



## **Institutionalising Open Source Intelligence (OSINT) in India: An Analysis**

**Amiy Krishna**

**Himachal Pradesh National Law University, Shimla**

---

### **Acknowledgement**

This paper has benefited from the direct contributions of Mr. Robert David Steele, the "father" of modern OSINT. Steele was born in the USA and grew up in Latin America and Asia. He earned multiple degrees and is a top non-fiction book reviewer with over 2000 reviews posted across 98 categories of reading. A former Marine Corps infantry officer and CIA spy, Steele was recommended for the Nobel Peace Prize in 2017 for his integration of holistic analytics, true cost economics, and Open Source Everything Engineering (OSEE). Mr. Steele's extended contributions to this project, including many graphics and links can be accessed at <https://phibetaiota.net/?s=Answers+on+OSINT>. All his works and publications are available at <https://phibetaiota.net/>.

I would also like to extend my sincere gratitude to Ms. Kanchana Ramanujam, Former Research Assistant at CLAWS and Former Assistant Professor, School of Military Affairs, Strategy and Logistics at the Rashtriya Raksha University (Gujarat) for her support in writing the paper.

### List of Abbreviations

<b>AIRMS</b>	All India Radio Monitoring Service
<b>CIA</b>	Central Intelligence Agency
<b>FBIS</b>	Foreign Broadcast Information Service
<b>FBMS</b>	Foreign Broadcast Monitoring Service
<b>GEOINT</b>	Geospatial Intelligence
<b>HUMINT</b>	Human Intelligence
<b>IB</b>	Intelligence Bureau
<b>ICT</b>	Information and Communications Technology
<b>IMINT</b>	Imagery Intelligence
<b>IPKF</b>	Indian Peace Keeping Force
<b>MASINT</b>	Measurement and Signature Intelligence
<b>NATGRID</b>	National Intelligence Grid
<b>NGA</b>	National Geospatial-Intelligence Agency
<b>NSA</b>	National Security Agency
<b>OSA</b>	Open Source Agency
<b>OSC</b>	Open Source Center
<b>OSD</b>	Open Source Data
<b>OSE</b>	Open Source Enterprise
<b>OSINF</b>	Open Source Information
<b>OSINT</b>	Open Source Intelligence
<b>R&amp;AW</b>	Research and Analysis Wing
<b>S&amp;T</b>	Science and Technology
<b>SIGINT</b>	Signals Intelligence
<b>TECHINT</b>	Technical Intelligence

**O**pen Source Intelligence (OSINT), refers to unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question.<sup>1</sup> The acquisition techniques for OSINT are unintrusive<sup>2</sup>, legal and ethical. Such public information may either be collected by observation, or requesting to the holder of such information, or be acquired through subscription or purchase.<sup>3</sup> OSINT provides the foundation for other intelligence disciplines.<sup>4</sup> When applied in a systematic fashion, OSINT can drastically reduce the burden on other intelligence collection disciplines by limiting requests for information only to those questions that cannot be answered by open sources.<sup>5</sup>

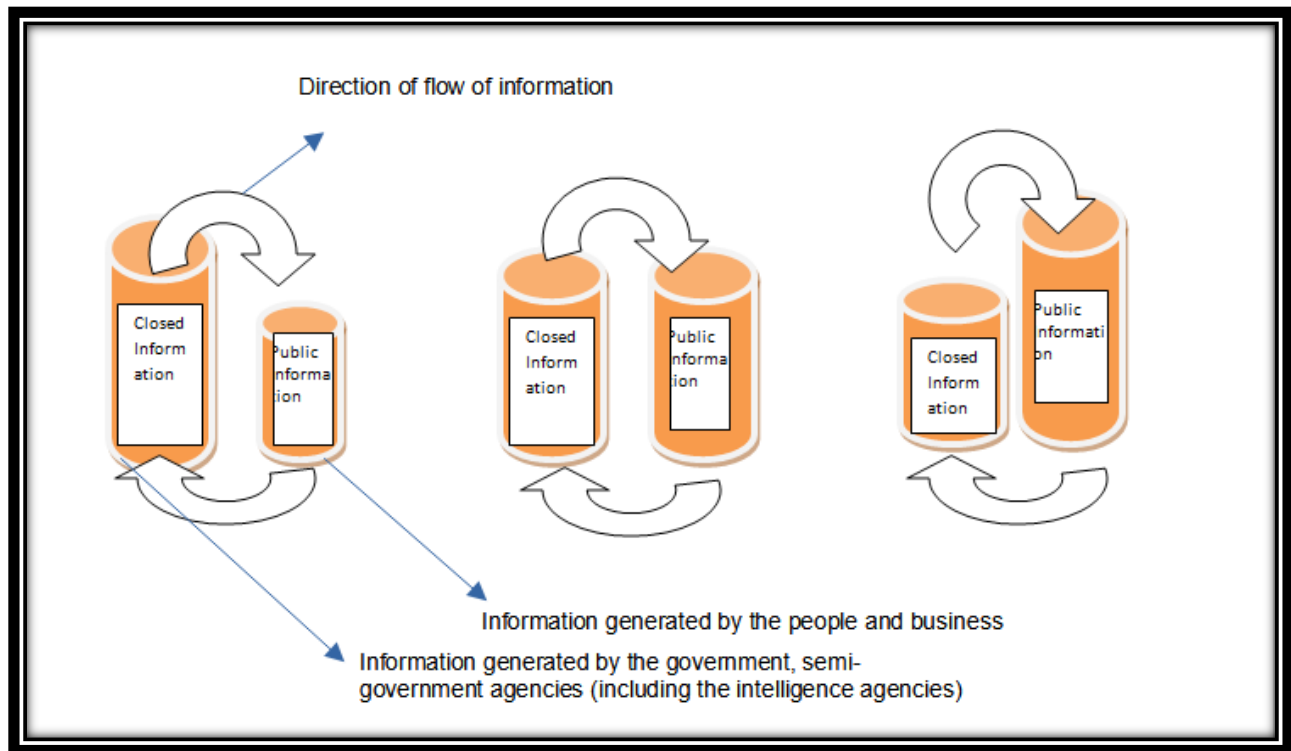
Allen Dulles, former Director of the Central Intelligence Agency (CIA) stated as back as in 1947 that a proper analysis of the overt sources of information would provide over 80 per cent of the total information needed in their national policy making.<sup>6</sup> Scheuer, the former head of the CIA's special Bin Laden unit has said that: "90 per cent of what you need to know comes from open source intelligence".<sup>7</sup> United States' CIA Community Open Source Programme officially figured the contribution of OSINT to 40 per cent on average; the outliers ranging from about 10 per cent in denied areas to about 90 per cent in international economics.<sup>8</sup> In short, experiences world over depicts the increased capability of OSINT to provide a large chunk of intelligence, larger than the other intelligence collection disciplines.

Today, with a more open and independent world, open sources have even greater value for intelligence. It is imperative that these sources are given the needed emphasis and biases towards other sophisticated intelligence disciplines are checked.

### **Drivers of OSINT**

The debate on OSINT is driven by three major factors namely— globalisation<sup>9</sup>, ICT<sup>10</sup> and market liberalisation. A mix of these factors incentivises the information creator as well as the information holder to disseminate the information to a well broad section of the public. The information creators/holders do it to meet the expectations of those who are directly or indirectly affected by their actions.

**Figure 1: The Information Scenario**



ICT, globalisation and greater participation of the private sector has resulted in an information explosion — the availability of multitude of unclassified, open sources of information that can be used advantageously by the intelligence agencies.<sup>11</sup> The multimedia explosion and the associated information thus produced have outpaced the collection and analysis by intelligence agencies.

**Figure 1** gives us an idea of the information scenario just before the advent of the information age. Consider the whole existing information to be divided into two silos— *one*, depicting the government while the ‘other’, depicting the people (or public information). The information flow, before the advent of the information age, was from bigger government silos to smaller public silos, due to non-existence of ICT technologies and lesser number of incentives that would ask for greater information publishing. Control of information was its business; and unique access to others’ secrets, was its advantage.<sup>12</sup>

With time, the ICT technologies and private sector growth changed the scenario. In second part of **Figure 1**, information produced by the people gave a hard fight to previously controlled information disseminators. Public information got nourished; people and the private sector

started to become better at creating new information and knowledge. Slowly and steadily, the information flow got directed from the people to the government.

The third part of **Figure 1** shows the present scenario in which the private businesses & people generate more and better information than the government. Consequently, the information quantum got tilted towards the private sector and people. Thus, the main actors are the people who are not in the government sector. This information imbalance is the main reason for leveraging the OSINT capabilities of any government. The government needs to realise that it no more controls information creation and dissemination. Intelligence is no more about secret sources previously collected by expensive and risky methods.<sup>13</sup> The government and the intelligence agencies nowadays are 'customers of information' rather than being 'creators of information'.

### **Why is Information Available?**

In recent decades, advancements in ICT have provided with better, cheaper and faster information sharing platforms, but the phenomenon does not explain the incentives that functions in the background to motivate the information creator to disseminate his works. ICT is not the behavioural reason behind the phenomenon of wider information availability. It is the 'information creator' who has to decide whether or not to distribute information.

The benefits of publicising information are greater — academics publishes to get promoted; commercial organisations publishes to get advertised and fulfil government regulations. Government publishes information to maintain its legitimacy; the media publishes information to widen its reader base while the military publishes information to fulfil its legal obligations. Information Operations is also an incentive. The non-profit organisations need to get donations and the law-enforcement publishes to do crime statistics.<sup>14</sup>

All the actors mentioned shares information deliberately. They understand the consequences of wider dissemination of information. Another passive but massive creator and disseminator of public information is the average individual who does it honestly and unknowingly via online system and Internet of Things (IoT). These individuals acts like a 'chicken which feeds itself', later on, to be 'utilised as meat'. Similarly, the individual who is surrounded by electromagnetic devices, plays the role of a product by unconsciously selling his information for short-lived comfort. The information thus harvested outpaces the information collected through other sources. Such information harvesting is possible through algorithms that makes the user spend

more time over an online platform or application. This addictive behaviour creates a symbiotic relationship between the technologies and humans. So, as the information moves at an ever greater pace, through this symbiotic structure, a gravitational pull is created. This gravitational pull disallows an individual to resort to traditional sources of information and makes him believe in whatever he is deliberately shown.<sup>15</sup>

### **Why OSINT: The Three Questions and its Relationship with Closed Sources**

It is consequential to know the relationship between closed sources and open sources of information. The author asked Mr. Steele the following three questions<sup>16</sup>-

- Are Open Sources richer than closed ones?
- Are Open Sources as rich as the closed ones?
- Are Open Sources the chiseled out bits of closed sources which when put together tells us about the closed sources they owe their existence to?

General Anthony Zinni, Former Commander of the US Central Command (USCENTCOM) officially observed that, secret sources provided him 'at best 4per cent' of whatever he needed to know; 16 per cent of what he needed to know, he got them easily; 80per cent of what he needed to know came from open sources.

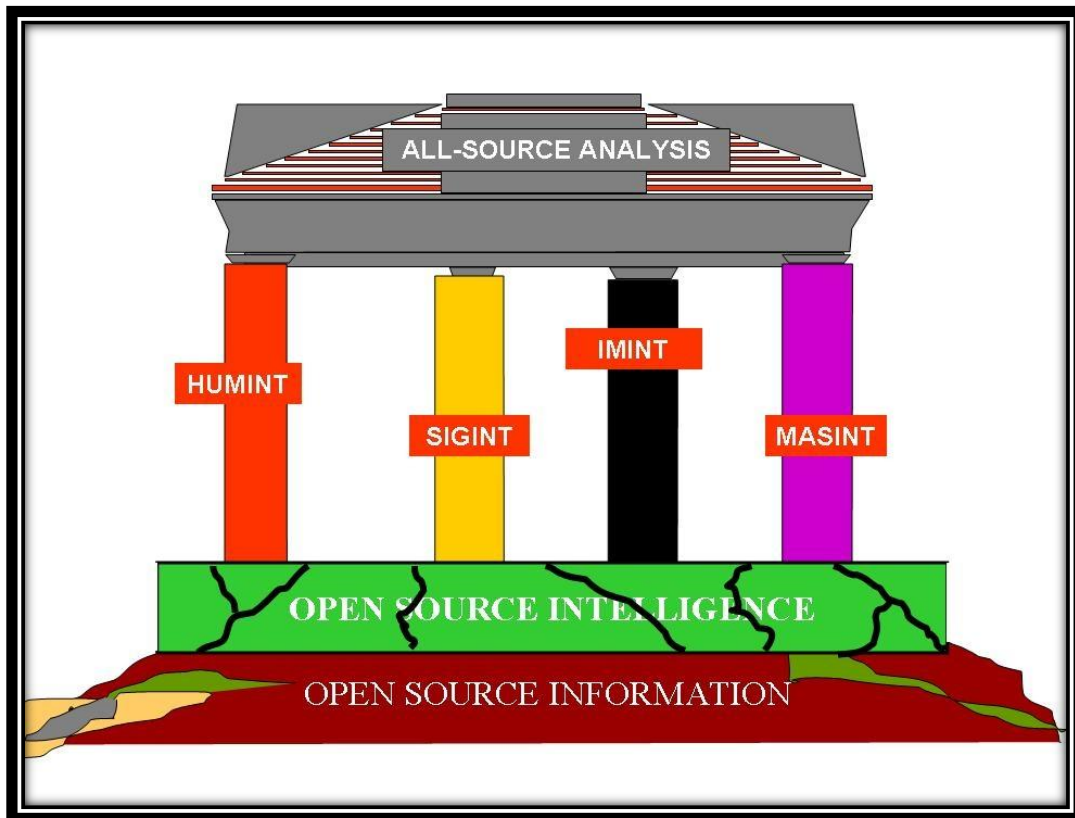
Open Sources are vastly richer than closed ones. These can properly provide information about the past, the present and the future. Everything that we term as 'closed' was previously open source information that has been classified now. For example, dual-use technologies were available in the open source for atleast two years before they were classified.<sup>17</sup>

The '80 per cent rule' tells us that the success ratio is 'case dependent'. The ratio can get as low as 20 per cent for hard and denied areas. But as a general rule, open sources must be fully exploited before resorting to other methods. The Dutch Intelligence Service does not allow resorting to closed sources until it has exhausted the open sources.

Extremely valuable open sources are called Black OSINT—so valuable and revealing that they should be immediately classified. Also, it is tough to understand what closed sources are. For example, a bystander observes troops movement or counts the number and type of weapons with them. Now, for the army, it is classified information but for the bystander it is open and there exist no impediments in sharing it. The only closed source information is the intention and motive of the adversaries. Intelligence aims to predict these intentions.

OSINT is not only a separate discipline in its own right; it also provides a very strong foundation for other disciplines by helping the commander to precisely design his intelligence requirements.

**Figure 2: OSINT is a Strong Foundation for other INTs<sup>18</sup>**



A clandestine Human Intelligence (HUMINT) cycle consists of spotting, assessing, recruiting and handling. OSINT provides a strong foundational base by:

- Mapping contacts and research areas thus planning approach to specific people (Spotting).
- Conducting background investigations of individuals before recruiting them and evaluating the relative potential of individuals with different forms of access (Assessing).
- It has been helpful in intelligence and counterintelligence by vetting people and checking their claimed recollection against publicly available information sources (Handling).

The following graphic shows the optimum potential of OSINT. The percentage ratios given shows the practical utility of OSINT.

**Figure 3: OSINT Done Optimally<sup>19</sup>**

Economic and social threats, including	95%
• Poverty	99%
• Infectious Disease	95%
• Environmental Degradation	90%
Interstate Conflict	75%
Internal Conflict including	90%
• Civil War	80%
• Genocide	95%
• Other Large-Scale Atrocities (e.g. Human Trafficking)	90%
Proliferation (nuclear, radiological, chemical, biological)	75%
Terrorism	80%
Transnational Organized Crime	80%

## Evolution of OSINT

Espionage is considered to be the second oldest profession. Ancient and medieval espionage considered ‘news’ to be synonymous with ‘secret information’.<sup>20</sup> This section aims to explore the key players and institutions through which OSINT was institutionalised into decision-making. A broad historical timeline of OSINT is given in the **Figure 4** below.

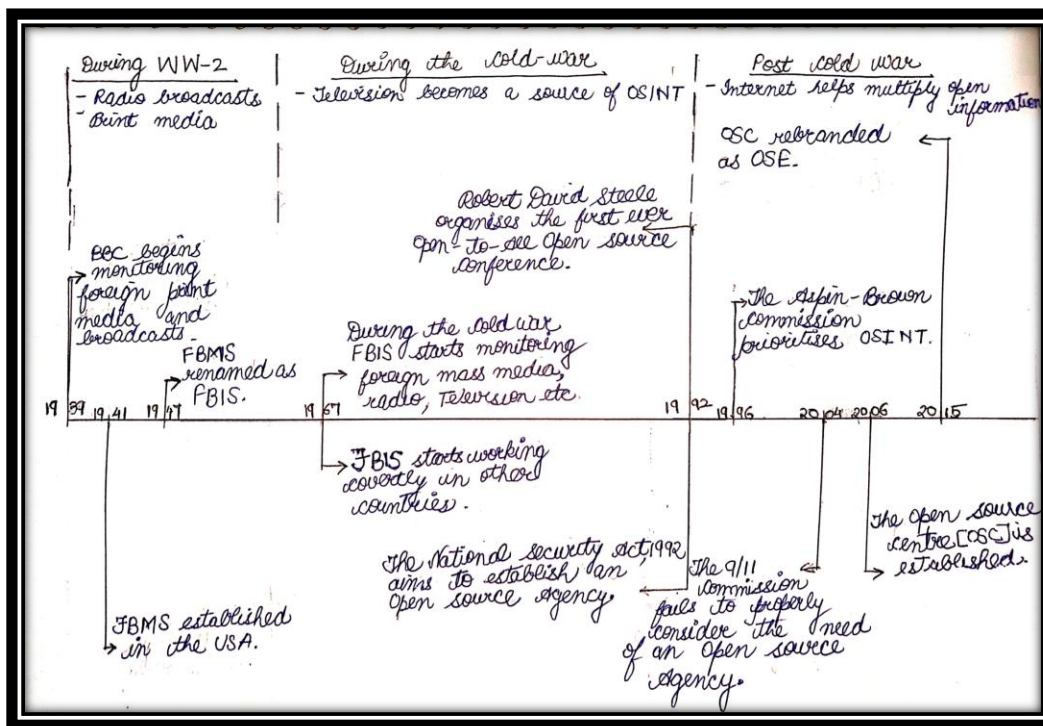
The evolution of OSINT can be presented in three different phases:

- Pre-World War I blurred differences between open and secret sources; news and secret information.
- During and post World War II till the end of the Cold War, intelligence experts realised the importance of newspapers, radio and personal witness accounts.
- End of the Cold War to present and the ‘revival of OSINT’. Internet and development of ICT, along with the spurt in information produced by non-government sector breaks the information-monopoly of the intelligence agencies. The period also witnesses the growth of private sector participation in areas previously controlled, example being commercial imagery.



In 1939, the British Government tasked the British Broadcasting Corporation to monitor foreign print journalism and radio broadcasts.<sup>21</sup> BBC and the US government partnered in 1947/48 to share this information.

Figure 4: A Basic Timeline of Evolution of OSINT<sup>22</sup>



Before the establishment of CIA in 1947<sup>23</sup>, intelligence activities of the US were carried out by the Office of Strategic Services (OSS) which was established in 1944.<sup>24</sup> Founded by William Donovan, the OSS carried majority of its work by collecting and analysing open sources of information.<sup>25</sup> The USA also established the Foreign Broadcast Monitoring Service (FBMS) in 1941, to monitor the media and radio broadcasts of its adversaries;<sup>26</sup> German propaganda radio channels, aired over shortwave radio transmissions, were given extra importance.<sup>27</sup> The information collected by FBMS was sometimes shared with the US public.<sup>28</sup> Later, the FBMS was merged with the CIA and renamed the Foreign Broadcast Information Service (FBIS) in 1947 with the enactment of the National Security Act, 1947.<sup>29</sup>

The second phase of OSINT evolution covers the Cold War era until the division of the former Union of Soviet Socialist Republics (USSR). This phase is marked by two important technological revolutions— wider use of the Television and later on; the Information Revolution

due to the internet and better computing technologies. In 1961, the State Department, the CIA and the FBIS used to collect, translate, analyse and disseminate open source information.<sup>30</sup> In 1967, FBIS was ordered to operate overtly around the world.<sup>31</sup>

This period also saw the increasing use of other INTs of intelligence. Technological advancements, on one hand, found developed Signals Intelligence (SIGINT) and Technical Intelligence (TECHINT) methodologies and, on the other hand, the same technological developments led to a wide flow of public information. A declassified study observes a spurt in the number of scientific titles by around 4.5 times and sociological titles by 2 times. The study also observes that the CIA obtained around 75 to 90 per cent of total economic, scientific and geographical information from open sources.

The end of the Cold War further put more open source information into circulation.<sup>32</sup> The later period witnessed an exponential increase in the use of the internet. After the end of the Cold War, the open source debate was enlarged when an 'open to all' OSINT conference was organised by Robert David Steele.<sup>33</sup> The conference saw the participation of around 600 participants from the government as well as the private sector from more than 40 countries. The conference was symbolic as the big attendance proved the need and benefits of getting more and more persons in the OSINT loop. In the same year, a US senator had proposed a National Security legislation that would create an open source intelligence agency under the Deputy Director of National Intelligence for Estimates and Analysis.<sup>34</sup> However, the legislation never passed.

In 1996, the Aspin-Brown Commission was constituted to look into intelligence reforms in the US and noted that the intelligence agencies were slow to access open databases and recommended the creation of a network that connected the intelligence experts with open databases.<sup>35</sup>

In 2004, the 9/11 Commission submitted its report. Interestingly the 9/11 victims had provided valuable information to the Commission, collected from open sources.<sup>36</sup> Sadly, the final report only touched on the issue of OSINT and didn't try to deliberate further into the matter. It only recommended the creation of an Open Source Agency within the CIA.<sup>37</sup> The Committee was however ignored the fact that, the 9/11 hijackers and planners had relied on public telephone directories, aviation magazines, aeroplane timelines etc.<sup>38</sup>

In 2006, USA established the Open Source Centre (OSC). The agency also merged the FBIS with it.<sup>39</sup>It disseminated reports through a website (www.opensource.gov, **see Figure 5**) People could login and read the reports according to the clearance level. The website could even be accessed by common US citizens, although the material available to them was limited. The OSC was later on rebranded as the Open Source Enterprise (OSE) in 2015.<sup>40</sup>

**Figure 5: The OSC Website's Login Page (as was on Feb 16, 2013)<sup>41</sup>**



## OSINT and Other INTs

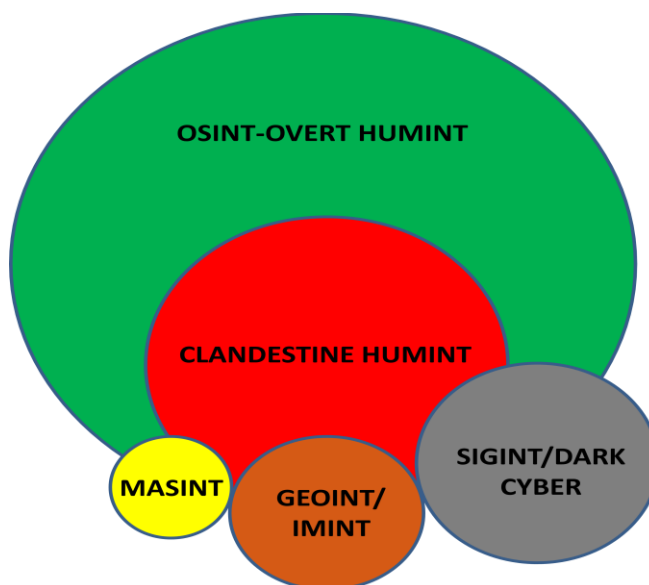
Intelligence collection is a mix of four major disciplines other than OSINT. A brief understanding of each discipline is given below:

- **Human Intelligence (HUMINT).** HUMINT is intelligence collection by human-to-human interaction. Intelligence can be collected overtly, covertly and clandestinely.

- **Signals Intelligence (SIGINT).** SIGINT employs interception of communications or messages between individuals (done electronically) termed as COMINT (Communications Intelligence) and the interception of Electric signals (for example, monitoring of radars) termed as ELINT (Electronic Intelligence).<sup>42</sup>
- **Geospatial Intelligence (GEOINT).** GEOINT is the visual representation of activities.<sup>43</sup> It includes the analysis of images to extract information of intelligence value which is called IMINT (Imagery Intelligence).
- **Measurements and Signals Intelligence (MASINT).** MASINT is scientific and technical information obtained by analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydro-magnetic) derived from technical sensors for identifying any distinctive features associated with the source, emitter, or sender, and to facilitate subsequent identification and/or measurement of the same.<sup>44</sup>

OSINT is necessarily HUMINT.<sup>45</sup> OSINT is HUMINT as majority of open sources are not available online (discussed separately) and not in the language the intelligence analyst is adept in. To understand OSINT and its fusion with other INTs, it is important to understand the importance of HUMINT. OSINT is 'Overt-HUMINT', as the sources on which it relies are available with the public (though information overflow, negligence and aversion might obscure such information from the public).

Figure 6: OSINT's relation to Other INTs<sup>46</sup>



Majority of open source information are not available over the internet and the only way to collect them is to use manpower. This makes OSINT a variant of HUMINT rather than a technology dependent discipline. In the graphic, one would find it odd that the circle showing OSINT is bigger than the circle showing Clandestine HUMINT. The reason is that organisations/agencies that were 'previously net producers of information', are now 'net consumers of information' dependent on the information out of their substantive control.

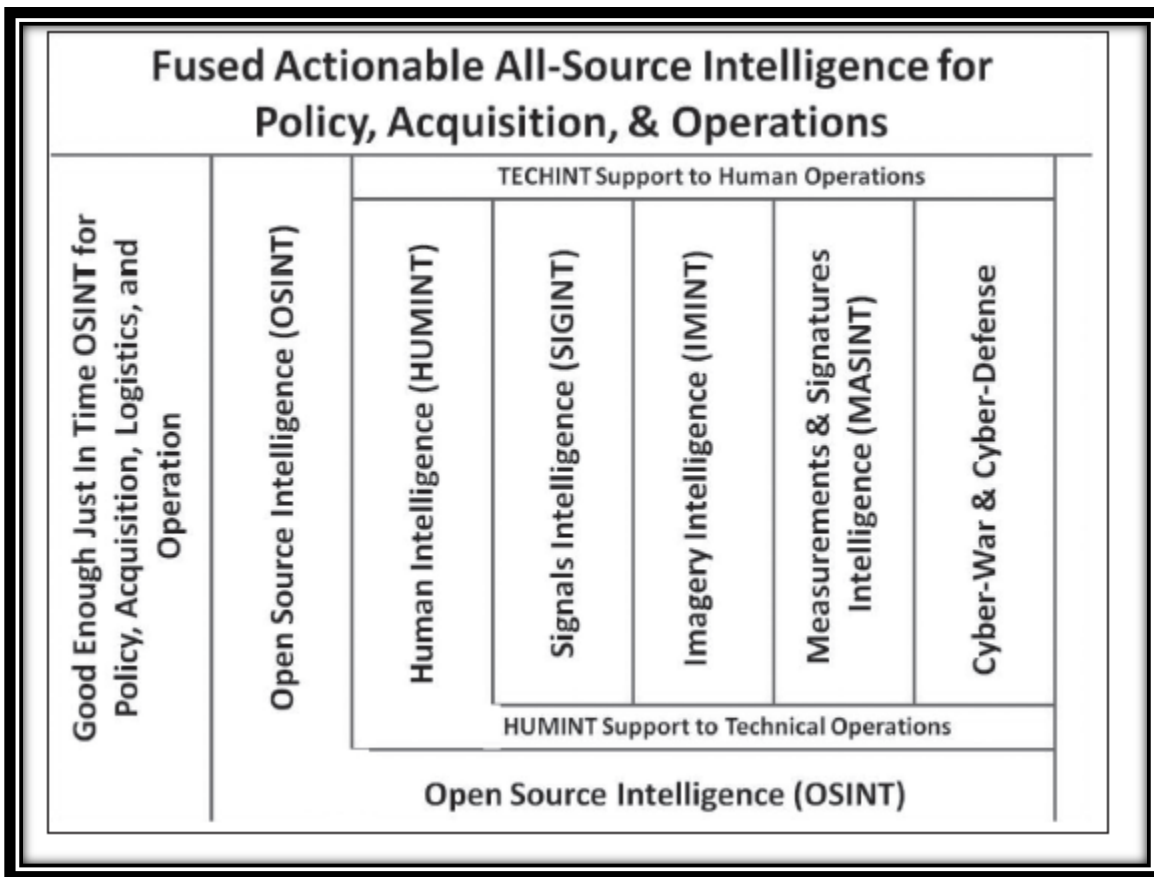
OVERTOSINT is a confusing term *prima facie*. One might get confused with the word "Overt". The word doesn't mean that the collection is done publicly.<sup>47</sup> Overt refers to the sources and to the collection methodology. Thus, the identity of the analyst is not made public. Now, that we understand the human character of OSINT, it is to be understood that only HUMINT is complete in itself. Other INT disciplines can never eliminate the need and support of HUMINT. Without HUMINT, most technical intelligence is noise. Without HUMINT, decisions will continue to be made in a vacuum, at (sic) great cost.<sup>48</sup>

SIGINT mainly relies on HUMINT; HUMINT has to develop the foundation of SIGINT operations by informing the Commander about the communication devices used by the adversaries, the number of radars and the cryptography involved in communication. Maintaining of listening posts and manual translation of unknown languages and dialects are to be done by humans.<sup>49</sup> Humans transform the uncountable, 'esoteric pixels' into meaningful, digestible pieces of hard information.<sup>50</sup>

GEOINT and IMINT fail miserably in wide-area surveillance; clouds, canopies, caves and also underground instalments decrease their efficiency. Unmanned Aerial Vehicles (UAVs) have increased the capacity of GEOINT but UAVs have limited flying hours and altitude endurance.<sup>51</sup>

MASINT is dependent on sensors that are to be manually placed. Even in cyber warfare, the decision making power rests with humans. Thus, in every INT discipline, human involvement is not only necessary but also forms the core of the discipline.<sup>52</sup>

Figure 7: HUMINT vis-a-vis other INTs



### OSINT (The only Self-Sufficient INT)

OSINT is the only INT that gives a panoramic view of the situation. OSINT based SIGINT involves resorting to open source information on the adversary's radars, communication devices etc. Also, in the case of the internet, analysing the traffic on a website and monitoring the views.<sup>53</sup>

Commercial imagery is capable of giving high-resolution images and is generally available to anyone for a price.<sup>54</sup>The private sector has been able to utilise such services. This shows the use of OSINT in GEOINT/IMINT.

Anything that involves technology, available for sale or transfer to anyone, the technology being supportive in conducting MASINT, shows the use of open technology in MASINT. The analyst

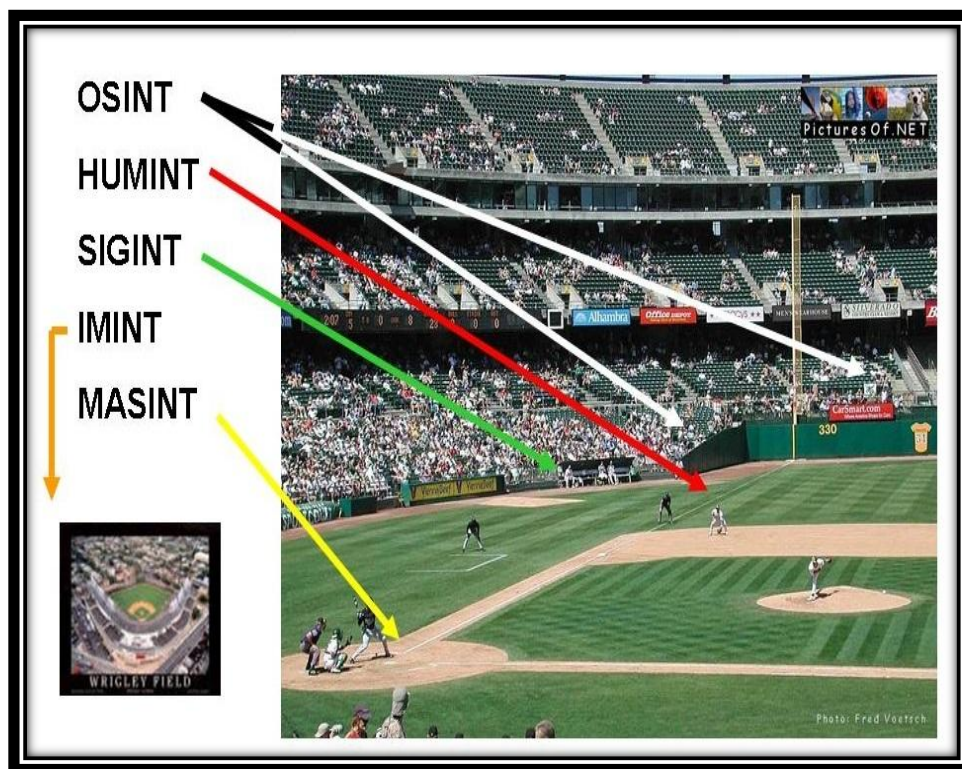


can also purchase or gather information directly which he could have otherwise obtained by conducting expensive and risky MASINT operations.

The Baseball analogy graphic gives an easy understanding of OSINT and other INTs.<sup>55</sup> Assume the playground to be the battleground and concentrate on the following actions and the respective limitations:

- The SIGINT expert 'places bugs and listening devices' to listen to what the players say.
- HUMINT 'recruits a player' to drop or catch the ball on command, but the covert nature of HUMINT makes commanding risky and time taking.

**Figure 8: OSINT Baseball Analogy**



- MASINT 'places sensors' to sniff the ball leaving the glove.
- IMINT 'covers the ground' by occasionally taking aerial pictures.

The crowd depicts OSINT. It is the crowd that can see, sense and analyse everything. It can record every player's actions. It has access to a commercial imagery service similar to the one which the IMINT operator makes use of. The crowd has access to live score through the internet

and is capable of presenting a 3D idea of the scenario. The players cannot tilt their head sideways due to limited capabilities. They capture only an iota of the bigger picture. Sadly, the crowd (OSINT) is hardly resorted to as a source in decision making. The crowd is a cheaper source too when compared to the players who bill and rate their services highly even for limited information.

### **Understanding OSINT**

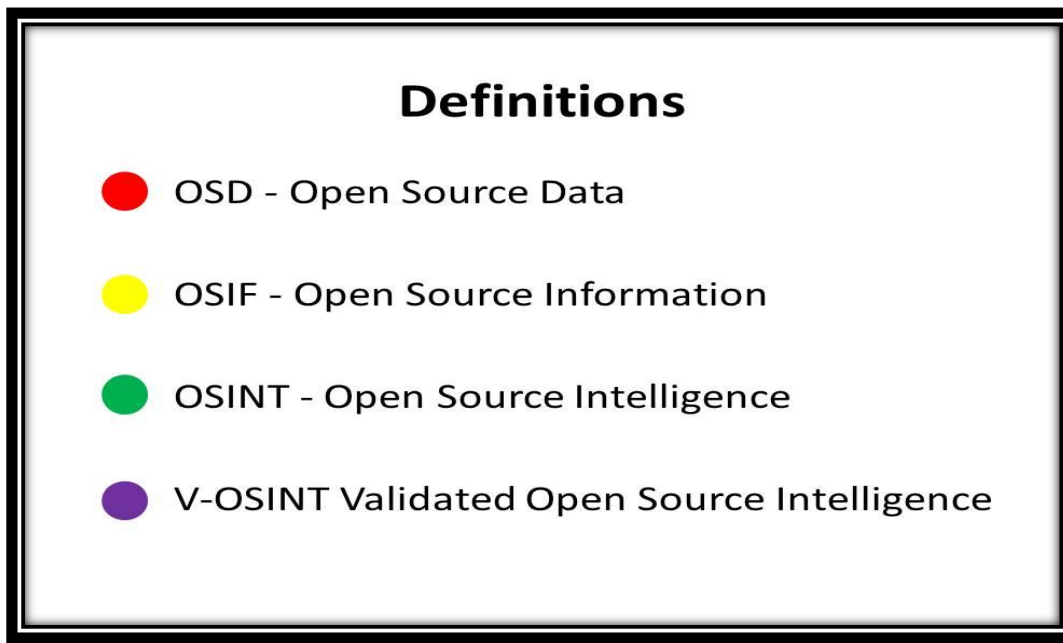
The Information Age ended the information monopoly of the Government, consequently making it a netconsumer of information. This changed paradigm requires extra effort by the government to compete in this Information Era. The Government needs to understand the 'sources and methods' of information that would help in decision making. Before proceeding any further, the reader should recollect the following:

- Intelligence is 'decision support'. Intelligence helps in choosing from one of the many (or few) recourses available.<sup>56</sup>
- Intelligence is 'requirements (need) driven'. Prior to the collection of information, it is pertinent to frame the need like what is needed?, how much is needed? By whom? To what extent? In which form?<sup>57</sup> If not framed properly then external conditions would drive decision making rather than internal requirements.
- Intelligence is not about knowing secrets or collecting confidential information— it is about leveraging capacity. Intelligence is more about the quality of information than the source of information. The government has become a consumer of information and it is a global phenomenon. Thus, everything that was presumed to be confidential is now available publicly somewhere. This necessitates the exploitation of such information.



## Open Source Data, Open Source Information, Open Source Intelligence

Figure 9: Open Sources (Data, Information and Intelligence) and OSINT-V<sup>58</sup>

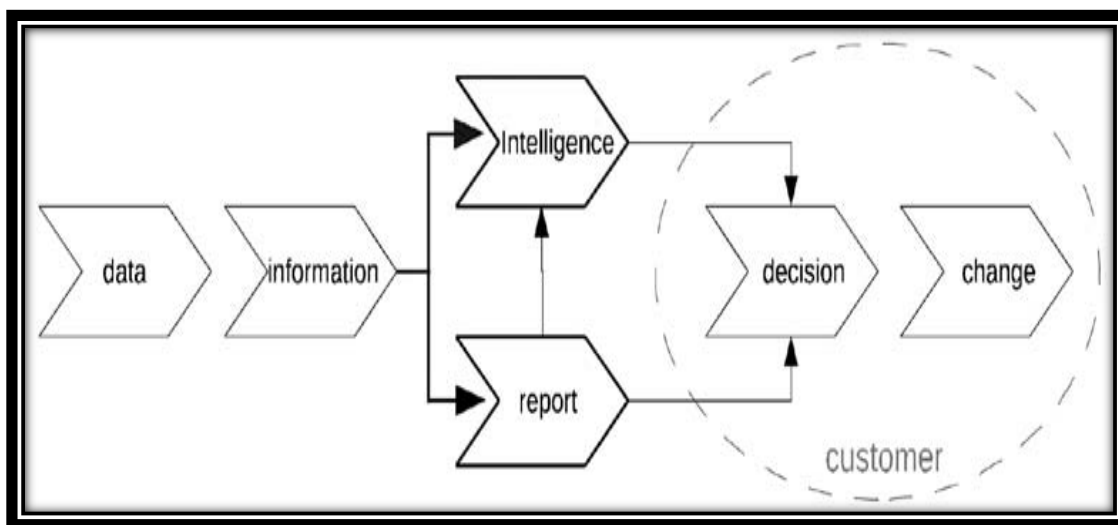


Every piece of information is not a generic finding, rather it is a culmination of many bits of data that are put together to churn out the meaning. Open Source Data, Open Source Information and OSINT are different, though they are synthesised (or unsynthesised) forms of each other. OSINT is understood as being “any” information that is publicly available. It is where the conceptual understanding goes wrong. To clarify, it is important to note the following definitions:

- **Open Source Data (OSD).** Data are the raw prints, broadcasts, pictures, letters, recordings, and documents.<sup>59</sup> Data cannot convey a message on their own.
- **Open Source Information (OSINF).** Datasets put together and arranged in a manner that may convey some message. Data can also be augmented or corroborated with previous pieces of information to create some new information. News pieces, reports, research papers etc are all OSINF.
- **OSINT.** OSINF that is put through the intelligence cycle and the product received is used in decision making. It must address a particular question or requirement of the commander or the leader.

- Validated OSINT (OSINT-V).**<sup>60</sup> OSINT, on which a high degree of certainty can be attributed, is generally made possible after validating the sources or comparing the OSINT product with other classified sources of information.<sup>61</sup> The classified sources must either confirm the OSINT product or not negate the intelligence gathered through OSINT. For example, a news article claims that a certain bridge, that is vital for the forces, exists. Classified sources may either confirm the existence of such a bridge or they don't negate its existence.<sup>62</sup>

**Figure 10: Data, Information and Intelligence**<sup>63</sup>



OSINT and OSINF however differs and are not synonymous. A misconception is that any openly available information has intelligence value. Intelligence is ‘not information’; intelligence is also not that ‘piece of information’ which contains new facts having incriminating nature. Intelligence is an answer to a specific question. Information (or OSINF) is generic, unstructured and practically useless as it does not answer the specific requirement of the commander. Intelligence, on the other hand, is a highly specific answer to the commander’s question. The deciding factor is, whether the commander does something or abstains from doing something based on the information— in short, ‘information is the genus while intelligence is the species’. Even the ‘intelligence’ that one agency might share is information for the other agency.<sup>64</sup> The most ably mapped and illustrated report also does not make it intelligence until utilised in decision making.

OSINT is a product and not an input. The input is OSINF. Also, unless a product helps in decision-making, it is not very useful. For instance, the well-known Okinawa Report<sup>65</sup> of the

OSC, which falls under OSINF as it does not help in decision making. It might be an excellent report but it is not OSINT.

### **OSINT Intelligence Cycle (The Diamond Model)**

The generic intelligence cycle consists of a four-step process<sup>66</sup>(even five, six or eight but the core philosophy remains the same). The cycle can be summarised as under:

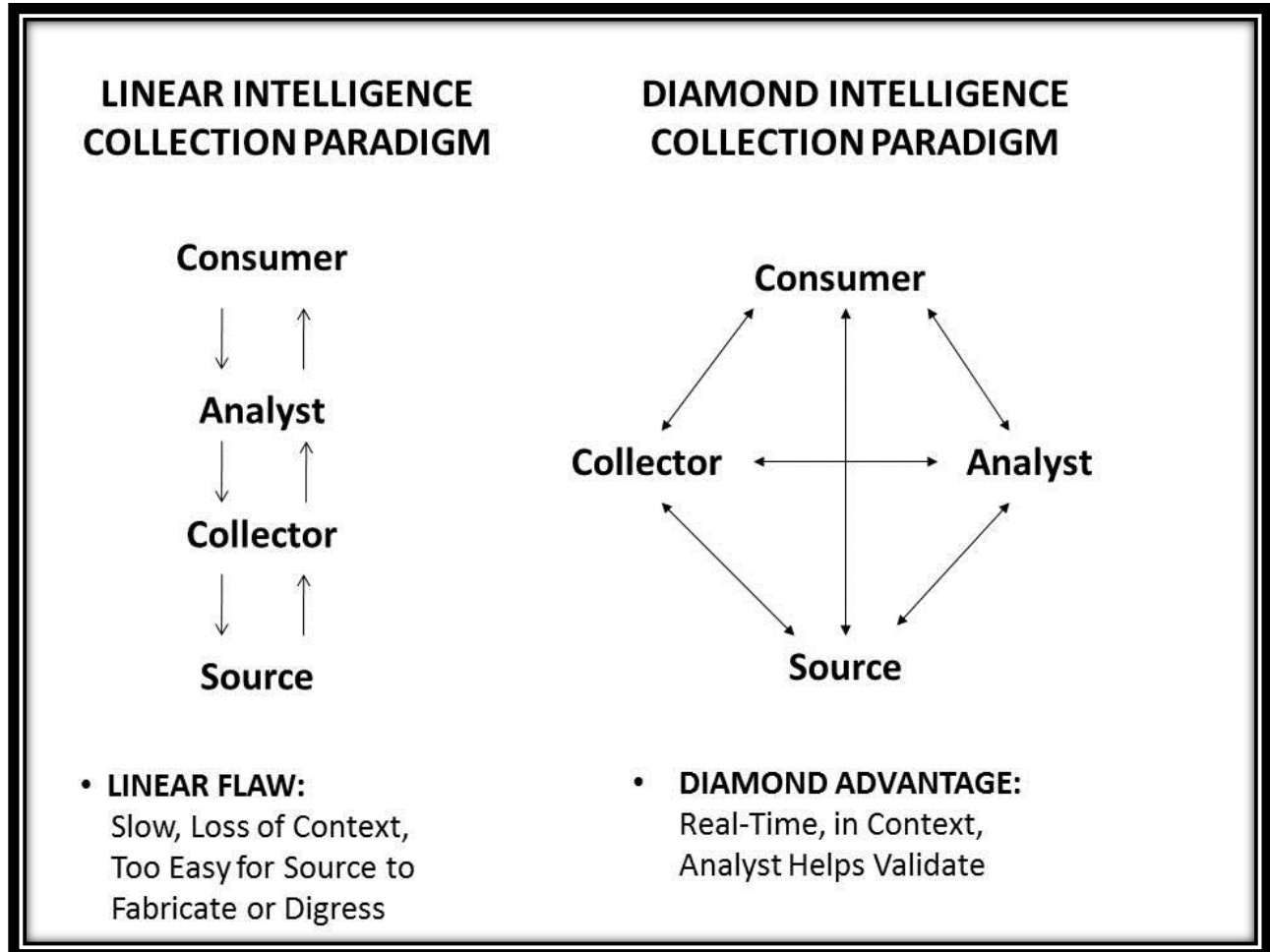
- i. **Direction.** Commanders decide the requirements and scope of the information they need for decision making.
- ii. **Collection.** Raw information and/or data is collected through covert, clandestine or overt means.
- iii. **Analysis/Processing.** The data/information collected is processed and turned into meaningful information. It involves drawing conclusions from the data and finding its proper application. Also, information is put through 'All-Source Analysis'.
- iv. **Dissemination.** The information is forwarded to the leader who decides whether or not to take or avoid any action or decision. It is at this step only that information is converted to intelligence (utility in decision making).

The cycle explained above doesn't suit OSINT. It has a limited scope of brainstorming as the people involved in one part of the cycle are cut off from their counterparts. The time consumed in the cycle undermines the requirement of fast decision making.

Even the smallest mistake at one part gets cascaded in the next part. Individuals involved in the cycle can also knowingly or unknowingly disseminate false facts, biased opinions which would add unwanted burden to the finished intelligence product(s).

OSINT, on the other hand, requires greater flexibility and openness as the sources involved are publicly available and there exists no new need to obscure them. Thus, the following model on the right side of **Figure 11** (The Diamond Model) fits suitably.

Figure 11: Linear v/s. Diamond-Model of Intelligence Cycle<sup>67</sup>



The model eliminates the inherently bureaucratic and slow nature of the generic intelligence cycle. No communication barriers exist among the different parts of the cycle. This helps in faster decision making and allows the leadership to take into consideration any information at any stage, thus eliminating the possibility of any error and malafide amendments.

### Tribes of Information: Government a Net Acceptor

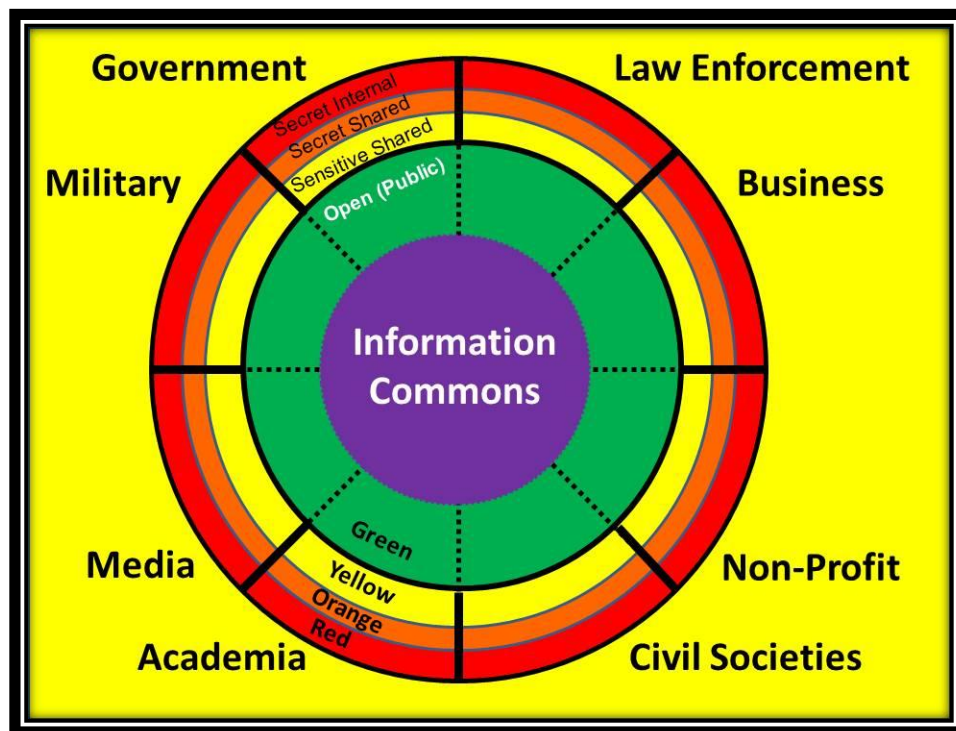
Most nations have eight key players who produces, utilises, disseminates and deals in information. The information ecosystem requires them to cooperate and institutionalise information sharing. This concept, known as the 'Intelligence Commons', is presented in **Figure 12** below and the eight key players are called the "Eight Tribes".

As per the concept, the Eight Tribes 'produces and possesses information', more worthy than what the government, military and law enforcement 'together produces and possesses'. Of all

information available, every tribe consumes or produces to the extent of its mandate, with a false presumption that, it has all the information it needs without realising the nature of information and its attributes like volume, velocity and dual-nature.

Sadly, the tribes are disunited by impervious walls that disallows them to apportion information even though a clear picture is possible only when the Eight Tribes collaborate. The tribes have capabilities and capacities developed over time and it is not practical for one tribe to learn or to imitate what the other has learned. Imagine it like a football team with each player getting a chance to hit the ball. The team cannot win without mutual support and synchronisation and no one player can be replaced with a substitute without providing him with proper training. The training is cumbersome considering the quick pace of the match.

Figure 12: Steele's Eight Tribes Model<sup>68</sup>



One might find different groupings for the tribes. For example, in the Indian Context, 'Law Enforcement' could be replaced by "Internal Security" and 'Non-Profit and' 'Civil Societies' can be clubbed together. Similarly, 'Think-Tanks' are a part of the Government and are included under it. The gist is that, information is distributed and no clear-cut monopoly exists. Hence, sharing is the only solution.

## **Perceived v/s Real OSINT: Myths v/s Realities**

OSINT was not able to develop as a separate INT, because certain myths had developed due to 'cocooned thinking', 'limited knowledge' and 'aversion' towards OSINT.

Ask a simple question— How does information or data originate? An average answer would be that any action, omission or incident gets recorded either orally or in writing, in audio-visual expressional form or format. Such recording is very raw and generic and falls mostly under the category of 'data'. These 'data' are then compared or fused to make it worth conveying something. Data thus turns into information. At this stage of 'information' or the stage of 'data', the material is exploited by various institutions or organisations. These institutions develop expertise in one type of data. With time, these institutions develop an understanding of, what we might call a 'data/information landscape'. Thereafter, such institutions develop expertise in a particular landscape virtually at the omission of others.

This paper does not discuss 'the Sources of Information' because the information ecosystem is so big and diversified that any such attempt would limit the scope and application of OSINT to a small number of items. Generally, sources of information include newspapers, journals, television and radio broadcasts, magazines, research papers, periodicals, grey literature, etc. (offline and online).<sup>69</sup> Worth special mention is 'Grey Literature'. Grey Literature is the open source information that is available through highly specialised channels and is meant to be utilised by a specific section of the public. Examples include dissertations, conference papers, market surveys, meeting proceedings etc.<sup>70</sup> These materials are unclassified, although their circulation is restricted and limited. Such literature has information that is often not available through other sources.<sup>71</sup>

The biggest myth that prevails is that, OSINT is nothing but a collection of information through these sources. It is misunderstood as collecting a photograph, a newspaper article, a research paper, a television or radio broadcast and sticking them on a thumb-pin board and performing average level analysis. This myth originates as it is presumed that-

- Every piece of information, meant to be put for public use, is also available publicly.
- The information ecosystem is an inhibited area devoid of any noise, partialness and opinions.
- It is easy to master the way information is produced, disseminated and even destroyed in a particular information landscape.

This approach is Passive OSINT which denotes OSINT that lacks the indispensable rigour and zealotry. This reduces OSINT to 'rag-picking' of information. This attitude exhausts the collector as he tries to reconnoitre the 'information black-hole'. More information gets added by the time the collector becomes adept in the sources—the collector keeps on searching for that particular eye opener piece of information which is complete in itself. This reduces OSINT to 'by chance' intelligence.

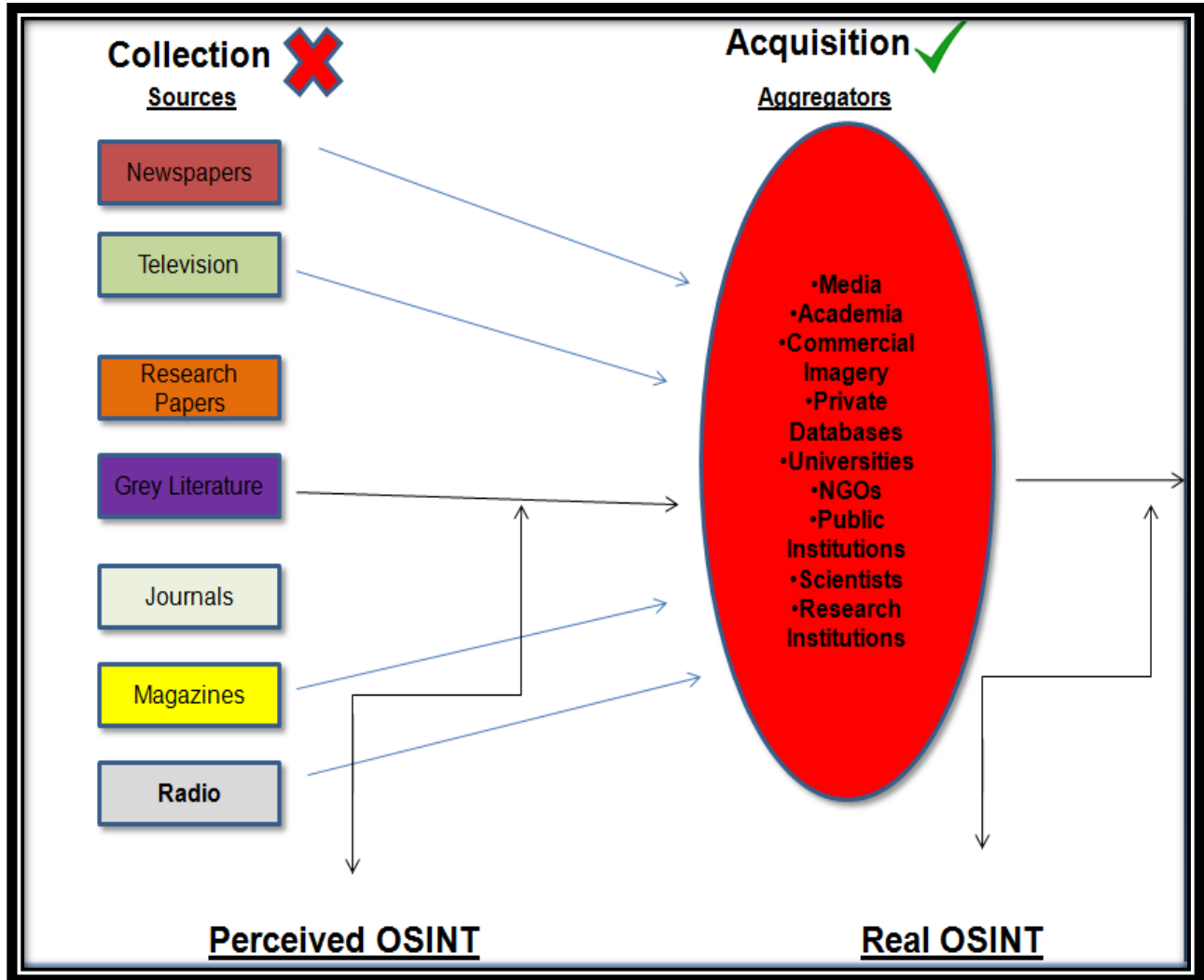
### **Collection v/s. Acquisition: Recall the definition of OSINT**

OSINT nowhere uses the term 'collection'. Rather, it uses the word 'discovery'. Real OSINT never involves an indiscriminate collection of published sources. Recollect that, 'not every piece of information that is public gets published'. The sources of information previously discussed are snippets of what is available. The word 'publish' refers to the information that has been put through 'established channels of dissemination'. For example, any information conveyed by a newspaper article isn't the cessation of it—there subsist facts beyond the ones covered by it. Out of the limited time available for collection and analysis, if the generic collection methodology of 'rag picking' is followed then little time would be left for analysis.

This brings us to 'acquisition'<sup>72</sup> which means acquiring the information, through request or purchase, which others have gathered over time. Thus, instead of sifting through newspaper reports, one should reach out directly to the journalist or newspaper publications—it will be preposterous to develop the expertise the journalist has developed over time. Not only does he/she understand what exists beyond the newspaper article, but additionally the person understands the information landscape he works on. He knows his field better than the intelligence officer does. Most importantly, this eliminates duplicity of information. Thus, instead of wasting time over 'collection', one should focus upon 'acquisition'.

Real OSINT is HUMINT when applied correctly. The 'collector' needs to maintain 'contacts, contracts and rapports' with those 'who already know'. These are the 'aggregators' of information. Recall the Eight Tribes Concept—the Government, the military and the law enforcement, even when clubbed together, forms only a fraction of the information ecosystem. Every tribe is an expert in its domain and sharing of information is the only way to success.

Figure 13: Perceived v/s. Real OSINT (Acquire, Don't Collect)





Source: Annotated by the Author



Let's clarify this with the help of the following illustrative situation:

**Mission Statement: To Understand Chinese Stealth Technology including Plasma.**<sup>73</sup>

<b>Collections Approach</b> 	<b>Acquisitions Approach</b> 
<p>1- Search on the internet.</p> <p>2- Read and collect articles from Chinese newspapers and media.</p> <p>3- Collect info from research papers.</p> <p>4- Listen to podcasts and radio.</p> <p><b>Fuse everything and make motley.</b></p> <p><b>(useless)</b></p>	<p>Approach a University student, fluent in Mandarin, to provide a crisp report on Chinese stealth tech along with photos and graphs<sup>74</sup>.</p> <p>(Illustrative, suggestive of the need for expertise. One can also reach a company dealing in such tech).</p>

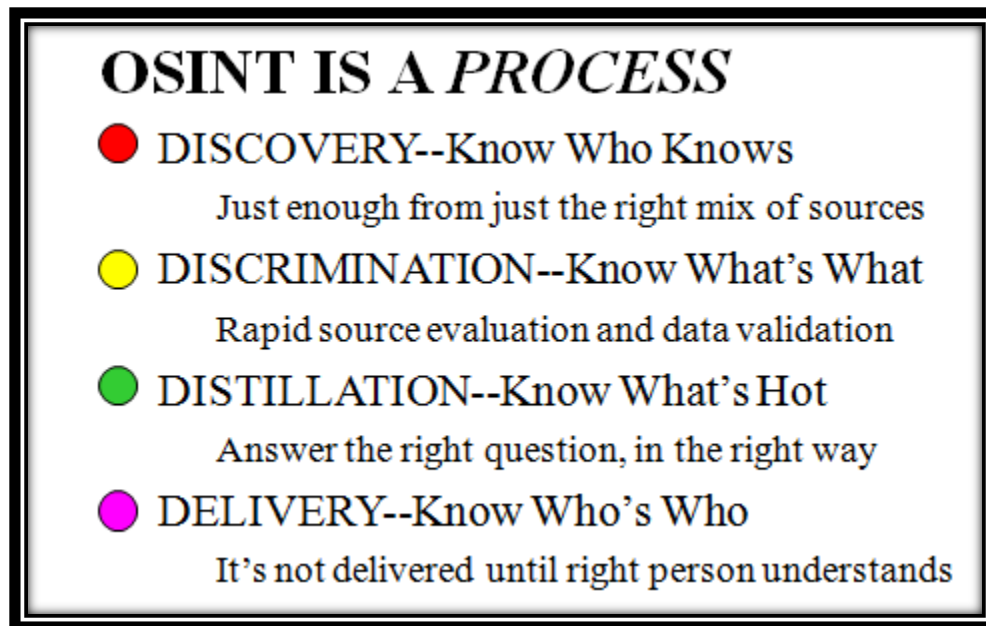
Dr. Stevan Dedijer, the Father of Business Intelligence, summarised it in three simple words—<sup>75</sup> “*Know Who Knows*”. Surprisingly, this was back in 1992 during the first OSS Conference. He had correctly predicted that, it would be impossible to consume and know everything. Instead, one needs to bring into the loop, the person who knows what you are trying to know.

OSINT does not mean the following:<sup>76</sup>

- OSINT is not the internet (discussed later).
- OSINT is not academic research.
- OSINT is not think-tank product.
- OSINT is not commercial study or market survey.
- OSINT is also not Commander Biography.

The following graphic (**Figure 14**) sums the core philosophy of 'OSINT Done Right'.

**Figure 14: OSINT Process**<sup>77</sup>



The acquisition doctrine mainly follows three steps:<sup>78</sup>

- **'Find'** the information for free if you know it.
- **'Get'** the information for free from your allies.
- **'Buy'** the information if you cannot get it for free.
- **'Task'** the classified collectors as the last measure.

### **The Internet is Not OSINT**

The HUMINT nature of OSINT—the most important characteristic of it— is also the most discarded and discredited aspect. The internet proliferated in the 90s. Over-dependence on the internet overshadowed the analogue sources<sup>79</sup> of information. The internet is now filled with poorly drafted and hastily curated directories containing long lists of 'important websites', good enough to write an average research paper but useless for OSINT— 'Internet is a medium of communication and not a source of information'. Information is not produced online; it is put online to be conveyed.

The internet is a minute directory (almost negligent) of snippets of information available offline. Understand it like this:

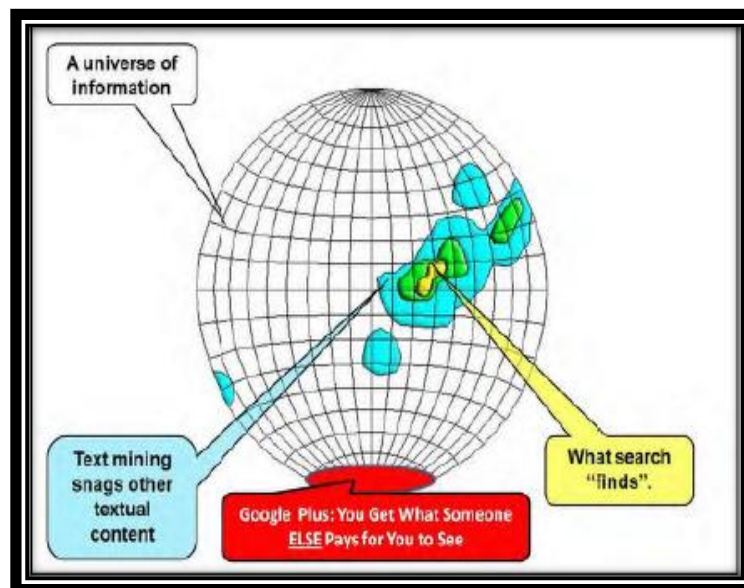
- Internet is 1 per cent of what is known.<sup>80</sup>
- This 1 per cent is severely fragmented and un-indexed. (Refer **Figure 15**).

The Surface Web is what a search engine provides us. A search engine is ‘a crawler or a spider’ that search websites for new content. The websites have a “robots.txt” file that limits the extent to which these crawlers can penetrate to index the contents.<sup>81</sup> Understand it otherwise— the absence of such crawlers would make content that is paid or restricted, open to the public. Typically, this ‘un-indexed’ comprises the Deep Web. Searching this content requires manual searches. Such content forms about 95 per cent of the total content.

The search engines further complicates the situation. Even the best search engine can search, at best, 4 per cent of the 5 per cent of Surface Web.<sup>82</sup>

A typical search query displays results that either someone else has paid for you to see or it displays what people generally like—search engines can easily manipulate the results they display. Refer to the following **Figure 15**.

**Figure 15: Internet is ‘Useless’ for OSINT**



Internet search results suffer from the ‘Echo Effect’<sup>83</sup> i.e. same piece of information is made available on different websites, often the paraphrased versions of the original one. Further, there exist no entry barriers to publishing information over the internet, therefore adding unnecessary noise to the information.

The Dark Web is the ‘impenetrable layer’ of the internet. It is used as a means of communication rather than as a media of information. Websites are temporarily set up—their URLs are conveyed offline and disposed of later. To control crime over the Dark Web, it is important to ramp up HUMINT and not TECHINT.

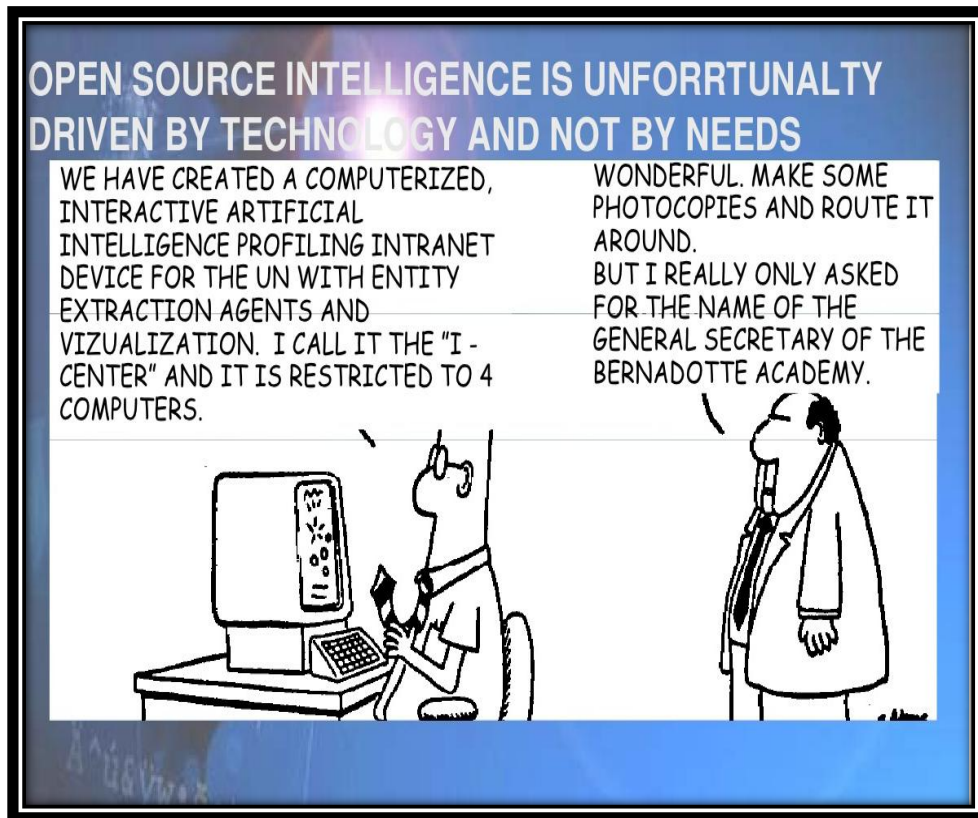
Figure 16: Layers of the Internet



The internet, on the other hand, is an excellent medium for communication. It enables to carry out Citation Analytics i.e. measuring the relative importance of an author or an article by counting the number of times that author or article has been cited in other works or by other authors.<sup>84</sup>

The following picture (**Figure 17**) sums the misnomers surrounding OSINT. Use the right technology, use it rightly and don't exclusively depend on it.

**Figure 17: The Picture Sums It Up<sup>85</sup>**



## The Indian Context

OSINT has not been institutionalised in India. The All India Radio Monitoring Service (AIRMS)<sup>86</sup>, headquartered in Shimla was tasked with monitoring non-encrypted broadcasts from Pakistan, Afghanistan, Bangladesh, Sri Lanka and China, similar to what the FBIS did. AIRMS was also tasked with radio interception during military operations.

Information on Indian intelligence agencies are rare.<sup>87</sup> It is redundant to mention the details of the agencies involved in what might be called as an 'intelligence-investigation mix'.<sup>88</sup> Based on a report titled "A Case for Intelligence Reforms in India" by IDSA<sup>89</sup>, a book titled *Defence Reforms: A National Imperative*<sup>90</sup> and an Observer Research Foundation Issue Brief titled "India's Intelligence Agencies: In Need of Reform and Oversight"<sup>91</sup> the following observations tries to sum up the deficiencies in the intelligence infrastructure of India:<sup>92</sup>

- **Absence of Necessary Intelligence.** No intelligence on Chinese intentions in Tibet (The Chinese had weak Airpower, and a timely strike during the 1962 War could have turned tables). Similarly, no intelligence was present on the 1965 infiltration of the Pakistan Army personnel disguised as civilians and similar infiltrations during the Kargil war. Pakistan's nuclear programme was not properly covered.
- **Growing Unpopularity of Sheikh Mujibur Rahman in West Pakistan.** Links between the Pakistani intelligence and the Phizo.
- Inadequate and inaccurate intelligence on Rajiv Gandhi's assassination and the movement of 12 Naga groups to Yunnan.
- The Indian Peace Keeping Force (IPKF) was not provided by timely assessments and maps of the theatre of operations were made available by the Research and Analysis Wing (R&AW) to the Forces.
- The growth of Sikh Separatist Movements and the volume of arsenal inside the Golden Temple were inadequately assessed by the agencies.

## Assessing the Deficiencies

The same sources confirm the existence of the following main deficiencies:

- **Our HUMINT Network Is Weak.** This has been reiterated by the Kargil Review Committee Report. We needed more penetration into the Pakistan Army but we lacked. Extra reliance is paid to TECHINT, often at the expense of HUMINT. HUMINT is typically the only way out in highly denied areas like the Naxal hit areas. GEOINT/IMINT cannot penetrate the canopy.
- **The Agencies are Not Interconnected and Does Not Synchronise their Operations.** The reports mention the tussles between the Aviation Research Centre (ARC) and the National Technical Research Organisation (NTRO) over asset distribution.

- ***The Distribution of Resources is Highly Unequal.*** The IDSA book observes that the Military has the biggest and the best pool of talented men with varied lingual and technical skills that is hardly put into use as HUMINT is generally done by civilian-manned agencies.
- ***Lack of Clear-Cut Requirements From the Customers.*** If this step is not executed properly then the whole intelligence cycle loses track.
- ***Lack of a Clear-Cut Organisational Structure.*** The R&AW serves the Cabinet Secretariat; the IB reports to the Home Minister. Four Ministries vis. Home, Defence, Finance and Information & Broadcasting along with the Cabinet Secretariat are responsible for intelligence. This disrupts the information flow and much-needed synchronisation. Lack of pyramidal structure results in multi-point decision-making even on the same issue.

For example, in the United States Intelligence Community, the President of the US (POTUS) sits at the top. In India, it becomes a multi-ministerial affair and highly bureaucratic.

### **Have We Been Doing OSINT? Have We Been Doing It the Right Way?<sup>93</sup>**

The IDSA Task Force Report, sadly and surprisingly (for it is written by former intelligence officers), gets OSINT wrong at every place wherever mentioned. On page 8, the report places it under the 'Technology Upgrade' section. On page 52, the report mentions 'collation'. Only on page 60, the report gets it somewhat right as it mentions the importance of 'vernacular publications' and asserts the importance of different databases. commercially available, but it gives unnecessary emphasis on search engines. Surprisingly, Open Source Information and Open Source Intelligence are both abbreviated as OSINT twice. This cannot be considered as a typing error. The report does not record the HUMINT nature of OSINT. The ORF Report, on the other hand, observes that R&AW relies too much on TECHINT and OSINT rather than on HUMINT contradicting what the IDSA report points out. This is a sorry state of affairs. The latest of all is an article titled "The Rise of Open Source Intelligence: Impact to the Security and Public Discourses"<sup>94</sup> dated 28 December 2020 The article discusses only the pretentious OSINT handles over Twitter. Here too, the writer is ignorant of the veracity of information and believes in whatever is published online.

### **Understanding 'Institutionalisation of OSINT'**

The Institutionalisation of OSINT refers to the process of formally recognising it as a separate INT discipline and utilising it as the base for 'All-Source Analysis'.

Ideally, OSINT should be done by a separate OSINT Agency. An Open Source Agency (OSA) is a legal and ethical intelligence-gathering and decision-support organisation, relying exclusively on sources and methods that are open<sup>95</sup> and has the following characteristics:

- It communicates, in real-time, with the Eight Tribes.
- The acquisition of information is decentralised.

- It is independent of other intelligence agencies.
- It directly supports the decision-maker and the agencies doing all-source analysis.
- It is free from bureaucratic channels and red-tapism.

### **Where should it be placed in the National Intelligence Infrastructure?**

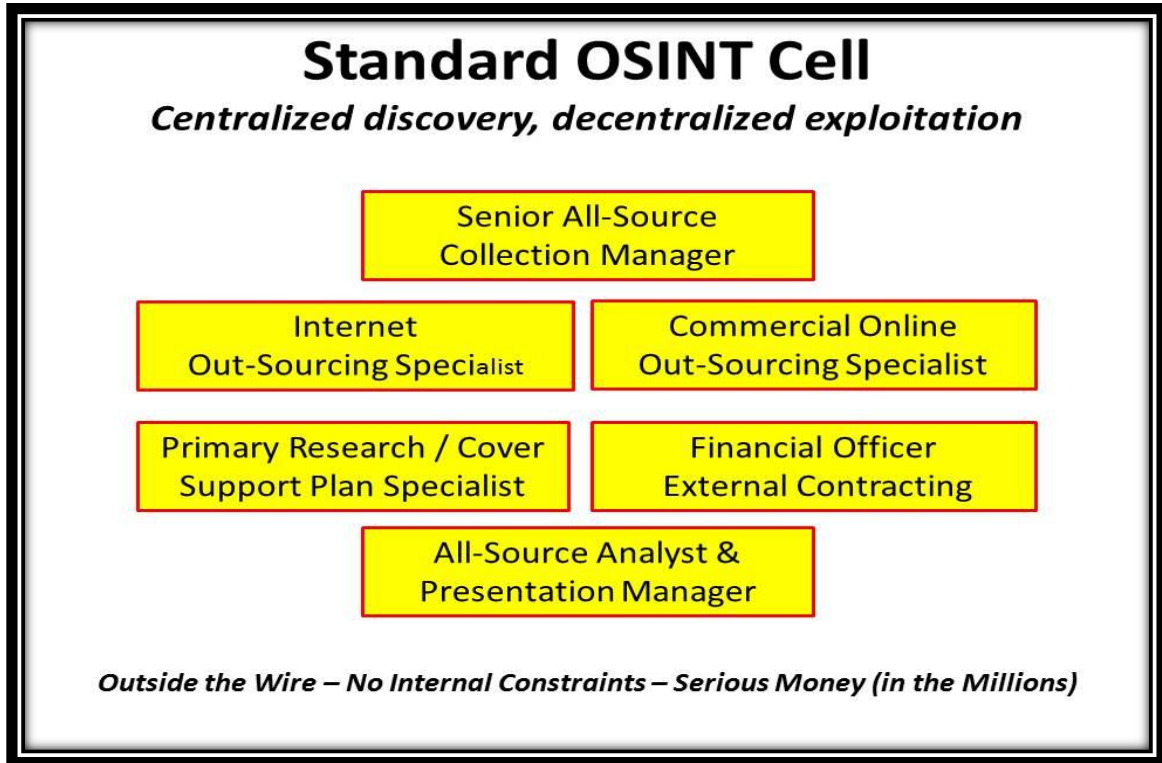
BrigadierGeneral James Cox rightly observed – *“If I was (sic) king of the world, I would build an OSINT organization to rival existing national SIGINT organizations {CSEC in Canada, NSA in (sic) US} and HUMINT organizations (CSIS in Canada, CIA in (sic) US). This OSINT organization would be in a number of big buildings around the country, tapped into all the sources you have long written about (media, experts, academia ... all tribes) AND they would produce magnificent ‘single source’ OSINT products that could be added to SIGINT, HUMINT, IMINT etc. products at the national level”*.<sup>96</sup>

He stressed on the presence of the ‘Generic OSINT Cell’ that can be possibly integrated into ‘any’ institution whether it is a University, Police Station or even a Ministry. This OSINT Cell can be presented in the following figure. Mandates of each of the six members are given below:

- The Internet Outsourcing Manager is to hire the right people. He is an expert in internet searches and Citation Analytics. He hires people who are subject matter experts and skilled at using multiple forms of search.
- The Commercial Online Outsourcing Specialist brings into loop people and organisations that render information services like online database companies, freelance journalists, private investigators and academics. He also hires language experts and subject matter experts and people who know the local conditions. All such people can be hired as short-term consultants for a specific need.
- The PrimaryResearch Specialist brings meaning to the Citation Analytics results and develop human networks ‘on-the-fly’ and rapidly survey the human domain of the society.
- The Financial Officer rapidly makes payments to those who render information. He uses conventional and unconventional, methods of payments—ranging from cash to even Debit Card, Online Transfers etc.
- The Senior AllSource Collection Manager and the All Source Analyst are to collect and analyse respectively. They do the ‘OSINT-V’ step. They do ‘All-Source Analysis’.



Figure 18: The Generic OSINT Cell<sup>97</sup>



This Generic OSINT cell constantly communicates with the Eight Tribes and also with other OSINT Cells. This brings us to two important points:

- **Communications.** General AI Grey gave the following quote:  
*“Communications without intelligence is noise: intelligence without communications is irrelevant”.*<sup>98</sup>

The IDSA Report points out that on some occasions, one agency had the information but it was not conveyed to another agency that needed it, due to absence of subsisting channel of communications. One agency develops a fiduciary relationship with its asset and out of the desideratum to not blow its cover, it is compelled to keep it secret. OSINT eliminates this trepidation as the source is public and sharing the source won't jeopardise security.

We have the expertise that can develop solutions for collaboration and communications. The Centre for Development of Advanced Computing (C-DAC) developed the SAI application that allows secure communication for soldiers.<sup>99</sup> C-DAC is also known to develop software by utilising available open source codes.

- **Sharing and Collaboration.** Tom Atlee, the Guru of Collective Intelligence notes: “Quite simply, secrecy impedes dialogue and the flow of information, without which collective intelligence of any type is impossible. Unnecessary secrecy will prove to be the security bars on the window that prevent us from escaping the burning house”.<sup>100</sup>

**Figure 19: OSINT Cell in Action**

**OSINT Cell In Action: How It Is To Be Done?**

Clarify with the help of the following illustration:

A Battalion Commander in Kashmir requires the tactical map of an area, which is a possible hideout for terrorists. The forces have no tactical maps of the area. The blueprint of the suspected house would be even better.

- **Battalion Commander to the OSINT Cell:** I need the tactical map of area ‘X’.
- **OSINT Cell to the Block Level Development Officer:** Provide the latest survey maps of the area(The BDOs have detailed maps of their respective areas).

The OSINT Cell gets the map and sends it to the Battalion Commander.

For any given topic, the Cell must be able to bring into loop the following people/ institutions:<sup>101</sup>

- Local Academia that knows or writes in the vernacular language.
- NGO heads and workers.
- Religious leaders.
- Businessmen of the area.
- Government officials and the police department.
- Media, Journalists including freelancers.

- University students.
- Research Institutions.

## Recommendations and Way Forward

- **Get the Definition Right and Develop Consensus.** A deeper study of the American efforts to define and understand OSINT shows that different American Intelligence Community (IC) members have a different definition of OSINT— there was no consensus on its definition, scope, role and functions. Real OSINT acquires the information that can be legally acquired. Paradoxically, an Al-Qaida manual released observed –“....*openly and without resorting to illegal means, it is possible to gather at least 80% of (sic) information of the enemy*”.<sup>102</sup>
- **Draft a White Paper.** The White Paper should outline and address the current problems and ascertain the place wherein OSINT should get in the Intelligence infrastructure of the country. Excerpts should then be placed in the open domain and expert comments must be allowed.
- **Learn From The NATGRID Experience.** The National Intelligence Grid (NATGRID) could not succeed due to bureaucratic fiefdom.<sup>103</sup>
- **Connect the Eight Tribes.**<sup>104</sup> The real potential is in the room and not in the individuals in the room. A communication network connecting the Information Commons should be set up.
- **Engage the Embassies.**<sup>105</sup> Diplomatic Missions and Embassies can be harnessed as excellent centres for OSINT. The Defence Attaches can provide their leadership. The Embassies are able to develop more contacts as lesser interaction barriers exist. Developing brutal OSINT capabilities in our embassies in China, Pakistan, Nepal, and Sri Lanka etc. would give us an advantage. OSINT operations will not raise alarms.
- **Conduct OSINT and Juxtapose.** Conduct OSINT on previously answered requirements and then check yourself that to what extent closed sources have been unable to address the decision making. This will help in understanding potential OSINT applications of our interest.
- **Theatre Level OSINT (Clear Advantage over China).** The US and Japan together runs the Asian Studies Detachment (ASD)— a theatre level OSINT office located in Japan. It is managed by the personnel of both countries and provides tailored OSINT at the

theatre and national levels to both the countries<sup>106</sup>. We must integrate OSINT as a separate INT discipline dedicated to a particular target. For instance, in case of China, theatre level OSINT should bring into loop expert individuals and the private sector, not only from India but also from Japan, South Korea, Taiwan, Vietnam and Australia.

- **Understand the Importance of Languages. Robert** Steele did an analysis of all terror promoting websites and found that, terror outfits around the globe used 31 main languages (and 131 others).<sup>107</sup> Misconception is that, every piece of information is available in English or Spanish. Contrarily, the following languages were found to be equally important: Arabic, Aramaic, Berber, Catalan, Chinese, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish, Urdu.<sup>108</sup> Luckily, the military has personnel capable of speaking and writing the 22 official languages. Thus, instead of recruiting or outsourcing translations, the military can do in-house OSINT to an appreciable extent.
- **The Military to Lead.** The military has a vast pool of officers who speak different languages, have different skillsets and are highly organised and disciplined. Its intelligence apparatus has a clear cut Command & Control and presence from the Siachen to the cantonments— a perfect setup for pan-India OSINT Cell. It needs to focus on leveraging these capabilities and opportunities.

## Case Studies

Given below are some case studies:

- The author was able to get the generalised versions of the success stories. Minute details and methodologies were confidential:<sup>109</sup>
  - A 100 times increase in illicit wealth confiscation by the Scotland Yard.
  - An Arab terrorist submarine was identified in the shipyard and it was ready for delivery.
  - Russian Military maps were procured overnight.
  - Russian tank specifications were made available by a commercial source.
  - Science and Technology(S&T) Overviews for micro-UAVs (Unmanned Aerial Vehicles).

- In the late 1940s, Jawaharlal Nehru and Bertrand Russell asked Prof. Kothari to make a report on the effect of nuclear bombing on Japan. The Kothari Report's findings were very close to the closed source findings of the USA.<sup>110</sup>
- The Burundi Exercise<sup>111</sup> was a *pro-bono* exercise, after the Aspin-Brown Commission work that was undertaken by Open Source Solutions Inc. The aim was to show the utility of OSINT vis-à-vis other INTs. Burundi was not a country of interest for the USIC though they had some previous information on it. On the other hand, Steele, who was tasked with conducting this trial, had no prior experience in Burundi.<sup>112</sup> He was given four days to collect information on Burundi. However, he provided the government with the following:
  - From Lexis-Nexis, a list of top ten journalists covering the genocide in Rwanda and Burundi, all available for debriefing.
  - A list of 100 experts from worldwide, on Burundi situation, available for immediate debriefing and also helpful in identifying other such experts, from the Institute of Scientific Information.
  - Reports from Oxford Analytica having summaries of the situation in Burundi about the risks, UN Operations, and US Foreign Policy objectives or lack thereof.
  - From Janes Information Group, a complete story of all publication of Janes' on Burundi and a series of one-page tribal "orders of battle", essentially describing tribal leadership, tribal manpower, and tribal capabilities including what are called "technicals" or normal small trucks with mounted machine-guns (this one was an exclusively created product).
  - From East View Cartographic, 1:1,50,000 maps for tactical military and humanitarian operations.
  - From SPOT Image, commercial imagery, all cloud-free and less than three years old.

In contrast, the CIA had provided an old map of Burundi and an outdated economic study. The National Security Agency (NSA) and the National Geospatial-Intelligence Agency (NGA) had nothing.<sup>113</sup>

## **Conclusion**

OSINT, if done correctly, can prove to be a vital solution to the deficiencies discussed. Diluting the HUMINT base of OSINT makes it a 'featherless bird' expected to 'fly like an eagle'. OSINT is

acquired through human-to-human contact. The future of OSINT in India is dependent on the manner it is institutionalised. Incessant research, optimal budgeting and felicitous resource allocation must be the guiding principles of OSINT in India. The Armed Forces have clear-cut advantage over their civilian counterparts. Subsisting HUMINT channels are to be exploited by the time an OSA is established.

It is consequential that the regime realises that it no longer controls the flow of information. Rather, it is a net acceptor of information. The regime engenders negligible information. In contrast, it requires voluminous quantities of it for decision making. The cognisance lies 'in the room and not in the people who are inside it'. You require to "Know Who Knows".

---

*Disclaimer: The views expressed and suggestions made in the Issue Brief (s) are solely of the author(s) in his/her personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author. The contents of this paper are based on the analysis of materials accessed from open sources. The contents, therefore, may not be quoted or cited as representing the views or policy of the Government of India, or Integrated Headquarters of the Ministry of Defence (MoD) (Army), or the Centre for Land Warfare Studies. The photographs used on the cover are all from open sources and CLAWS does not claim copyright of the same.*

## End Notes

---

<sup>1</sup> Robert David Steele, *Handbook of Intelligence Studies*, Ed, Loch K. Johnson, (New York, Routledge, 2007), Page no 129 (Robert David Steele).

<sup>2</sup> United States, "US Army Field Manual Interim" 2-22.9 *Open Source Intelligence* (Washington DC: United States, 2006).

<sup>3</sup> United States, US Army, *Army Techniques Publication 2.22-9* (Washington DC: US, 2017).

<sup>4</sup>N.1.

<sup>5</sup> North Atlantic Treaty Organisation (NATO) *Open Source Intelligence Handbook* (NATO, 2001).

<sup>6</sup> "Office of the Director of National Intelligence", *National Open Source Enterprise* (United States). Available at-<https://fas.org/irp/dni/osc/nose.pdf>.

<sup>7</sup>Susan B Glasser, "Probing Galaxy of Data for Nuggets", *Washington Post*, 25 November 2005.

<sup>8</sup> Cranfield University, Defence College of Management and Technology, "Open Source Intelligence: A Contemporary Timeline" (Cranfield University, 2007).

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> US Navy, Naval Postgraduate College, "Non-traditional Forms of Intelligence" (California: US Navy, 1993)

<sup>12</sup> Hamilton Bean, "No More Secrets: Open Source Information and the Shaping of US Intelligence", (Praeger Security International, 2011).

---

<sup>13</sup> N.1.

<sup>14</sup> Email Correspondence with Mr Robert David Steele. Excerpts publicly available at- <https://phibetaiota.net/2020/12/answers-on-osint-for-india-18-why-does-information-exist-the-death-of-knowledge-video-with-stephen-e-arnold/>.

<sup>15</sup> Ibid.

<sup>16</sup> Email Correspondence with Mr Robert David Steele. Excerpts publicly at- <https://phibetaiota.net/2021/01/answers-on-osint-for-india-39-how-are-open-and-closed-sources-related/>.

<sup>17</sup> Robert David Steele, "1993: Theory and Practice of Intelligence in the Age of Information", Open Source Solutions, Inc, (Sept 17, 1993).

<sup>18</sup> "Graphic: OSINT All Source-Temple, Phibetaiota", <https://phibetaiota.net/1994/08/graphic-osint-all-source-temple/>, accessed on December 30, 2020).

<sup>19</sup> Email Correspondence with Mr Robert David Steele

<sup>20</sup> N.12.

<sup>21</sup> Florian Schauer and Jan Störger, "The Evolution of Open Source Intelligence (OSINT)", *Journal of US Intelligence Studies*, Volume 19, Number 3, Winter/Spring 2013, [https://www.afio.com/publications/Schauer\\_Storger\\_Evo\\_of\\_OSINT\\_WINTERSPRING2013.pdf](https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf).

<sup>22</sup> Made by the Author.

<sup>23</sup> "Key Events in CIA's History", *Federation of American Scientists*, <https://fas.org/irp/cia/product/fact97/keyevent.htm>, accessed on January 10, 2021.

<sup>24</sup> Ibid.

<sup>25</sup> Ibid.

<sup>26</sup> Central Intelligence Agency, Foreign Broadcast Information Service, History: Part I: 1941-1947(Washington DC: CIA, 1969).

<sup>27</sup> Ibid.

<sup>28</sup> Romanian Intelligence Service, *OSINT Handbook*, (Budapest: Romanian Intelligence Service).

<sup>29</sup> Ibid.

<sup>30</sup> N.12.

<sup>31</sup> Ibid.

<sup>32</sup> National Defence University, National War College, "The Generation Gap: Open Source Information, Intelligence and the Government" (Washington DC: NDU, 1994).

<sup>33</sup> Robert David Steele, *Open Source Everything Engineering Manifesto*, (California: Evolver Editions, 2012).

<sup>34</sup> N.1,

<sup>35</sup> OSINT: Issues for the Congress.

<sup>36</sup> N.12.

<sup>37</sup> N.12.

<sup>38</sup> N.12.

<sup>39</sup> N.12.

<sup>40</sup> Steven Aftergood, "Open Source Centre (OSC) Becomes Open Source Enterprise (OSE)", *Federation of American Scientists*, 28 October 2015, <https://fas.org/blogs/secrecy/2015/10/osc-ose/>.

<sup>41</sup> Login Page, Open Source Center, <https://web.archive.org/web/20130216183901/https://opensource.gov/public/content/login/login.fcc->

<sup>42</sup> Eric Rosenbach and Aki J Peritz, "Intelligence Basics", *Belfer Center for Science and Intelligence Affairs*, <https://www.belfercenter.org/sites/default/files/legacy/files/intelligence-basics.pdf>.

<sup>43</sup> Ibid.

- 
- <sup>44</sup> “Measurement and Signature Intelligence (MASINT), Federation of American Scientists, <https://fas.org/irp/program/masint.htm>.
- <sup>45</sup> Email correspondence with Mr Robert David Steele ( 25 November 2020). Excerpts publicly available at- <https://phibetaiota.net/2020/11/answers-on-osint-for-india-6/>.
- <sup>46</sup> Email correspondence with Mr Robert Steele. Excerpts publicly available at- <https://phibetaiota.net/2020/11/answers-on-osint-for-india-14/>.
- <sup>47</sup> Email correspondence with Mr Robert David Steele.
- <sup>48</sup> Robert David Steele, *Human Intelligence: All Humans, All Minds, All the Time*, (US Army War College, 2010), <https://phibetaiota.net/2011/11/reference-human-intelligence-humint-all-humans-all-minds-all-the-time-full-text-online-for-google-translate/>.
- <sup>49</sup> Ibid.
- <sup>50</sup> Requirements, Collection, and Current Awareness: The Human Dimension, Open Source Solutions Inc.
- <sup>51</sup> Ibid.
- <sup>52</sup> Ibid.
- <sup>53</sup> Mark M Lowenthal, “OSINT: The State of the Art, The Artless State”, Central Intelligence Agency, <https://www.cia.gov/readingroom/document/0006122548>.
- <sup>54</sup> Ibid.
- <sup>55</sup> Graphic: OSINT Baseball, Phibetaiota, <https://phibetaiota.net/2008/08/graphics/>.
- <sup>56</sup> N.33.
- <sup>57</sup> Ibid.
- <sup>58</sup> Email Correspondence with Mr Robert David Steele. Excerpts publicly available at- <https://phibetaiota.net/2020/11/answers-on-osint-for-india-8/>.
- <sup>59</sup> N.1.
- <sup>60</sup> This term was coined by Dr Joseph Markowitz, the then Director of COSPO- Community Open Source Program Office. The term lays down the foundation of an OSINT included ‘All-Source Analysis’ of Intelligence.
- <sup>61</sup> N. 59.
- <sup>62</sup> E Ben Benavides, “Open Source Intelligence (OSINT) 2oolKit On The Go”, <https://osint.co.nz/wp-content/uploads/2018/09/2016-OSINT-2oolKit-Benavides.pdf>.
- <sup>63</sup> Arno H.P. Reuser, The RIS Open Source Intelligence Cycle, (Journal of Mediterranean and Balkan Intelligence), (Volume 10 no 2), (December 2017); pp. 29-44.
- <sup>64</sup> Ibid.
- <sup>65</sup> Open Source Center (OSC), A Master Narratives Approach to Understanding Base Politics in Okinawa, (Open Source Center, 2012).
- <sup>66</sup> Available at <http://www.intelligence101.com/an-introduction-to-the-intelligence-cycle/>.
- <sup>67</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at- <https://phibetaiota.net/2020/11/answers-on-osint-for-india-15/>.
- <sup>68</sup> Eight Tribes, Phibetaiota, <https://phibetaiota.net/wp-content/uploads/2013/01/IADB-Eight-Tribes-and-Commons.jpg>.
- <sup>69</sup> A Very Long List of such items is available at- <https://phibetaiota.net/2012/12/chris-pallaris-mindmap-table-of-indirect-open-sources/>.
- <sup>70</sup> North Atlantic Treaty Organisation, NATO Open Source Intelligence Reader (NATO, 2002).
- <sup>71</sup> Best example can be the Bombshell Magazine published by the National Bomb Data Centre (NBDC) of the National Security Guards (NSG).
- <sup>72</sup> Email Correspondence with Mr. Robert David Steele.
- <sup>73</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly, <https://phibetaiota.net/2021/01/answers-on-osint-for-india-31-osint-primer-for-spies/>.
- <sup>74</sup> Email Correspondence with Mr. Robert David Steele.
- <sup>75</sup> Email correspondence with Mr. Robert David Steele. Excerpts publicly available at- <https://phibetaiota.net/2021/01/answers-on-osint-for-india-41-training/>.



---

<sup>76</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at-  
<https://phibetaiota.net/2020/12/answers-on-osint-for-india-28-what-osint-is-not/>.

<sup>77</sup> Email Correspondence with Mr. Robert David Steele.

<sup>78</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at-  
<https://phibetaiota.net/2021/01/answers-on-osint-for-india-38-osint-is-acquisition-not-collection/>.

<sup>79</sup> 'Analogue' information is the information that is offline and includes the information that is in digital format but is not put online or is not meant to be put so.

<sup>80</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at-  
<https://phibetaiota.net/2020/12/answers-on-osint-for-india-26-the-internet-is-not-osint/>.

<sup>81</sup> Nihad A. Hassan and Rami Hijazi, *Open Source Intelligence Methods and Tools A Practical Guide to Online Intelligence*, (New York: Apress, 2018).

<sup>82</sup> The figure is further reduced when a user searches on complicated topics relating to National Security because information on such topics is simply not meant for general consumption.

<sup>83</sup> United States, Congressional Research Service, *Open Source Intelligence: Issues for the Congress*, (United States, 2007)

<sup>84</sup> Scholarly Impact and Citation Analysis, Wooster Campus Research Library,  
[https://osu.libguides.com/oardc/citation\\_analysis/whatis#:~:text=Citation%20analysis%20is%20a%20way,been%20cited%20by%20other%20works.](https://osu.libguides.com/oardc/citation_analysis/whatis#:~:text=Citation%20analysis%20is%20a%20way,been%20cited%20by%20other%20works.)

<sup>85</sup> Mats Björe, "Reinventing Open Source Intelligence: A catalyst for change and sharing", Infosphere,  
<https://www.slideshare.net/mumlan/14-mar-2007-osint-presentation>.

<sup>86</sup> The Australian National University, Strategic and Defence Studies Centre, *Signals Intelligence (SIGINT) in South Asia*, (Canberra: Australia, 1992).

<sup>87</sup> Paradoxically our democratic setup requires transparency and proper oversight. Almost all of our intelligence agencies are setup through Executive Orders and not by Parliamentary laws.

<sup>88</sup> Agencies like the Intelligence Bureau do intelligence, as well as, investigation. Example, IB is tasked with doing background checks on the applicants for Amateur Radio license.

<sup>89</sup> IDSA Task Force Report, *A Case for Intelligence Reforms in India*, (Delhi: India, 2012), Available at-  
[https://idsa.in/system/files/book/book\\_IntelligenceReform.pdf](https://idsa.in/system/files/book/book_IntelligenceReform.pdf)

<sup>90</sup> Kamal Davar, *Defence Reforms: A National Imperative*, Ed. Gurmeet Kanwal and Neha Kohli, (New Delhi: Pentagon Press, 2018) Page no- 109 (Kamal Davar)

<sup>91</sup> Manoj Joshi and Pushan Das, "India's Intelligence Agencies: In Need of Reform and Oversight", ORF Issue Brief, No 98, (2015), [https://www.orfonline.org/wp-content/uploads/2015/07/IssueBrief\\_98.pdf](https://www.orfonline.org/wp-content/uploads/2015/07/IssueBrief_98.pdf), accessed on- Nov 30, 2020

<sup>92</sup> These two books and the report sum up almost every important aspect of our intelligence agencies. Also presently, these documents are the best public documents that discuss OSINT. The choice has been made carefully after sifting through many articles, reports and books.

<sup>93</sup> Readers are requested to recall the section on "Perceived v/s. Real OSINT".

<sup>94</sup> Thejus Gireesh, "The Rise of Open Source Intelligence: Impact to the Security and Public Discourses", *Centre for Land Warfare Studies (CLAWS)*, 28 2020, <https://www.claws.in/the-rise-of-open-source-intelligence-impact-to-the-security-and-public-discourses/>.

<sup>95</sup> Open Source Intelligence Requires an Open Source Agency, Phibetaiota, Obtained from Mr. Robert David Steele.

<sup>96</sup> 2013 BGen James Cox, CA (Ret) On the Record on Open Source Information versus Open Source Intelligence versus Secret Intelligence, Phibetaiota, <https://phibetaiota.net/2013/02/bgen-james-cox-ca-ret-on-the-record-on-open-source/>.

<sup>97</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at-  
<https://phibetaiota.net/2021/01/answers-on-osint-for-india-41-training/>.

<sup>98</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at-  
<https://phibetaiota.net/2021/01/answers-on-osint-for-india-35-should-osint-technical-be-separate-from-osint-analysis/>.

---

<sup>99</sup> ANI, “Indian Army Launches Indigenous Messaging App SAI, Similar to WhatsApp”, *NDTV*, 30 October 2020, <https://gadgets.ndtv.com/apps/news/indian-army-sai-whatsapp-messaging-app-secure-application-internet-2317894>.

<sup>100</sup> Tom Atlee, “Beyond Intelligence Reform: Shifting From Intelligence to Co-Intelligence”, Paper Presented to Open Source Solutions, Inc, 16 April 2004.

<sup>101</sup> Email Correspondence with Mr. Robert David Steele. Excerpts publicly available at <https://phibetaiota.net/2020/12/answers-on-osint-for-india-22-offline-osint/>.

<sup>102</sup> The Al Qaeda Manual at Page 80, [https://fas.org/irp/world/para/manualpart1\\_3.pdf](https://fas.org/irp/world/para/manualpart1_3.pdf).

<sup>103</sup> Vinay Kaura, “Too many spies spoil the intelligence broth”, *Livemint*, 17 May 2017.

<sup>104</sup> NGOs and Civil Societies can be grouped together.

<sup>105</sup> OSCOL, Central Intelligence Agency, <https://www.cia.gov/library/readingroom/docs/CIA-RDP90-00509R000100030001-3.pdf>.

<sup>106</sup> N.2.

<sup>107</sup> Robert David Steele, “Presentation on Open Source Intelligence by Robert David Steele”, 21 April 2016, Forsvarsakademiet, <https://www.youtube.com/watch?v=p9qLISSHo7I>.

<sup>108</sup> 2017 Robert Steele: OSINT Done Right, Phibetaiota, <https://phibetaiota.net/2016/02/2016-robert-steele-on-osint-why-and-how/>.

<sup>109</sup> Email correspondence with Mr. Robert David Steele. Excerpts publicly available at <https://phibetaiota.net/2020/12/answers-on-osint-for-india-29-case-studies-persuading-a-station-head-to-use-osint/>.

<sup>110</sup> Stevan Dedijer, “Intelligence and Secrecy”, Paper presented for the Proceedings of the Open Source Solutions Symposium, Washington D.C., 01-03 December 1992.

<sup>111</sup> OSS Inc, MEMORANDUM FROM ROBERT DAVID STEELE VIVAS, (United States, 2004)

<sup>112</sup> Email Correspondence with Mr. Robert David Steele.

<sup>113</sup> *Ibid*.

## About the Author



**Amiy Krishna** is a final year student of Law and Management at the Himachal Pradesh National Law University, Shimla. He is also a recipient of Gold Medal in the UN Rio+24 IDRC India Program (2018-19) competition.