OSINT 2.0 The Next Generation in Open Source Intelligence

July 2011

iJET®
a 3i-MIND company

OSINT 2.0

Recent History

In 2004, the 9/11 Commission recommended that an open source directorate be established within the Central Intelligence Agency to gather and capitalize on multiple information types from vastly disparate sources, including the Internet, multi-lingual radio, television, global press outlets, publicly accessible databases, geospatial data, photographs and images. Roughly a year and a half later, the Open Source Center was established by the Director of National Intelligence and tasked with widening the search for publicly available information that might head-off the next terrorist attack on U.S. soil and protect national interests abroad. Interest in OSINT has been growing within government agencies and police departments ever since. In fact, for most government agencies, OSINT is becoming a major source of intelligence and is increasingly recognized as a significant contributor to many of today's intelligence challenges.

…

Open Source Intelligence (OSINT) is information collected and analyzed from multiple publicly available sources, including the Internet. Primarily, OSINT includes any subject in any language found anywhere on the Web. But in contrast to common search engines, the information targeted, collected and analyzed by OSINT solutions (lawfully) creates an aggregated, rich, validated intelligence product, including information from social networks, forums and chat rooms.

Traditional OSINT, or OSINT 1.0, relies heavily on the acquisition of raw data, often translations from foreign language sources and from search results produced by Web search engines. Frequently, especially in national security and law enforcement arenas, this simply meant piles of additional information for the analyst to sift through. Faced with a stack of information gleaned through covert efforts and a larger stack of information gathered at little to no cost, traditional analysts have tended to focus on classified or proprietary information that their enterprise risked much or paid dearly for. Unclassified information has traditionally been seen as a high-volume, low-value pool to sift through, if and only if, classified sources are not productive.

The reality is that the Web is not a collection of static pages to be found once one knows where to look. It's a dynamic collection of databases and constantly changing content. In many respects, the Web is a moving target that requires the skills of a sharpshooter. OSINT 1.0 was simply not agile enough. Both evolution and revolution were in order.

The OSINT 2.0 Advantage

Fused Analytical Products & Consolidation

The best of next-generation OSINT tools will deliver fused analytics while consolidating existing automated collection and persistent search methods into fewer and fewer screens, fields and mouse clicks. For investigators, the best new tools offer broader, more relevant link analysis and pattern detection (essentially the revelation of non-obvious connections), as well as rapid corroboration. For those working in classified environments or with proprietary data, OSINT 2.0 products can push intelligence directly into investigators' workflows.

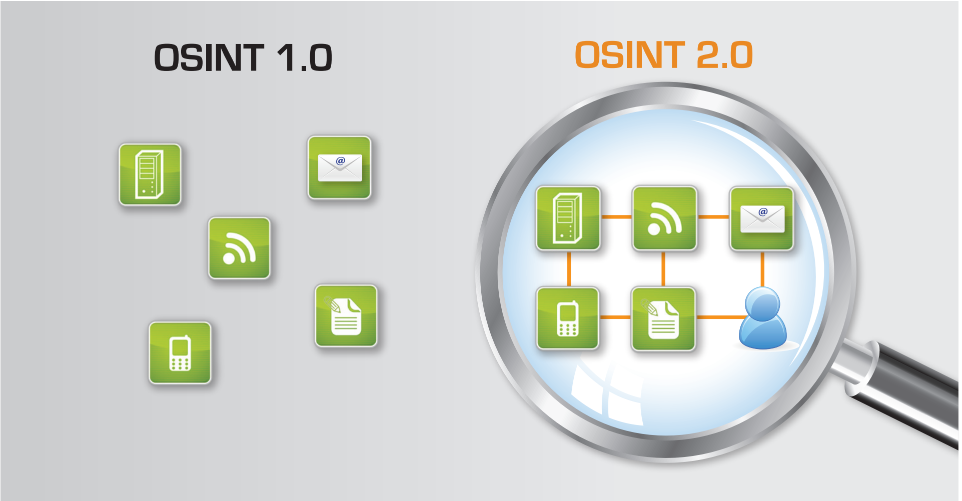
Where OSINT 1.0 focused on the collection of data from unclassified sources, OSINT 2.0 focuses on deriving meaning from those sources. OSINT 2.0 yields mission-specific fused intelligence products based on information from multiple sources and multiple source types. Rather than receiving three translated news articles about a gun battle in Nuevo Leon, Mexico involving the Zetas cartel (raw data), OSINT 2.0 will provide an analytical product that fuses information from those three articles, with information gathered from phone conversations with local law enforcement personnel, security providers and business professionals; and geo-spatial data.

Man and Machine

OSINT 2.0 puts a premium on human networks and contacts (HUMINT)—what a machine can facilitate, but not replicate. In practice, OSINT 2.0 will facilitate the maintenance and expansion of human networks through ongoing identification, recruitment and relationship management. To do so, it will require robust source control and management systems, building on best practices from the intelligence community's own HUMINT source management systems. This will include monitoring and ranking source reliability and timeliness and tracking interactions with sources throughout an investigation or enterprise.

OSINT 2.0

Looking at the existing capabilities of OSINT or any of the "ints," a critical observation emerges: even the best machines alone are insufficient to find, collate, package and analyze data. **The key to successfully producing indispensable intelligence is combining honed human analytical abilities with technologies that are getting better and better at isolating an intended query amid vast streams of information.**



OSINT 2.0: Mission-specific, fused intel combining OSINT & HUMINT

Improved Knowledge Capture

Machine-assisted analysis will effectively educate the user, offering enhanced terms and concepts for consideration during the course of an investigation. Every concluded investigation will return the sourced data, initially used during the analysis, to be used again—this time to assess, in hindsight, the quality and direction of the analysis that was conducted. As a result, there should be less and less concern that the departure of an experienced analyst will mean the loss of effective investigative methodologies or "know how". Over time, the ability to leverage lessons learned will yield intuitive users, able to conduct deeper and deeper Web forays in search of information.

More Time to Focus on Investigative Work

Next-generation services will include critical time-saving enhancements such as high-quality, automatic language translation; entity extraction; and voice-to-text automation for creating searchable transcripts. OSINT 2.0 will allow practitioners to further focus on their investigations instead of the means by which to extract intelligence.

Deeper Search

The World Wide Web, targeted by OSINT 1.0, consists of only a fraction of the information available online. Search engines, whose crawls are limited to the Web and whose results are consistently being manipulated by sophisticated search-engine optimization (SEO) campaigns, are focused on providing information that is more likely to be of commercial value than intelligence value.

OSINT 2.0 holds that the production of intelligence relies on an analytical process that locates, validates, distills, prioritizes and assesses information from all relevant, unclassified sources, including non-published sources, social networks and individuals.

OSINT TOOLS

As OSINT 2.0 produces fused and complete intelligence products, the model must include tools for OSINT analysts to systematically and effectively analyze unclassified data. OSINT 2.0 will provide the following mechanisms, allowing for empowered analysis and leading to the identification of patterns, non-obvious connections and weak signals:

- Link Analysis
- Trend Analysis
- Geospatial Analysis
- Collaborative Investigation Environment

Budget Considerations

The most immediate advantages of OSINT 2 in comparison to other intelligence disciplines are cost and return on investment—of particular relevance to organizations and countries with budget constraints. OSINT is considerably less expensive and much more available than collecting information via traditional means of HUMINT-, SIGINT- and IMINT-dedicated solutions. Human intelligence, communications intelligence and high-quality imagery intelligence is freely available on the Web. Although an OSINT solution can become a major component for intelligence collection and analysis, it is best utilized in collaboration with all other intelligence sources in order to generate an intelligence synergy.

Social Networking & Links

Not only do social networks facilitate the establishment and maintenance of friendships, they are also tools used by revolutionaries and organizers of flash mobs. One blog post, or even a single photo can end a politician's career, break a news story, or herald the arrival of American helicopters over a compound in Abbotabad.

There is a reason why social networks that can guarantee greater levels of security will be the most successful in the years to come. In a relatively short period of time, users have come to recognize that even the most stringent profile settings leave them vulnerable to criminals and opportunists. Social networking provides us with a powerful example of a linked environment: a vast crowd of people willingly sharing their daily habits, likes and dislikes, job histories and contact information—all accompanied by photos and links to friends and family. Users open themselves up to employers running due diligence checks, aggressive marketers and criminals.

Fortunately for law enforcement, criminals sometimes post self-incriminating evidence. A few police departments have already seen the benefits of monitoring social networking sites. In November, 2010, detectives from the New York City Police Department discovered a picture on one popular social network of a known felon showing off a ring that he'd stolen at a bus stop the previous day. This is a modern example of a criminal's tendency to brag about his activities.

In the past, war-time innovations in technology and medicine lent themselves to life-changing civilian uses, but now we're seeing the reverse: the revolution in social networking sites, which began on college campuses, has had a major impact on the priorities of governments, law enforcement and corporations.

Perhaps no other innovation has so aptly established the need for synergy between human and technological analysis, nor demonstrated so well the need for OSINT 2.0, as has social networking. Understanding and properly using this vast "web-within-a-web" is the challenge facing OSINT technologies in the 21st century.

Conclusion

Investigators can now find answers to most of their elementary information needs using OSINT from professional software products designed and built for that purpose. These products support the complete intelligence lifecycle and user workflows based on established methodologies. They utilize core technology engines in the areas of information harvesting, data fusion, text analysis, link visualization, rules-based alerts and reporting in order to provide today's intelligence analyst a rich investigation environment and intuitive user experience. At the same time, these tools provide an excellent return on investment as users can generate critical intelligence with minimal effort.

The Web as a whole offers exponential amounts of information just as budgets to pay analysts and investigators are shrinking amid economic downturn. The current climate demands efficiency, and if OSINT 2.0 is designed for anything, it is that. The first generation of OSINT accomplished its mission: the data is there. OSINT 2.0 is here to make sense of it.