**Open Source Intelligence (OSINT)**

**Robert David Steele**

Intelligence is the art and science of evidence-based decision-support. Intelligence is not defined by its inputs (spies, secrecy, money, risk) but rather by its outputs – tailored actionable decision-support. In this context, the fastest, least expensive, and very often the best intelligence is achievable using mostly – and sometime only – open sources and methods.

Open Source Intelligence (OSINT) is the only discipline that is both a necessary foundation for effective classified intelligence collection and analysis, and a full multimedia discipline in its own right, combining overt human intelligence from indigenous observers to international subject matter experts (SME); foreign broadcast and global social media monitoring; and commercial and hobbyist imagery (including humanitarian assistance Unmanned Aerial Vehicles (UAV) and observational balloons).

OSINT is uniquely important and valuable in part because it can easily draw upon the knowledge of everyone outside the national government and in part because it can easily be shared with everyone outside the national government. OSINT is the intelligence discipline most able to support Information Operations (IO) that include public diplomacy, early warning, peacekeeping, stabilization & reconstruction operations and – within the homeland – national education and research as well as acquisition and logistics intelligence.

**OSINT is 80% or More of the Solution**

Below is a table intended to emphasize the importance of OSINT in relation to the ten high-level threats to humanity as identified and prioritized in 2004 by the United Nations High-Level Panel on Threats, Challenge, and Change.

**Economic and social threats, including: 95%**

01 Poverty 99%

02 Infectious Disease 95%

03 Environmental Degradation 90%

**04 Interstate Conflict 75%**

**Internal conflict, including: 90%**

05 Civil War 80%

06 Genocide 95%

07 Other Large-Scale Atrocities 95%

**08 Nuclear, radiological, chemical, biological 75%**

**09 Terrorism 80%**

**10 Transnational Organized Crime 80%**

It is not possible to over-state the importance of OSINT to doing serious intelligence (decision-support) for strategy, for policy, for acquisition, and for operations. I am a former spy – one of the first to be assigned terrorists as a full-time target (in the 1980’s). I will state without equivocation that 90% of US spying is very expensive waste and mostly collects and processes Internet and cellular chatter of no value or human lies that the Americans accept from official and individual sources because the Americans are naïve and out of touch with multi-lingual reality such as OSINT can easily and inexpensively provide.

Below is a graphic illustrating the manner in which the craft of intelligence is evolving.



The aspiring intelligence professional should notice that OSINT offers utility across a much broader range of threats than the traditional focus on threats that are armed with weapons. Indeed, it was the Secure Acute Respiratory Syndrome (SARS) threat in 2002-2003 that led to the realization by the Singapore military and Singapore police that they were responsible for protecting the public from all threats, not just those armed with traditional weapons.

If one recognizes that intelligence should be supporting the entire government (what some call Whole of Government) across all policy domains (including, for instance, Agriculture, Diplomacy, Economy, Education, Energy, Family, Health, Immigration, Justice, Security, Society, and Water) then it becomes clear that the traditional focus on spies and secrecy has been supporting only two of the major policy domains, and neglecting the other ten. OSINT allows for balanced support to all policy domains.

OSINT acquires extra value from being useful in both domestic public dialog and deliberation, and in Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing and Sense-Making (M4IS2). Among the many short-comings of secret intelligence – apart from its often being wrong, late, and expensive – are its restrictions on sharing. To the extent that the secret world shares, it shares bi-laterally, not multilaterally. Smaller countries have much to gain from forming multinational information-sharing and sense-making networks able to analyze Great Power operations – including operations intended to be secret – by sharing source and methods rooted in openness. Much is not all of the public statements of the Great Powers are lies – misrepresentations intended to pacify or arouse their own publics while deceiving other publics. OSINT, shared with one’s own public, is the only antidote to these common international threats, what some have called “weapons of mass deception.”

I like to say that “the truth at any cost lowers all other costs.” Governments and corporations that waste time on the basis of lies from others are incurring substantial costs in lost time and money – and in lost opportunities to challenge these lies from the earliest possible moment.

**Open Sources and Methods**

OSINT is HUMINT – it is *not* Technical Intelligence (TECHINT). As a general statement, less than 10-15% of what we might need to know is to be found on the Internet, and it is often not indexed. By its own admission Google indexes less than 4% of the Internet (I personally think it is less than 2%). Roughly 1% of “Big Data” is actually processed – everything else is stored without being processed. Hence the Internet, while useful as a starting point, is the least important open source.



Everything else – included limited edition localized print publications – is best accessed through specific human beings. In today’s environment where six billion cellular telephones are spread across nine billion people, the trick is, as Stefan Dedijer (Croatia, Sweden) shouted out in 1992, to “know who knows.”

It is now possible to identify, via social media, a specific person standing on a specific street corner in the Ukraine and text them a straight up question and financial offer. Answer this question (or take this photo on this bearing) and get $100 via PayPal. It’s that simple.

The more people know what you are interested in, the more likely they are to call you when they notice something relevant. People are the primary open source as well as the most valuable closed source.

The more information you share, the more likely you will receive ten times more information in return. This was studied by a Hackers Conference in 1994. They concluded that for every piece of information shared, one received 100 pieces of information back, 10 of which were both very valuable, and would never have been noticed by any planned search. So this is a ten to one noise to signal ratio, and a ten to one return on investment. Sharing, not secrecy, is the foundation for 21st Century intelligence.

Put another way: the intelligence professional, whether a collector or an analyst, does not have the possibility of accessing all information in all languages all the time – nor the processing power even if they could.

It is humans who serve as filters, humans who devote decades to being in a local place or studying a specific topic, who have “pre-processed” all relevant information. It is humans who can create new tailored actionable OSINT “in the moment” to serve the needs of the intelligence professional. OSINT is HUMINT.

**OSINT Applications**

Here is a simple illustration of the utility of OSINT at each of the four levels of intelligence analysis:



Too few are conscious of history or regional context. Too few are able to challenge lies in the media or understanding hidden personalities such as billionaires with ties to foreign powers. Too few understand the critical importance of commercial imagery for tactical situational awareness when maps are not available, or the urgency of evaluating all information in all local languages, not only the information available in Russian and English and German, for exampleToo few recognize that buying systems from the Great Powers is a prescription for poverty, completely apart from the likelihood that all systems purchased from Great Powers have “off” switches buried within them, and therefore cannot be trusted if the day comes when the Great Power chooses to invade while neutralizing those systems via a pre-arranged cyber-signal.

A valuable approach to organizing the use of OSINT has been suggested by Mr. Jan Herring, the former National Intelligence Officer (NIO) for Science & Technology at the US Central Intelligence Agency (CIA). He suggests four levels of effort:

* Strategic Warning & Overwatch: 40% of the cost, 10% of the effort
* Operational Special Studies: 30% of the cost, 20% of the effort
* Help Desk Answering Questions on Demand: 20% of the cost, 30% of the effort
* Current Awareness Monitoring: 10% of the cost, 40% of the effort

The point is that OSINT must be managed across requirements definition, collection management, processing, and production. OSINT should be collected on a “just enough, just in time” basis, it should *not* be “vacuum-cleaned.”

***OSINT and the Whole***

This final illustration shows how OSINT supports the Whole.



The key here is the recognition that all aspects of government require intelligence support; that OSINT is the best means of providing tailored evidence-based decision-support to all aspects of government; and that OSINT benefits from – and contributes to – multinational information-sharing and sense-making that can produce multinational decision-support. Europe, for example, desperately needs a European Intelligence and Operations Centre focused on North Africa and the Middle East while a case could also be made for a separate European Intelligence and Operations Centre in Romania focused on the Caucasus and Central Asia. Such centers would be multinational in all respects, and rely largely but not completely on open sources and methods to create multinational intelligence – tailored actionable decision-support.

**OSINT and Intelligence Tradecraft**

For the purposes of this short overview, I will briefly address how OSINT could be – but is not – better managed in collection, processing, and dissemination.

In collection, instead of the normal intelligence cycle (customer to analyst to collector to source and back up again – the linear paradigm) we have the possibility of putting the customer in direct contact with one or more sources who can interact directly with the customer (ideally with the analyst and collector listening and where appropriate interjecting) so that new intelligence – decision-support – is created “in the moment” and perfectly aligned with the customer’s needs – the diamond paradigm.

In processing, we still lack a generic analytic tool-kit with the eighteen functionalities identified in 1989 and illustrated below. Today we know that this analytic tool-kit should be created using open source software and open source hardware accompanied by a global commitment to open cloud, open data, open standards, and open spectrum. This is how we create a larger community able to share information and make sense together, this is how we create a “Smart Nation.” The open source ecology of a Smart Nation is illustrated alongside the analytic tool-kit elements.

|  |  |
| --- | --- |
|  |  |

In dissemination we still lack the means to broadly distribute OSINT to all eight of the “tribes” of information-intelligence at the same time that we lack public policy, public budget, and public “serious game” capabilities that enable us to harness the distributed intelligence of a “Smart Nation.” These two concepts are illustrated below as well.

|  |  |
| --- | --- |
|  |  |

Eventually, as shown in the evolution graphic previously, the intelligence specialist will be at the center of a much larger universe of intelligence nodes spanning all topics, all locations, all organizations – individual citizens will be “intelligence minutemen” as Alessandro Politi of Italy put it so well in 1992 and his later article.

We are at the beginning of a revolution in intelligence affairs; the smaller nations, not the Great Powers, will lead this revolution.

Learn more at <http://www.phibetaiota.net>

**Selected References**

2014 [Applied Collective Intelligence](http://www.phibetaiota.net/2015/01/2014-robert-steele-applied-collective-intelligence/) (*Spanda Journal*)

2014 [On Defense Intelligence – Seven Strikes](http://www.phibetaiota.net/2014/07/2014-robert-steele-on-defense-intelligence-seven-strikes/) (*CounterPunch*)

2013 [The Evolving Craft of Intelligence](http://www.phibetaiota.net/2012/02/preprint-for-comment-the-craft-of-intelligence/) (*Routledge Companion to Intelligence Studies*)

2009 [Human Intelligence: All Humans, All Minds, All the Time](http://www.phibetaiota.net/2011/11/reference-human-intelligence-humint-all-humans-all-minds-all-the-time-full-text-online-for-google-translate/) (US Army War College)

2007 [Open Source Intelligence](http://www.phibetaiota.net/2012/12/open-source-intelligence-strategic-utilidad-osint-estrategico/) (*Strategic Intelligence: The Intelligence Cycle*)

**About the Author**

Robert David Steele, a former spy and honorary hacker, is the founder of the modern Open Source Intelligence (OSINT) movement and the author of the handbooks on OSINT for the North Atlantic Treaty Organization (NATO) and Partnership for Peace (PfP), the Defense Intelligence Agency (DIA), and the Special Forces (SOF). He created the basic OSINT course for the United Nations and is the architect for the United Nations Open-Source Decision-Support Information Network (UNODIN), a proposed multinational endeavor intended to counter the media monopoly of the Great Powers. He is also the #1 Amazon reviewer for non-fiction, reading in [98 categories](http://www.phibetaiota.net/reviews/). Learn more about him and access his body of work at [www.robertdavidsteele.com](file:///C%3A%5CUsers%5CRobertSteele%5CDocuments%5C2015%5C2015%20Conferences%20%26%20Writing%5C2015%20Romania%5Cwww.robertdavidsteele.com).