

# RISE TO PEACE

RESEARCH PUBLICATION

---

## OSINT Best Practices Manual and Guide

---

**Author**

Amber N.K. Antony, MPS  
Georgetown University

OSINT Practitioner & Counterterrorism Salam Research Fellow

Rise to Peace

**Edited by**  
Etienne Darcas  
Program Lead, Rise to Peace

2025

# Contents

<b>1.</b>	<b>Preface</b>	<b>3</b>
<b>2.</b>	<b>Introduction to OSINT</b>	<b>5</b>
	What is Intelligence?	5
	What is OSINT?	7
<b>3.</b>	<b>Foundations of OSINT and Its Components</b>	<b>8</b>
	The Advantages and Disadvantages of OSINT	8
	The Components of OSINT	8
<b>4.</b>	<b>Practical Examples of Using OSINT</b>	<b>9</b>
	Academic Research	9
	Counterterrorism	10
	Risk and Threat Management	12
<b>5.</b>	<b>Formatting, Tools, and Software</b>	<b>15</b>
	Formatting	15
	Tools and Software	16
<b>6.</b>	<b>Conclusion</b>	<b>24</b>
<b>7.</b>	<b>References</b>	<b>25</b>

## Preface

The mission of Rise to Peace has a very specific focus on counterterrorism and combating extremism, and in remaining true to what our organization focuses on, we are proud to offer a comprehensive look into the technical craft that is intelligence analysis. Open-Source Intelligence (OSINT) contributes in such a significant way to the overall field of intelligence because of its ability to help guide the analyst in their initial efforts of searching for information on a particular person, group, or subject. However, like with all the intelligence collection methods, OSINT is just a small, but vital piece of the puzzle to achieving information that can be synthesized into strategic, operational, or tactical intelligence—the actionability of the intelligence gained is what *really* matters because this will help to define the next steps that are taken.

This manual and guide are written with the best interest of the reader to help enable them to utilize OSINT to its full capability. If you are an analyst, researcher, investigator, or simply new to OSINT altogether, hopefully this will serve as a practical means to help navigate the vastness of what OSINT entails, because at its core that is what it is; information that is not yet intelligence, but is vast, both simple yet complex, and entirely accessible in the modern era if you know *where* and *how* to access it. What truly is critical, though, is having the capability to successfully employ OSINT, and turn open-source information into intelligence, to fulfill any intelligence requirements.

This guidebook will be comprised of five main sections: 1) *An Introduction to OSINT*, 2) *Foundations of OSINT and Its Components*, 3) *Practical Examples of Using OSINT in the Fields of Academic Research, Counterterrorism, and Risk and Threat Management (Extremism/Radicalization)*, 4) *Formatting, Tools, and Software*, and 5) *Conclusion*. There will be references to some key material from the United States Intelligence Community (IC) and the United States Military's Joint Publication, specifically *Joint Publication 2-0*, which serves as a critical document providing the foundation and fundamental principles of intelligence gathering at the highest of levels. Each section within this guidebook was written with the analyst at the forefront, because OSINT results would be questionable if the analyst did not have the appropriate tools or prior understanding of said tools to be able to generate an accurate, concise, and usable report. Basically, the analyst has all the resources at their fingertips, but if certain actions are not taken, or if they do not know how to properly employ these resources, they will run the risk of having a disorganized mixture of some useful intelligence or no usefulness at all, and any environment that relies on that analysis will be severely impeded.

Intelligence analysis is a very special tradecraft that is intricate in what it focuses on, to include the results that are formulated from the analysis, and the causal impact that inevitably occurs from the analysis itself. Therefore, with the digital times that we are living in, learning about a slice of the intelligence analysis methods (i.e., OSINT), will be of great advantage to anyone hoping to gain specialized knowledge that will benefit them in traversing the technological sphere that is modern day, from being able to collect intelligence from a wide-range of publicly available sources, to being able to properly disseminate that intelligence to the consumer.

# Introduction to OSINT

## What is Intelligence?

Before understanding OSINT, it is important to know what exactly intelligence is, and in this case, it is the collection of specific information that has been processed through a cycle to create a final product that is accurate and informative—this intelligence can then drive an operation forward. To get a more in-depth understanding of what intelligence is, according to the Office of the Director of National Intelligence (ODNI) (n.d.):

*Intelligence is information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security (para. 1).*

ODNI's definition is great at providing context to something that can otherwise be left ambiguous, but it is also crucial to explain that in terms of this manual and guide, intelligence, particularly that of OSINT, is not focused solely on the United States nor in benefitting only national security—OSINT can be of great assistance universally to practitioners, scholars, and across a multitude of disciplines. Intelligence, specifically OSINT, is not only utilized in the federal government or for military purposes, but it is also used in law enforcement with criminal intelligence, the legal field to provide additional support to cases, and businesses seeking to gain leverage on competitors, as an example.

Now that we understand what intelligence is, it is equally important to know what intelligence is not. Intelligence is not simply information, nor is it a collection of information that has not been put through the intelligence cycle. First, the intelligence cycle is a series of steps that must be taken after collecting intelligence. It is comprised of the following six steps according to Joint Publication 2.0 as observed in the U.S. Naval War College Library (2025):

1. *Requirements, Planning, and Direction*
2. *Collection of Intelligence*
3. *Processing Intelligence*
4. *Analysis and Production of Intelligence*
5. *Dissemination of Intelligence*
6. *Feedback*

Requirements, planning, and direction, the **first step** in the intelligence cycle—this is the very foundation of which intelligence collection, whichever gathering method of collection is chosen, will rely upon. To provide a little bit of context, requirements are a set of very fine-tuned questions, topics/goals, issues, and tasks pertaining to the intelligence that is desired to be collected. An intelligence requirement really sets the stage for the analyst to know what and where exactly they should be focusing their efforts on (i.e., what takes priority). For example, suppose the focus was on political violence and extremism, and the analyst was tasked by a decision maker with trying to gain intelligence on this matter, the more general intelligence question could be, "*what location are these*

*violent trends most taking place?"* and the specific intelligence question could then be, "*what can be observed to be the driving force behind these violent trends (e.g., social media groups spreading propaganda)?"*. The planning and direction, once these intelligence requirements are established, can then be determined (i.e., what will be needed to collect the intelligence, how will it be collected, and who is going to be responsible for the intelligence collected).

The **second step**, collection of intelligence, is basically an entirely separate set of steps where a collection plan is formed and executed to collect said intelligence. One of the most critical components of this step, however, is that this is where the actual collection of intelligence is going to take place through one of the intelligence collection methods, which are officially Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signals Intelligence (MASINT), and Open-Source Intelligence (OSINT). This collection plan will generally consist of the already proposed intelligence requirements, establishing the resources necessary and identifying any foreseen hindrances to the collection plan, setting priorities to keep things on track, following tasks based on the requirements and the priorities set forth, and continuously monitoring and evaluating the progress of the collection method. If the overall collection plan needs to be revised now would be the time to do that before continuing to advance in collection.

The **third step** is to process intelligence, and this is where all the unprocessed information that has been collected will undergo a form of evaluation; this is a vital step no matter what collection method was employed. This evaluation consists of determining what is relevant, what is accurate and reliable, what is not usable, and what needs to be deciphered or translated (in cases of foreign language, encryption/coding, etc.).

The **fourth step** is analysis and production of intelligence. This is when the analyst will take the processed intelligence and begin to make necessary connections (e.g., connecting the dots, so to speak) and applying other forms of gained knowledge that they might have to be able to produce a final product. The **fifth step** is dissemination of intelligence and this when the completed work is disseminated to the client; the way it is disseminated relies on who is receiving it, when it is needed, and what form it is being presented in (e.g., written or verbal). Lastly, the **sixth step** is feedback. This is an opportunity to receive constructive criticism on the intelligence report/briefing regarding the intelligence collected and whether additional steps need to be taken.

## What is OSINT?

Now that the brief basics of what intelligence is has been explained, we can move forward to the main purpose of *what OSINT is* and *what it is not*.

First, OSINT is one of the intelligence collection methods that focuses on collecting intelligence through publicly available sources. The official definition, as explained by the United States Intelligence Community (n.d.) states, "OSINT is intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps" (p. 1). It is utilizing the intelligence cycle process to gain intelligence through social media (e.g.,

social media platforms, chatrooms/groups, etc.), books and media, search engines, grey literature, other academic publications, geolocation/maps/imagery, and though not necessarily public, the dark web (i.e., a piece of the internet that consists of web pages otherwise inaccessible without the proper software that is, however, legal and publicly available). OSINT has come a long way from what it once was, and that is partly one of the misconceptions about it in the modern day is that OSINT is new, when it is actually not a new concept at all. It has been in use by the military dating back to at least World War II, but it has developed since then into the OSINT term, and then advanced to meet the demands of the world that we now live in—OSINT is continued to be in use by the military, IC, law enforcement, the criminal justice system, law firms, cybersecurity professionals, businesses, and many other professions/professionals both in the private and public sectors.

Second, as much as it is important to know what OSINT is, it is just as imperative to know what OSINT is not. OSINT is not simply putting a name into a search engine and collecting any of the raw data that is populated and calling it "intelligence." OSINT is not using a computer-generated interactive data report from one of the many websites that offer these services and calling it "intelligence" or "OSINT." And, ultimately, OSINT is not conducting a quick social media search and expecting that to produce all of the intelligence that is needed. These are all useful tools that can be used and great sources that could produce information that could potentially produce intelligence, but to claim that this is all that OSINT is would be a mockery of the specialized craft, and a disservice to the skills that OSINT requires someone to possess. But, most importantly, relying on this type of information that has not been fully processed can have serious consequences. For example, an academic scholar conducting OSINT for a project and relying on information that has not been processed for credibility or accuracy, could produce a project that is unreliable and factually wrong, thus spreading further misinformation. Or, for example, a crime analyst tasked with building a case on gang violence in a particular area, and utilizing OSINT to further their profiles on suspected members without fully processing the data, runs the risk of hindering the entire investigation if that information is wrong or if its missing something vital. The same could be said for counterterrorism or investigations, but in some instances the lack of proper OSINT techniques is very black and white with no room for error, and if not properly employed, could be one of the factors in getting someone killed, wrongfully arrested, ruin a case, and many other adverse outcomes.

## Foundations of OSINT and Its Components

### The Advantages and Disadvantages of OSINT

OSINT can be incredibly advantageous in terms of being able to find information about an individual, organization, or subject, which can include full names, date of birth, location/addresses, organizational ideology, members of an organization, associated photos of said individuals, history, and so much more depending on what the purpose of the OSINT is—building a case or investigation, writing a historical report of events, creating profiles on people and groups, are just some of the things that benefit from this type of intelligence collection method. However, as with most things, there are always going to be disadvantages. In this case, OSINT does have a few known disadvantages, such as not being able to provide enough intelligence without the use of another intelligence collection method to provide more context, improper handling and analysis, and confusion on the part of the analyst or the client regarding not understanding OSINT fully and how it is conducted. Ultimately, the best way to combat any confusion on what to do and what not to do, to work within the advantages and disadvantages, is to apply the intelligence cycle. To further expand on this, however, and how it is applicable when using any one of the intelligence collection methods, Builta and Heller stated the following in *Studies in Intelligence Vol. 55, No. 3 (2011)*:

*Whether this "force" is a policy maker, law enforcement official, collector, or military operator, analysts must be acutely aware of the decision cycles and intelligence requirements of that force. Put another way, analysts must simply know for what purpose they are producing a given product. Not every product can or should translate into a direct operational decision (p. 8).*

### The Components of OSINT

It is important to remember that OSINT at its very foundation, along with all its various components, is simply a data-oriented tool to exploit public information on anyone or anything for the purpose of gaining intelligence. Therefore, the analyst themselves needs to also have a good working knowledge of how to source this data using the widely available tools or have the ability to learn how to use these tools, which can be varied in its simplicity or complexity. Knowledge is paramount when it comes to overall intelligence analysis, and that applies to OSINT as well; the more knowledge the individual has who is conducting OSINT will have a greater chance at success because they can apply the knowledge to a variety of areas. Publicly available resources to use as the basis for collection, data mining and categorization, understanding the purpose of intelligence and the intelligence cycle (i.e., what it consists of and how it is applied), critical thinking, and also being able to have some type of/variety of specialized skills to efficiently collect intelligence, such as strong research skills, ability to speak/read a foreign language (helpful when relevant), full understanding of the subject matter (e.g., whatever subject it might be), or technical capabilities (e.g., cybersecurity). Depending on the purpose of the OSINT, some or all components are critical and necessary to achieve the desired results.

## Practical Examples of Using OSINT

in the Fields of Academic Research, Counterterrorism, and Risk and Threat Management (Extremism/Radicalization)

### Academic Research

In academic research, OSINT can be extremely beneficial when having to complete specific projects or reports because it allows the researcher to determine what they are trying to complete, how they plan to go about completing the specific tasks (e.g., establishing a timeframe), what publicly available sources can they use to complete their research, and ultimately how they are going to disseminate the final product and to who the receiver will be. For example, if a researcher was given an assignment to work in a team setting on a collaborative project, and the topic was on major intelligence failures that have happened throughout history, with a due date of four months, a collection method of OSINT can be chosen, and the intelligence cycle can be applied. As an example, this type of scenario could look like this when choosing the intelligence collection method (i.e., OSINT) and applying the intelligence cycle:

**Step 1:** The *requirements, planning, and direction* would look slightly different for this scenario because it is of an academic nature, but at its core, can be applied to anything where there is a need to define a course of action and how to plan around that to keep on track. The requirements could be identified by reviewing what the professor, for example, is requesting from you and your team; this is what the entire project will be adherent to. The planning will take into consideration the timeframe, any material that has been given (e.g., the syllabus), what resources are needed to complete the project, and how OSINT can be applied to collecting information on major intelligence failures throughout history. Each team member could be assigned a specific thing/topic to search for. And in this instance, the direction of collecting intelligence will fall on the team members, as well as a clear direction on where to search, but the final direction would come from the team leader on behalf of the professor.

**Step 2:** The *collection of intelligence* will be OSINT. The type of sources that could be used is a physical library to read books on history, national security, politics, and other intelligence tradecraft material. In addition to this, online publications and reports could be read, as well as watching videos or documentaries on major intelligence failures throughout history. Publicly available statements from government officials and military leaders could also be collected. During this step, keeping on track to meet the demands of a four-month timeframe is critical, therefore using resources properly and assigning key tasks divided throughout the team is most important. As an example, one team member could be assigned to collect information from in-person reading material at a library, and another could be assigned to watch specific material and collect from that source. While the team leader could be responsible for compiling and verifying the information for evaluation.

**Step 3:** This is where *processing of intelligence* will occur. An evaluation needs to be conducted on the information collected and to determine its relevancy and accuracy, along with what else needs to be collected or revised. The positive side to an assignment where its collecting something on intelligence failures, or something of a more research-based academic topic, is that the information can be pulled from already verified sources (e.g., an official report or academic publication), therefore it can make the entire process easier because it is not just information from an unverified social media post, as an example. Dates, topic relevancy, authors, fact-checking official statements, checking for cognitive biases, are all part of this step.

**Step 4:** *Analysis and production of intelligence* take place during this step. For example, the team would need to take the intelligence that they have compiled and determine where each piece of intelligence can be applied to demonstrate the failures of intelligence that have happened throughout history. This could include sectioning off each piece of intelligence so that it fits in the overall construction of the product, making connections to the intelligence failures in history and how it was prominent failures, the effects and outcomes of these failures, and so forth.

**Step 5:** This step is when *dissemination of intelligence* happens. At this point, the four-month timeframe is up, and the final product is due to the decision maker (i.e., the professor or whoever is requesting the project to be delivered to them). During the very beginning of step 1, it would have already been determined how the final product will be delivered, for example, it could be delivered in a verbal brief or in a written report, or both, whatever it might be, but in this step this is when that takes place.

**Step 6:** Lastly, this is the step where *feedback* occurs. This could include the overall grade that is given on the final product, criticism or praise from the professor, and even individual statements from the team members to the team leader, and vice versa, regarding how the team functioned, how well the team worked to collect OSINT, and whether any methods and techniques in the future need to be revised to create a better final product.

## Counterterrorism

OSINT contributes significantly to counterterrorism efforts across the public and private sectors. In fact, one of the benefits of modernity and widespread use of the internet in society today is that even in faraway places where in the past it was incredibly difficult to gain intelligence, it is now more accessible. Emerging terrorist organizations, long-standing terrorist organizations, those that are supportive of the specific organizations' ideology, impending attacks in the present and potential attacks in the future, and really a long list of helpful intelligence that can assist in counterterrorism efforts are made possible through OSINT. For this example, an individual could be assigned to collect OSINT for a terrorist database on a known terrorist organization for the purpose of learning more about the organization in terms of what their goals are, what ideology they follow, what their history is, and anything else that can be of use.

**Step 1:** The *requirements, planning, and direction* for this scenario would be, first, focused on knowing the requirements, which is obtaining intelligence on a known terrorist organization for the

purpose of adding them and all of their information to a database. The planning aspect of this would be to know what timeframe the analyst has to complete this task and what areas of the internet would need to be searched to obtain this intelligence; once these are known, the planning can take place on how to accomplish these tasks. While the direction of this intelligence collection will be handled solely by the analyst, but again, also on behalf of the database holder/organization.

**Step 2:** The *collection of intelligence* is OSINT. For this type of scenario, this is a great intelligence collection method because the final goal is to collect intelligence on a known terrorist organization, but incremental goals include learning more about this terrorist organization and all of their various components (e.g., how they began, ideology, recruitment methods, etc.). The analyst could also compile a list of sources to check for this type of information, such as the terrorist organizations list from the CIA's World Factbook, and determine if the terrorist organization is listed on there (which is most likely because the advantage of this scenario is that it is already a *known* organization, and not a suspected one), and if so, find an additional source that has information, such as UMass Lowell's Center for Terrorism and Security Studies research section/resources list to see if they have anything on the terrorist organization as well that could be used. If the analyst is working alone in this scenario as it would appear to be, then they would need to work within the timeframe by setting specific goals that would need to be accomplished to stay on track and to review and/or revise accordingly.

**Step 3:** The *processing of intelligence* occurs here and could include going through the list of various sources and verifying information, determining what is relevant to the database, and really focusing on dates, facts, and names; this should be available because, as stated in the previous paragraph, the terrorist organization is known and that is an advantage in this instance when collecting OSINT because the analyst is not working with all unknown variables.

**Step 4:** The *analysis and production of intelligence* take place during this step. Since the OSINT is for a database, the analysis aspect will look slightly different because instead of producing intelligence to, for example, directly influence an intelligence operation or policy, it is for the purpose of research, but that research is also in the benefit of counterterrorism efforts. The analysis could be to take the obtained OSINT on the terrorist organization and formulate how it fits into the database, link the known facts from one source to another source to form a whole picture as to who the terrorist organization is and what they have done so far, and really focus on producing a full product that would not only enhance the database, but also ensure that whoever is going to read about the terrorist organization will have a full understanding, as much as is available, on it.

**Step 5:** The *dissemination of intelligence* occurs in this step. The final product will most likely be delivered in some form of a written report or in conjunction with a verbal brief and could potentially be periodic if the terrorist organization continues to grow/expand in the future—this is one of those areas that should be discussed with the client to determine next steps. The final product is going to include everything on the known terrorist organization and will be disseminated as such—history, location(s), ideology, affiliations, known members, and methodologies and tactics.

**Step 6:** The *feedback* will occur in this step. This is where the client is going to most likely discuss whether they received the OSINT on the known terrorist organization to their liking or if they need additional OSINT to be conducted for the database.

## Risk and Threat Management: Extremism/Radicalization

Another type of area where OSINT can be beneficial is when conducting risk and threat management, specifically when the content is regarding extremism and radicalization. Many incidents that have occurred in the past and in recent times where there was an element of extremism/radicalization that has been observed in social media and online postings went, unfortunately, unknown or were dismissed until post-incident—this has ranged from hateful rhetoric to actual cryptic social media postings of the desire to commit acts of violence. This is also not just applicable to, for example, terrorism or right-wing/left-wing extremism, but also cases of sadism/sexual violence. Therefore, it is extremely important for there to be this type of awareness when it comes to social media, and from a law enforcement or other government agency standpoint, to understand how OSINT and social media play critical roles in modern-day extremism/radicalization. For this scenario, imagine working in a consultant capacity, but assigned to a law enforcement agency with the task of monitoring and reporting on any content on social media that would appear to pose a significant threat to the community.

**Step 1:** The *requirements, planning, and direction* for this scenario would be centered on knowing the requirement of, for example, gathering flagged content that poses a risk to the general public in the area that the particular law enforcement agency has jurisdiction, while it could also be taking that data and determining how can these risks to the general public be mitigated to prevent future acts of violence from being carried out. In this type of scenario where it can appear to be simple on the surface of monitoring and reporting on any content on social media that appears to pose a threat to the community, it could also be more complex because many postings could appear suspicious or a threat, so it is important to remain very certain and clear of what the intelligence requirements are to be able to work with content that could be voluminous—this is where the planning aspect is critical. The consultant should create a plan that works within the scope of what the law enforcement agency wants and creates a plan that considers the resources made available to them, such as other personnel and monitoring equipment. The direction of collecting OSINT comes from the law enforcement agency, but the person responsible for this collection is the consultant.

**Step 2:** The *collection of intelligence* is OSINT. However, given the nature of what intelligence needs to be collected, potentially at some point another intelligence collection method could be utilized, such as Signals Intelligence/Communications Intelligence (SIGINT/COMINT). The consultant could make note of this at some point in their final product recommendations section to the client. OSINT is a great method at this point, regardless of the other intelligence collection methods, because of what it could potentially uncover, such as credible threats or actual planned acts of violence. This can be uncovered by not only being able to actively monitor flagged social media accounts, but it also could show user data that is vital, such as a full name, date of birth, location, known associates, personal interests of the subject, and details that would allow law

enforcement, if necessary, to prevent these violent acts from coming into fruition. Because social media is so prevalent, this is where that becomes a benefit to the consultant in terms of monitoring; they could have a set of social media platforms that are routinely monitored (the consultant could also make use of monitoring software) and check for specific terms that are associated with these types of extremism/radicalization to uncover profiles of people spreading propaganda or those who are making statements of wanting to commit acts of violence (e.g., a person could state when they plan to do this or how they plan to do it). Certain chat rooms or chat threads could also be actively monitored, if possible. This is really where the consultant can assist law enforcement in taking proactive measures based on the collection of OSINT rather than simply remaining to be reactive post-incident.

**Step 3:** The *processing of intelligence* is going to consist of eliminating all unnecessary OSINT that has been deemed not a threat, so it comes down to being able to take the OSINT that was gathered and effectively sort through it. There are a few factors to consider when doing this, such as where the information was retrieved (e.g., the social media platform and where within that social media platform was it posted, such as in an image or in a video or a caption with details), when was it posted, who was it posted by, and what factors of the post makes it credible enough to look more into as being an actual threat to the community. Basically, the consultant in this situation would probably have to remember during this step that even though some posts could be concerning, not everything that is concerning poses a threat to society.

**Step 4:** The *analysis and production of intelligence* will allow the consultant to take the OSINT (i.e., social media posts) and analyze it for further understanding of the threat that it poses. This could include taking one piece of a social media post from a user who has posted similar content on other social media platforms and compiling that together with additional intelligence, such as flagged content on their profile, public online groups they might belong to, comments that they have left on other accounts, etc., and linking all of these things together to depict how this person could be a credible threat. The consultant could also investigate ideology that the person posting on social media could be following, such as does it appear they have a strong belief in white supremacy or jihadism or are they posting frequently about idolizing people who have committed horrible atrocities (e.g., mass shooters). The final product would need to include all of this processed and analyzed intelligence, but to also highlight what could be actual imminent threats and why it has been labeled as such (i.e., what makes it a priority).

**Step 5:** The *dissemination of intelligence* will be to the law enforcement agency and delivered by the consultant in, most likely, a detailed report and a detailed verbal briefing as to the final product. Due to the nature of this focusing on monitoring and reporting on any social media that appears to pose a risk to society, this dissemination of intelligence could be one of many, as this type of intelligence gathering could be continuous. It is incredibly important for the consultant during this step to deliver the final product with the intelligence that takes priority, and to ensure that it is known why it takes priority, in the effort that the law enforcement agency has the intelligence needed to take some form of action.

**Step 6:** The *feedback* during this final step can be of great benefit to the consultant because it allows the law enforcement agency to provide the necessary comments of what was done correctly, ineffectively, or what they might need in the future regarding this same type of intelligence collection. Regardless of any of this, it provides the consultant with a good idea of what they can do better the next time, and being able to produce effective intelligence is really what will always matter.

## Formatting, Tools, and Software

Knowing how to format OSINT results, along with what tools and software to use during the collection phase, is just as important as knowing the basics of how to conduct OSINT, if not even more so. The reason it is so vital is because the product itself needs to be presented in a manner that is received well by the client; it needs to be easily digestible in terms of how the information is presented, but it also needs to be able to paint a full and accurate picture, so to speak. The right formatting and the right tools will always serve an analyst well when it comes time to deliver the intelligence product.

### Formatting

When giving a verbal brief or a written brief, bottom line up front (BLUF) is a good communication method because it immediately states the issue or explains what the subject matter is, as well as any important information—remember that you want the consumer to immediately know the main facts and the key results. Below I have included an example of the format that I have used many times when writing an intelligence report or delivering an intelligence brief verbally (the format can be applied to any subject, person, or organization):

#### **Example of OSINT Report Format for Final Product**

1. Understanding the intelligence requirements/re-stating it in the report
2. Summary of report and findings written in BLUF
3. Identifying numbers (i.e., Social Security Number (SSN), licenses, passport, etc.) if this involves an individual not solely an organization, but it can also be applied to an organization (i.e., known members/suspected members, physical location of members, etc.)
4. General personal data (i.e., full name, age, date of birth, address, etc.)
5. Family information or known associates/affiliates
6. Legal information/criminal history/civil history
7. Education information, training information, or military history
8. Work-related data, including additional places of work or additional businesses that the individual is affiliated with or owns
9. Address history
10. Properties, past, and present/full property transaction history
11. Vehicles; all relevant vehicles
12. Social media presence and listing of all known accounts
13. Recommendations for the client regarding what could be done with the intelligence
14. Supplementary material, such as photographs of person of interest, properties, vehicles, etc., anything that is verified and relevant

## Tools and Software

There is a plethora of tools and software that can be used to conduct OSINT, but it is also important to know how to use each one and to know what the desired results are. Of course, what is available depends on the country and what is publicly accessible. For example, collecting OSINT in the United States could be easier than collecting OSINT in Russia because in the United States it is a Liberal Democratic nation (i.e., free media, open social media, things of this nature), while in Russia and similar countries there are more restrictions over publicly accessible information. Therefore, the OSINT, while still available, could be limited or obscured to be an inaccurate representation of what the actual intelligence represents; it is important to be aware that this can happen in several situations, which is why proper analysis is crucial. Below are lists of some of the main tools and software that can be useful; it is not by any means a complete list, but it does cover some of the main tools, social media platforms, and very specific software. The results can vary depending on if profiles are public or private, or if the subject even has a social media presence, but then there are always other avenues to search as well, such as academic publications, mentions in the news, mentions on the social media platforms of known associates, etc.; using critical thinking skills will come in great use in knowing how to expand a search for someone or something even when it initially appears that there is nothing to be found.

### **Academic Tools (Counterterrorism/Militant/Extremism Focused)**

These academic tools can be used for research purposes (as explained in scenario 1 on page 9) or in any instance when there needs to be OSINT collected on subject matter that could be found in a scholarly publication or grey literature; it is always a good practice to check these sources just in case it leads to valuable information. In addition to this, regardless of being able to obtain OSINT, these academic tools also help broaden the knowledge of the user (e.g., when trying to understand counterterrorism issues or learn about a particular terrorist organization), and can assist them during the intelligence cycle, if applicable. For example, an analyst who is tasked with compiling a report on the effectiveness of the criminal justice system in the United States could access the NIJ and locate the NIJ Journal Issue 284: Justice Systems in the dropdown menu, download the full issue, and read through the various articles on the prison system, recidivism rates, sentencing reforms, and other similar topics. The benefit of the NIJ in this example is that it helps the analyst to gain valuable intelligence that could be of use to their report, and whether the analyst decides to use this intelligence is irrelevant because it is still from a credible source (i.e., NIJ through the Department of Justice (DOJ)), from credible and trusted authors (i.e., NIJ adheres to a strict scientific and research integrity policy), and can help the analyst to learn more about effective/ineffective practices of the criminal justice system—all of this bolsters the analyst's ability to produce a better final product. This is why knowing what tools to use for OSINT is so important because the analyst needs reliable information to eventually turn into intelligence and it is difficult, though not impossible, to do that from sources that are unreliable and contain information that is already questionable or unvetted (e.g., retrieving hate crime statistics from a social media post from an unofficial account with no references listed as to where the hate crime statistics originated from is not as beneficial as retrieving these hate crime statistics from the FBI's Uniform Crime Reporting system which is both official and already vetted). And the NIJ is just one of the examples of a good tool

to use, but there are many others as well, depending on the purpose of the OSINT.

#### *A List of Academic Tools*

- A Resources List for Terrorism Research: Journals, Websites, Bibliographies from JSTOR (2018 Edition) - <https://www.jstor.org>
- Perspectives on Terrorism, Peer-Reviewed Academic Journal from Leiden University (Netherlands) and University of St Andrews (Scotland) - <https://pt.icct.nl>
- International Centre for Counter-Terrorism - <https://icct.nl>
- SpringerLink - <https://link.springer.com>
- ResearchGate - <https://www.researchgate.net>
- Crime Statistics in the United States from the Crime/Law Enforcement Stats (Uniform Crime Reporting Program) at the Federal Bureau of Investigation (FBI) - <https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/ucr>
- National Institute of Justice (NIJ) - <https://nij.ojp.gov/library/nij-journal>

### **Business & Organization Tools**

Business and organization tools are used predominantly to gain OSINT on the background of a specific business or organization. What this means is that every entity has details that are important to the understanding of that business or organization, such as the owner(s), status of whether it is active or inactive, the address of where the entity was initially registered, etc. This type of information holds a significant amount of value in instances when the analyst is tasked with conducting a background investigation on a person, when conducting business intelligence and the client is requesting information on either a potential partner or competitor, or when using this information as an additional source of trying to gain more insight into an entity. An example of this could be when the analyst is looking into the validity of an organization to determine if it is a legitimate organization or not, in addition to also trying to learn about all aspects of this organization. OpenCorporates is a small example of a good tool to use because it is universally available and if the analyst has the name of the entity or the name of the suspected business owner, regardless of where the entity or owner is located in the world, they can conduct an advanced search on it—depending on the entity and what is publicly available within this search might yield more results than another search, but the basic information will still be available. For example, an analyst could be assigned with collecting OSINT on "Company A" and the analyst knows the name of the company and the location of where the company is located but does not know anything else. The analyst could use OpenCorporates, place the name of the company in the search bar, scroll through the list that will populate with the company name, and the analyst can go through the list until they find "Company A." The type of data that can be available would be the company number, status, incorporation date, company type, jurisdiction (i.e., state/country), agent name (i.e., registered owner), agent address, associated officers, recent business filings (e.g., Articles of Organization), and the company address.

#### *A List of Business & Organization Tools*

- U.S. Securities and Exchange Commission (SEC) to search for electronic filings of a company/person - <https://www.sec.gov/edgar/search>
- OpenCorporates to gather company profile data and to check the legitimacy of a business (i.e., the business agents, the location and the address of the business, etc.). This is a legitimate source and has a B Corp certification - <https://opencorporates.com>
- Business Annual Reports/Foreign Registries - <https://www.gov.uk/government/publications/overseas-registries/overseas-registries>
- Value Added Tax Identification Number (VAT) European Commission Search - [https://ec.europa.eu/taxation\\_customs/vies/#/vat-validation](https://ec.europa.eu/taxation_customs/vies/#/vat-validation)
- LittleSis is a research platform designed for transparency and accountability of corporate and government entities, which also shows maps, lists, and tags of these entities and how they are connected (e.g., Wall Street connections or political figures and their investments). LittleSis, however, is user-based and people have the option to create data visuals, therefore discretion regarding validity and accuracy should always be used - <https://littlesis.org/home>

### **Criminal History & Legal Tools**

It is always a good practice when conducting OSINT on an individual to search for their criminal history, and if available, any civil proceedings as well. There are various reasons as to why an individual would want to know this type of information about a person and it could be applicable in several situations, such as when conducting a background investigation on a person for hiring purposes or when conducting a civil or criminal investigation—it is vital information that can help to guide a person in how they handle the subject or how they handle the case. There are numerous criminal history and legal tools that are available to collect OSINT, but it also depends on the state and the country. For example, in the United States, particularly in Hawaii, the access to this information is greater than in Washington, D.C. In Hawaii, if one were to access the judicial system, specifically the Judiciary Information Management System (JIMS), they would be able to conduct a party search, vehicle search, case search, review any upcoming court hearings, and view/purchase documents. All of this information is publicly accessible with the person conducting this search only needing the subject's name, license plate, or case number; if the subject has traffic infractions or a criminal/civil court case, the information will be available. However, in Washington, D.C., if a person wanted to have access to the same type of information, it is available to the public, but you would have to go through the proper channels (i.e., Metropolitan Police Department) to be able to retrieve the information and you would need to have a qualifying reason to access the information (e.g., employment).

#### *A List of Criminal History & Legal Tools*

- National Sex Offender Public Website (NSOPW) in the United States - <https://www.nsopw.gov>
- State Records in the United States for Criminal and Civil Purposes - <https://staterecords.org/criminal.php>
- European Criminal Records Information Services (ECRIS), European criminal background check on EU citizens, established by the European Commission -

<https://ecris.eu/eu-criminal-record-check>

- Within each state in the United States there are specific websites that you can utilize to gain intelligence on an individual if you have simply their full name or other key information (e.g., license plate); you just need to know where to look. This varies, however, between different states and countries, as to what is publicly available—some states are far more restrictive than others.

## **Cybersecurity & Dark Web/Deep Web Tools**

Cybersecurity, dark web, and deep web tools can be useful if the situation arises, but traversing the types of environments that would require these tools does need a good level of technical understanding on the part of the analyst, as well as some technical understanding on the part of the client, in order to request something, for example, involving the dark web (which by nature is not public). A good question that some might ask is how cybersecurity or the dark web/deep web relates to OSINT, and how can OSINT be produced. First, cybersecurity relies on OSINT in numerous ways, such as an analyst needing to monitor specific activity relating to potential cyber-attacks, threat mitigation, obtaining data collection to further prevent and strengthen any gaps in security, checking for open ports, to name a few. Second, the dark web and deep web are not public and can be viewed as parts of the internet that to varying degrees are hidden, but with the right tools and knowledge, are accessible. The deep web, however, unlike the dark web, can be accessed using specific search engines that are not atypically used (i.e., Google, Bing, Yahoo, etc., will not be used). The reason for this is that a normal search engine, for example Google, is optimized to present results from web pages based on the user typing in a keyword or a search phrase and due to indexing results will populate. To put it simply, a web index is a collection of stored web pages that are accessible on any one of the browsers, but the deep web is not indexed. The best analogy to apply when trying to understand this is to think of a filing cabinet that is open and filled with many files that a person can grab at any point in time to view, and then to think of a filing cabinet that contains the same files, or additional ones, but is locked and can only be opened with a key; that is what the deep web is like. The dark web, on the other hand, is part of the internet, but is hidden and requires specific software, like Tor Browser, to access it; this browser can be freely downloaded. The caveat to that is proper network configuration is needed to access the content once Tor is downloaded; it is not as simple as typing in a search term on Google and having results appear. That is the intrigue and one of the reasons why the dark web is used frequently by those who could be conducting nefarious business/acts. The OSINT that can be gathered, however, from the dark web or the deep web can be very valuable, as it could pertain to more in-depth research publications no longer available on a website or information on specific businesses that has since become outdated but is still of some relevance (deep web) or being able to access underground networks with the purpose of collecting criminal intelligence, such as for law enforcement purposes (dark web).

### *A List of Cybersecurity & Dark Web/Deep Web Tools*

- Tor Browser to install and access the dark web. It is a *legal* browser in most countries, but the content that can be accessed on the dark web can be *illegal*. Using discretion with something like this is critical, as well as knowing how to use it - <https://www.torproject.org/download>

- Internet Archive - <https://archive.org>

## **Social Media Tools**

Social media can provide a significant amount of OSINT in terms of photos, posts/written content (e.g., lengthy captions that contain a variety of details), and insight into a person or an organization. There are many platforms that can contain different details and depending on the person, they might post more on one platform versus another, or they might feel comfortable sharing details on one platform versus another—this is why it is important for the analyst to check each social media platform and to try to understand why a person would utilize a particular platform in the first place (e.g., some people might post photos on Instagram with little to no details in the caption, but post a variety of information on their Facebook about themselves and their life that they otherwise would not post elsewhere). In addition to this, some platforms, like Discord, on the surface would appear to be a communication tool for gamers or communities that share the same interests, where users also have the option to stream (i.e., playing a game live), but because Discord is a communication tool, they also have private invite-only chat groups (i.e., servers); this is important to know for someone conducting OSINT because they know that if they had to use something like Discord to collect OSINT, it could be more limited or difficult to collect information from. A good example of why an analyst would be tasked with having to search through social media is if they are assigned to an investigation focusing on a missing person. On the surface someone might wonder what benefit is it to the analyst to look into these platforms and what can it provide in terms of locating the missing person. An analyst could uncover through social media details about the missing person or details about the social circle/acquaintances that could be of great use to those working in the field trying to find the missing person; details can include the last known location of the person, information about relationships/friendships, and somewhat of a personal look into the digital life of the missing person that could point the analyst/investigators in the right direction of where they are or what could have happened to them. Another example could be if an analyst was tasked with looking into the digital recruitment methods of a known terrorist organization for the purpose of uncovering how they recruit on social media (e.g., what type of methods they use to appeal to the public/potential members) and where they are recruiting from (e.g., the platform that they seem to use the most). The analyst can search through and monitor these social media platforms, track specific hashtags that are associated with the terrorist group that could then be traced to member profiles, sympathizers/supporter accounts, and groups, determine what social media platform seems to have the most activity, and based on all of the information gathered, this could lead to understanding more of what the terrorist organization focuses on to draw people in—this is a tactic that ISIS was carrying out for many years and they were known for their heavy use of social media to recruit members.

### *A List of Social Media Tools*

- Facebook - <https://www.facebook.com>
- Instagram - <https://www.instagram.com>
- Instagram Threads - <https://www.threads.com>
- X (FKA Twitter) - <https://x.com>

- Snapchat - <https://www.snapchat.com>
- TikTok - <https://www.tiktok.com>
- LinkedIn - <https://www.linkedin.com>
- Tumblr - <https://www.tumblr.com>
- YouTube - <https://www.youtube.com>
- Pinterest - <https://www.pinterest.com>
- Reddit - <https://www.reddit.com>
- Discord - <https://discord.com>
- Vkontakte (VK) (this is a Russian social media/networking site very similar to Facebook and can be useful if, for example, a background check is being conducted on an individual who is Russian) - <https://vk.com>

## **Software/Databases**

OSINT also relies on access to software and databases, which can broaden the amount of information available to the analyst; it is always a good practice to be aware of the many software and databases that exist if the need to use one presents itself. However, it should be noted that some of these tools are not readily available and do require payment, credentials, or both. For example, LexisNexis is a global data analytics company that has many products available to customers across the legal fields, government, law enforcement, private sector, etc., and one of the main services that they provide is a comprehensive public records search. Although to access the public records search, a person in the private sector would need to contact LexisNexis to request access to the public records search and discuss costs, but this can be an important tool to use, especially during a background investigation. Then there are very specific databases that are free and readily available, such as the Mapping Militants Project (MMP). MMP, for example, has over 133 full profiles on militant organizations; if an analyst was conducting OSINT on terrorist/militant organizations that are active or inactive and needed to compile information on, Al-Shabaab, for example, they would be able to find a full profile on them with a date of their first recorded activity, date of first attack, an overview, narrative, organizational structure, known strategies, and list of attacks.

### *A List of Software/Databases*

- Global Terrorism Database (GTD) from the University of Maryland National Consortium for the Study of Terrorism and the Responses to Terrorism via Department of Homeland Security. This is a comprehensive and downloadable database on various terrorist organizations - <https://www.start.umd.edu/gtd-download>
- Terrorist Organizations, The World Factbook at the Central Intelligence Agency (CIA) - <https://www.cia.gov/the-world-factbook/references/terrorist-organizations>
- Foreign Terrorist Organizations list at U.S. Department of State - <https://www.state.gov/foreign-terrorist-organizations>
- The Mapping Militants Project (MMP) is managed by Dr. Kaitlyn Robinson of Rice University and Dr. Martha Crenshaw of Stanford University. This is a comprehensive database of militant

organizations in specific locations throughout the world - <https://mappingmilitants.org>

- idiDATA (IDI), which has three main components: 1) idiCORE, 2) idiDATA, and 3) idiTRACE. This is beneficial because it is a comprehensive and fast automated generated report that focuses on the subject's history, background, and finances - <https://www.ididata.com>
- LexisNexis is a proprietary criminal records database search that includes state criminal records, state sex offender registries. Prison, parole, and release records from state departments of corrections, administrative offices of courts, and other state agencies. This is also internationally available to those who qualify - <https://www.lexisnexis.com>
- ShadowDragon is an OSINT software focusing on link analysis, monitoring, and collection - <https://shadowdragon.io>

### **Misc.**

These are some of the miscellaneous tools that are also beneficial to overall OSINT, but one that stands out is the OSINT Framework, which is public, free to use, and was created by an OSINT practitioner, Justin Nordine. The OSINT Framework is a compilation of the various tools and software that can be used to conduct OSINT displayed in a user-friendly diagram that allows a person to click on one of the many items, which will then populate with any related tools to that specific item. For example, selecting "*language translation*" will populate with options for text, pictures, videos, and analysis, and a user can then select any one of those options, which will populate with sources for each one (e.g., selecting "*text*" will provide a user with tools to use for translation like DeepL Translate or Google Translate).

#### *A List of Miscellaneous Tools*

- OSINT Framework - <https://osintframework.com>
- OSINT Tools Directory - <https://osint.broker>
- DeepL Translate for Language - <https://www.deepl.com/en/translator>
- IP Addresses/Domain Names (e.g., <https://www.nslookup.io> for Domain Name System (DNS) records or <https://who.is>)

## Conclusion

The role of OSINT plays more of an integral part than just gathering data that is available publicly—it is an intelligence collection method that if used correctly and to its full capability can gain an abundance of actionable intelligence without the individual conducting OSINT ever having to leave the confines of the computer, so to speak. It really is a remarkable tool that can help any organization to advance in their overall agenda, and if not an organization, simply a person looking to apply the same principles of OSINT for their own personal means (e.g., academically/research based). OSINT, however, does rely on the user to be knowledgeable in a few key areas, such as 1. The understanding of what intelligence is and how to apply the intelligence cycle, 2. What OSINT is and how to apply the intelligence cycle to OSINT, and 3. The ability to employ critical thinking skills at all points throughout the process, not just technical capabilities. These areas can determine the *quality* of the final intelligence product, and that is something that should always be taken into account when producing anything that has the ability to influence actions and policy. After all, OSINT is a unique craft within itself, much like the other intelligence collection methods are as well, but it is something that can be learned with the proper training, and if utilized effectively, can be applied to a broad spectrum of environments across the public and private sectors.

## References

- Builta, J.A., and Heller, E.N. (2011). Institutionalizing Best Practices: Reflections on 10 Years of Counterterrorism Analysis. *Studies in Intelligence, Vol. 55, No. 3*.  
<https://www.cia.gov/resources/csi/static/Reflections-on-10-Years.pdf>
- Office of the Director of National Intelligence. (n.d.). *What is Intelligence?*  
<https://www.odni.gov/index.php/what-we-do/what-is-intelligence>
- United States Intelligence Community. (n.d.). The IC OSINT strategy 2024-2026. *The INT of First Resort: Unlocking the Value of OSINT*.  
<https://www.cia.gov/static/9d89dd9a4fe41b63cfab00c5191a8803/IC-OSINT-Strategy.pdf>
- U.S. Naval War College. (2025). *Intelligence Studies: The Intelligence Cycle*.  
<https://usnwc.libguides.com/c.php?g=494120&p=3381427>