Open Source Intelligence Tools in Law Enforcement

Workshop, 21-22 June 2012, JRC Ispra, Italy

Abstracts

1. [redacted] - Research Manager, West Midlands Police Counter Terrorism Unit, United Kingdom

Open source intelligence - a practitioner's perspective

The presentation will cover a brief history of the Counter Terrorism Unit and its functions, followed by an overview of how the OSINT capability has been developed highlighting some of the issues, pitfalls, some of the solutions and the future. The presentation will contain examples of how OSINT assisted investigations including one case that led to a successful conviction.

2. [redacted] / [redacted] - Senior information analysts, Regional Police Force, Netherlands

Real time intelligence during events

During events, social media is scanned for signs of public disorder. Based on these signals, management information is produced. With this intelligence, police commanders are more able to give instructions to their police officers. In this presentation, examples and methods are discussed on the basis of the following three events: a demonstration of activists, a football match and the Dutch national celebration day "Queen's Day".

3. [redacted] - OSINT expert, [redacted], Romania

Romanian Muslims on social platforms

The communication changes registered by extremist organizations triggered a specialized approach in terms of monitoring the virtual space, in other words an appropriate management of the investigation results by means of an automated Social Network Analysis and Sentiment and Affect Analysis.

Given radicalization and self-radicalization high risks, security agencies need to establish the exact nature of an online social network by monitoring both quantitative elements (network dimension and volatility, frequency of participation in debates, number of messages per time unit) as well as qualitative issues (position of each member within the network; issuers' persuasive ability; discourse patterns; indoctrination level and radical transformation potential).

The lack of a violent discourse inside a social network, although extremely convenient for security organizations, could actually be just a cover for achieving Islamic extremism main goal – setting up an Islamic conscience to precede the establishment of the Caliphate, based on rooting out Western influences and the practice of the 'right' religion, in European Muslims' case.

In this particular context, one should use semantic analysis tools to explore a virtually unknown zone, namely translate human emotions into measurable data by resorting to sentiment analysis filters

(positive versus negative), in order to reveal their intensity (level of emotional expression), clarifying the evolution of the radicalization process by which a moderate individual or group comes to adopt radical ideas and disseminate them.

The study I will present to you right now reveals the interest in using social media in order to strengthen the ties within the community and exchange almost radical opinions. Seeds of an inflexible form of Islam have been noticed, the trend being visible especially among young native and converted, who, driven by the need to be fully accepted by their adoptive 'family', eagerly take part in activism projects.

4. [redacted] - [redacted] / [redacted], Netherlands

Public and private data analysis using open-source components in the real world with the iColumbo project

Data gathering, both on the public internet and from private sources, provides insight and relevance to intelligence and public institutions alike. With tangible implementations in the real world, we've built and used open-source components to provide search and data analysis capabilities that prove that these systems can be built using transparent open-source software and technical systems.

One of these implementations — part of the IRN / iColumbo Internet Monitoring project — focuses specifically on meeting the stringent privacy and security requirements set by public institutions. Its open and transparent design makes the technology suitable for democratic and legal review as well as meeting forensic standards to make the information suitable to be used as evidence in court cases.

Seajas

Seajas provides software solutions in the areas of enterprise search, metadata extraction, language-technology and web monitoring. We develop and implement based on open-source and open-standards, offering high-end quality products to customers the world over with expert support and follow-up.

5. [redacted] - [redacted], General Police Directorate, Slovenia

How to improve security of police databases

A large amount of data in log files can keep track of user's activities in police databases. Examination of these log data for insider abuse can be a hard work. This presentation is aimed at our approach to support the examination of the log files.

We support the examination by a recommender system that combines internal and external data in order to identify suspicious patterns and items. The identification is based on various data analysis techniques, from simple queries to advanced data visualization techniques and assessment models. The recommender system is composed of KNIME open source platform for data analyses, and data gathering tools such as OSINT Suite.

The presentation will be focused on integration between the OSINT Suite and the KNIME platform. The OSINT Suite provides additional data from public sources that can enrich log file data, and the KNIME integrates this data into the recommender system. This concept can also be used for examination of similar data such as emails and various documents.

6. [redacted] / [redacted] - Internet surveillance, Regional Police Force, Netherlands

Internet surveillance in practice

This presentation focusses on who we are, what we use and some examples of internet surveillance and investigation in our police region.

7. [redacted] - [redacted], Verisign iDefense, United Kingdom

The challenges of applying social network analysis to social media

One of the most powerful tools in the social scientists tools box is Social Network Analysis (SNA), a method that can reveals hidden meaning in otherwise formless social groups. SNA has been successfully applied by intelligence agencies for decades into mediums such as telephonic analysis and the social hierarchies of numerous criminal and terrorist groups. Can SNA be as effectively applied to the medium of cyber space, specifically the social groups active within online forums and chat channels? This talk examines both the pitfalls and possible solutions to applying SNA to the cyber medium.