals to access free research, white papers, reports, case studies, magazines, and eBooks. <http://www.tradepub.com/>

The Aviationist. Run by David Cenciotti (cenciotti@theaviationist.com), a journalist based in Rome, Italy, who launched the blog in 2006: since then, The Aviationist has become one of world's most authoritative and read military aviation websites. On a daily basis, it is quoted, cited or linked by the most important media outlets across the five continents including Huffington Post, Al Jazeera, Al Arabiya, Independent, Daily Mail, NYT, Corriere della Sera, Business Insider, Stern, Der Spiegel, etc. <http://theaviationist.com/>

War On The Rocks. Foreign policy and national security issues. <http://warontherocks.com/>

Canadian Security Intelligence Service <https://www.csis-scrs.gc.ca/index-en.php>

Financial Times. A global 24 hour multichannel news organization. <http://www.ft.com/home/us>

International Relations and Security Network. <http://www.isn.ethz.ch/>

NationMaster, a massive central data source and a handy way to graphically compare nations. NationMaster is a vast compilation of data from such sources as the CIA World Factbook, UN, and OECD. You can generate maps and graphs on all kinds of statistics with ease. We want to be the web's one-stop resource for country statistics on everything from soldiers to wall plug voltages. <http://www.nationmaster.com/au>

The International Monetary Fund (IMF) is an organization of 186 countries, working to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world. <http://www.imf.org/external/>

The World Bank. a vital source of financial and technical assistance to developing countries around the world. Our mission is to fight poverty with passion and professionalism for lasting results and to help people help themselves and their environment by providing resources, sharing knowledge, building capacity and forging partnerships in the public and private sectors. <http://www.worldbank.org/>

Academic Search <http://academic.research.microsoft.com/>

The Economist. The Economist online offers authoritative insight and opinion on international news, politics, business, finance, science and technology. <http://www.economist.com/>

The Economist Intelligence Unit. The EIU publishes a number of reports each year focusing on current issues affecting specific countries, regions and industries. These reports are available at no cost and help business leaders prepare for opportunity. <http://country.eiu.com/AllCountries.aspx>

Foreign Policy. American news publication, founded in 1970 and focused on global affairs, current events, and domestic and international policy. It produces content daily on its website, and in six print issues annually. <http://foreignpolicy.com/>

Foreign Affairs. American journal of international relations and U.S. foreign policy. <https://www.foreignaffairs.com/>

Combating Terrorism Center. The CTC's research program produces path-breaking analysis on the dynamic and evolving terrorist threat. The Center's deep intellectual capital and ability to apply theory to practice creates a unique research model that not only informs strategic counterterrorism thinking but moves the boundaries of academic knowledge. <https://www.ctc.usma.edu/>

Georgetown Journal of International Affairs. Founded to serve as an academic resource for scholars, business leaders, policy makers, and students of international relations alike, cultivating a dialogue accessible to those with all levels of knowledge about foreign affairs and international politics. <http://journal.georgetown.edu/>

Global Firepower (GFP). Provides unique analytical display of data concerning modern military powers. <http://www.globalfirepower.com/>

News Media Analysis

"The media's the most powerful entity on earth. They have the power to make the innocent guilty and to make the guilty innocent, and that's power. Because they control the minds of the masses." Malcolm X

If the headline grabs your attention you will read it, simple as that. Or put another way: If it's new, unusual and sensational it will grab you. Now what does the text convey? Does it influence you, does it make you see things differently, and does it anger you or make you happy? Remember what I said above in the preface, the primary mission of journalists is to inform but the way something is written or spoken will influence the recipient. Journalists will carefully craft their text to carry a consistent message and raise their ratings. Look at the same story from different networks (CNN, FOX News, NBC, CBS, etc.) and see how they have a different viewpoint. Is the network conservative or liberal leaning? Now take a look at the pictures, which usually accompany the text, and see how it affects you. Did you notice the different image angles from the various networks? How much did the image sway you? A picture is worth a thousand words. Dead bodies, starving children, earthquake aftermath, or the results of an air strike on a hospital carry a strong meaning. Who is the intended audience, the military, law enforcement, another country, or just the general public ([News media affects how Muslims are perceived, treated](#))? The point I'm trying to make is that as an OSINT Analyst you have to validate, validate, and validate because you are dealing with open source information that is perceived differently from unlike people.



There is always more information than is presented but the reporter/journalist has only so much time or space in a newspaper so they will only highlight certain areas. In the haste to break a story some will sacrifice accuracy while others will take their time in order to present as much accuracy as possible. So you have to ask the question, what information was intentionally left out? What do other sources say about the same event? Unless the analyst does more research, he/she may miss out on more important facts.

The movie "Vantage Point," I think, points out what I'm trying to convey. In the movie there is an attempt to assassinate the U.S. President while visiting Spain. There are eight witnesses with eight points of view but really only one truth. I think you'll enjoy it and it sends a well-intentioned message to the analyst.

Journalist's Toolbox <http://www.journaliststoolbox.org/>

OSINT Support to Counter Human Trafficking

No, I do not have relatives, friends, or even know of friends of friends that have been a victim/s of human trafficking but it is something that just concerns me. How can one human possibly abuse another human but it happens all the time. I suppose the one subject that really bothers me is the part of human trafficking for carnal servitude, especially of children. The only thing I can do is bring attention to it in the hopes that it may compel others to do be aware that it is happening and look for the indicators as outlined below.

Just like in the OSINT support to the INTs above, this is an area that also has its clues out in the open. It's just a matter of people being able to interpret them for what they are. What may seem like simple everyday activity may actually be a masking for human trafficking. It is estimated that human trafficking (2014 figures) generates approximately \$150 billion a year. More than half of the people are women and girls, and used mostly for commercial sexual exploitation and domestic work; men and boys are found primarily in economic exploitation in agriculture, construction, and mining. According to some estimates, approximately 80% of trafficking involves sexual exploitation, and 19% involves labor exploitation. And don't think this only happens in other countries; Americans are bought and sold or kidnapped or duped into slavery every day. America is not exactly squeaky clean for it has its own human trafficking problems.



Here are 11 facts about human trafficking. <https://www.dosomething.org/us/facts/11-facts-about-human-trafficking>

1. Globally, the average cost of a slave is \$90.
2. Trafficking primarily involves exploitation which comes in many forms, including: forcing victims into prostitution, subjecting victims to slavery or involuntary servitude and compelling victims to commit sex acts for the purpose of creating pornography.

3. According to some estimates, approximately 80% of trafficking involves sexual exploitation, and 19% involves labor exploitation.
4. There are approximately 20 to 30 million slaves in the world today.
5. According to the U.S. State Department, 600,000 to 800,000 people are trafficked across international borders every year, of which 80% are female and half are children.
6. The average age a teen enters the sex trade in the U.S. is 12 to 14-year-old. Many victims are runaway girls who were sexually abused as children.
7. California harbors 3 of the FBI's 13 highest child sex trafficking areas on the nation: Los Angeles, San Francisco and San Diego.
8. The National Human Trafficking Hotline receives more calls from Texas than any other state in the US. 15% of those calls are from the Dallas-Fort Worth area.
9. Between 14,500 and 17,500 people are trafficked into the U.S. each year.
10. Human trafficking is the third largest international crime industry (behind illegal drugs and arms trafficking). It reportedly generates a profit of \$32 billion every year. Of that number, \$15.5 billion is made in industrialized countries.
11. The International Labour Organization estimates that women and girls represent the largest share of forced labor victims with 11.4 million trafficked victims (55%) compared to 9.5 million (45%) men.

Open Source Indicators of Human Trafficking

- Does the person appear disconnected from family, friends, community organizations, or houses of worship?
- Has a child stopped attending school?
- Has the person had a sudden or dramatic change in behavior?
- Is a juvenile engaged in commercial sex acts?
- Is the person disoriented or confused, or showing signs of mental or physical abuse?
- Does the person have bruises in various stages of healing?
- Is the person fearful, timid, or submissive?
- Does the person show signs of having been denied food, water, sleep, or medical care?
- Is the person often in the company of someone to whom he or she defers? Or someone who seems to be in control of the situation, e.g., where they go or who they talk to?
- Does the person appear to be coached on what to say?
- Is the person living in unsuitable conditions?
- Does the person lack personal possessions and appear not to have a stable living situation?
- Does the person have freedom of movement? Can the person freely leave where they live? Are there unreasonable security measures?

site:.org "human trafficking" indicators filetype:pdf
 site:.org "human trafficking" indicators filetype:xls

<https://www.dhs.gov/blue-campaign/indicators-human-trafficking>

https://www.unodc.org/pdf/HT_indicators_E_LOWRES.pdf

<https://polarisproject.org/recognize-signs>

<http://hopeforjustice.org/spot-the-signs/>

<https://traffickingresourcecenter.org/what-human-trafficking/recognizing-signs>



[http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---
declaration/documents/publication/wcms_105023.pdf](http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_105023.pdf)

[http://www.givewaytofreedom.org/Human-Trafficking/human-trafficking-facts-
indicators.php](http://www.givewaytofreedom.org/Human-Trafficking/human-trafficking-facts-indicators.php)

Declassified Sample of Actual OSINT Collection

This page is part of a declassified document that shows why OSINT is so important nowadays. As you can see by the date, 1975, the Army has, I believe, led the way in the open source collection field. I am proud to have been part of that effort. (I know, I'm aging myself.) This particular project was named Sandune and I have no idea how the name came up. I must also add that at this time OSINT had still not been coined; it was simply open source collection.

CONFIDENTIAL

An example of order of battle intelligence obtained through this program was an intelligence report providing the probable organization of the 16th Tank Division. The information was derived from documents which included orders assigning first sergeants of various units to a method of instruction school, pieces of training schedules of various units, and other pieces of correspondence which contained signature blocks of commanders, designations of units, and field postal numbers.

Another example was a unit personnel register which provided both the unit's identification and a list of training required and completed by the various personnel of the unit.

The majority of recovered documents relate to training, the best examples of which are unit weekly training schedules.

In addition to information in the three categories mentioned, nearly all recovered documents provide useful chain of command and biographic data. USMIM has prepared several biographic reports derived from documents recovered from trash dumps, which have provided information on the staff of GSFC headquarters, three army headquarters, three divisional headquarters, and, in the case of one division, echelons down to and including battalion level.

G. (C) PLANS.

1. The signing of the Tri-Mission Indications and Warning Plan on 11 May 1976 and the publication of the first target list amendment later in the year constituted milestones in Tri-Mission history, especially in light of intense interest on the issue of warning times in Europe. Efforts continued throughout 1976 to further refine and develop this plan.

2. Published operation plans for Soviet Troop Rotation coverage and for the Warsaw Pact EW Response to REFORGER provided the basis for highly successful Tri-Mission collection and reporting. Evaluations of IR reporting on these two activities were consistently high and validated the combined approach.

3. Data collection in support of the USMIM Future Study commenced in 1976 with a completion target date in June 1977.

CONFIDENTIAL

F. (C) SPECIAL FEATURE: TRASH AS A SOURCE OF INTELLIGENCE.

While the collection of trash from military trash dumps is not new to USMIM, an intensified effort was mounted in the past year to exploit fully this important source. The overall effort included a heightened appreciation at USMIM for the intelligence value of trash; deliberate targeting of known dumps; an effort to identify other dumps, including coordination with air reconnaissance assets; and partial translation and terse analysis at USMIM to point the analyst in the right direction and highlight the value of recovered material.

Since this improved approach to trash collection was undertaken one year ago, approximately 40 percent of ground intelligence reports now derive from this important source. Among the more significant reports have been:

1. A partial tank firing training SOP for all Soviet armor units, published by the Ministry of Defense in May 1975.
2. A radar operator's log from a Soviet radar site located in north central GDR.
3. A notebook with complete characteristics and operating parameters of the R-118/BM-3 radio station.
4. A technical maintenance manual for the T-62 tank.
5. Firing tables and meteorological correction tables for the M-46 130mm gun and a fire direction center procedures manual.

In analyzing the overall results of the trash collection effort, the information gathered generally falls into three main categories of intelligence: technical, order of battle, and training.

Examples of documents falling into the technical intelligence category are:

1. Charts, such as one depicting and explaining deployment characteristics of the ZSU-23-4 antiaircraft weapon system.
2. A technical manual on the M-46 130mm gun and the M-47 (152mm). In addition, this manual included a chapter on both the 130mm and the 152mm ammunition with detailed drawings of the ammunition, ammunition crates, markings placed on each, ammunition tables, and explanations of both the markings and the tables.
3. Aside from documents of technical intelligence interest, items of equipment such as a chemical protective mask have been recovered and forwarded to the Foreign Science and Technology Center.