Exploiting Open Source Intelligence capabilities for the benefit of the Hellenic Air Force

Dimitris Gritzalis, Vasilis Stavrou

February 2016
Exploiting Open Source Intelligence capabilities for the benefit of the Hellenic Air Force

Dimitris Gritzalis, Vasilis Stavrou
Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics | Athens University of Economics & Business
Presentation outline

- Web 2.0 and Online Social Networks dynamics
- Open Source (& Social Media) Intelligence
- The **NEREUS** Framework
- SOCMINT and behavior prediction capabilities
  - Predisposition towards law enforcement
- Conclusions
Web 2.0 and Online Social Networks (OSN)
Open Source & Social Media Intelligence

- Open Source Information Transition 1455 to 2008

Open Source Intelligence (OSINT) is produced from publicly available information, which is:

- collected, exploited and disseminated in a timely manner
- offered to an appropriate audience
- used for the purpose of addressing a specific intelligence requirement

Publicly available information refers to (not only):

- Traditional media (e.g. television, newspapers, radio, magazines)
- Web-based communities (e.g. social networking sites, blogs)
- Public data (e.g. government reports, official data, public hearings)
- Amateur observation/reporting (e.g. amateur spotters, radio monitors)


SOCMINT is produced from Online Social Networks and the Web 2.0

Information/intelligence is now about linking actionable knowledge for immediate use of a particular user...
Value of OSINT/SOCMINT

Significant value offered to the originator or the dedicated recipient of the information:

– Journalists and researchers use OSINT/SOCMINT to generate a story or obtain greater information on a subject.

– OSINT/SOCMINT gives context to classified information. Generally, only selected information meets the criteria for classification, with unclassified sources of information filling the gaps.

– OSINT/SOCMINT gives adversarial forces a starting point and additional resources necessary to leverage further attacks or exploitation.

– OSINT/SOCMINT reveals the intent of friendly or adversarial forces.

– OSINT/SOCMINT reveals status, capabilities or other valuable information.

Source: http://www.opsecprofessionals.org/academy/
Who can exploit OSINT/SOCMINT?

- Business
- Law Enforcement
- Government
- Criminals
- Special Agencies
- Military

Source: http://www.opsecprofessionals.org/academy/
A selection of OSINT/SOCMINT capabilities

- Identify and predict insiders
- Detect sentiment of population w.r.t. specific intelligence demands
- Identify and predict public opinion on specific intelligence demands
- Identify and predict public opinion fluctuations
- Detect influential users capable of supporting a cause
- Detect appropriate means and content of communication for achieving optimum results
- Facilitate achievement of influence goals and success tactics
- Optimize efficiency of communication and influence tactics
Revealing attitude towards law enforcement/infringement

<table>
<thead>
<tr>
<th>OSINT</th>
<th>OSN: YouTube</th>
</tr>
</thead>
<tbody>
<tr>
<td>Means utilized for the analysis</td>
<td></td>
</tr>
<tr>
<td><strong>Science</strong></td>
<td><strong>Theory</strong></td>
</tr>
<tr>
<td>Computing</td>
<td>Machine Learning</td>
</tr>
<tr>
<td></td>
<td>Data Mining</td>
</tr>
<tr>
<td>Sociology</td>
<td>Social Learning Theory</td>
</tr>
</tbody>
</table>

**Application:** Detection/prediction of threats, capabilities for influence and divided loyalty.
NEREUS: Architecture in a nutshell

Flat data path

- YouTube User
- User classifier (naïve bayes)
- Flat data transformation
- Naïve Bayes metrics
  - Classes: P: 72, N: 93
  - Precision: P: 92, N: 73
  - F-Score: P: 81, N: 82
  - Accuracy: 81
- Categories
  - Negatively predisposed (P)
  - Not negatively predisposed (N)

Comments classification path

- Researchers’ compliance with ethical standards
- Legal Expert
- Anonymization layer
- YouTube Crawler
- Data preprocessing
- Comment classifier (LR)
- Comments results
- Storage
- Video, uploads, lists & favorites classifier

Legend

- Web 2.0 Medium: YouTube
- Domain Expert: Sociologist, Political Scientist

Metrics:

<table>
<thead>
<tr>
<th>Classifier</th>
<th>NBM</th>
<th>SVM</th>
<th>LR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes</td>
<td>P</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Precision</td>
<td>71</td>
<td>70</td>
<td>83</td>
</tr>
<tr>
<td>Recall</td>
<td>71</td>
<td>69</td>
<td>79</td>
</tr>
<tr>
<td>F-Score</td>
<td>71</td>
<td>69</td>
<td>79.5</td>
</tr>
<tr>
<td>Accuracy</td>
<td>70</td>
<td>80</td>
<td>81</td>
</tr>
</tbody>
</table>
The utmost importance of the social context

**Authoritarian Regimes**

Revealing personal attitude towards law enforcement/infringement will be used by the Regime against resisting pro-civic rights movements.

Pro-civic rights movements should prevent such platforms from being used by the Regime, using any available means.

**Democratic States**

Revealing personal attitude towards law enforcement/infringement may be used to protect Democracy from its opponents.

Democratic States may resist to social changes supported by, for example, grassroots political rights movements.

Democratic States may make use of such intrusive platforms, provided they are put under strict democratic control.
Attitude towards law infringement

Study: Motive, anger, frustrations, predisposition towards law enforcement/infringement

Means: Machine Learning, comment classification, flat data classification.

✓ Individuals tend to transfer online their offline behavior

✓ Identify users’ attitude towards law enforcement/infringement

✓ Trait of negative attitude towards law enforcement is connected to delinquent behavior via:

- Sense of entitlement
- Lack of empathy
- Anger and revenge syndrome and
- Inflated self-image
Dataset description

• Crawled YouTube and created dataset consists solely of **Greek** users.
• Utilized YouTube **REST-based API** (developers.google.com/youtube/):
  – Only publicly available data collected
  – Quote limitations (posed by YouTube) were respected
• Collected data were classified into three categories:
  – User-related information (profile, uploaded videos, subscriptions, favorite videos, playlists)
  – Video-related information (license, # of likes, # of dislikes, category, tags)
  – Comment-related information (comment content, # of likes, # of dislikes)

• Time span of collected data covered 7 years (Nov 2005 - Oct 2012).
• A basic anonymisation layer added to the collected data:
  – MD5 hashes instead of usernames
• Comment classified into categories of interest:
  – Process performed as **text classification**
  – Machine trained with **text examples** and the **category** each one belongs to
  – Excessive support by **field expert** (Sociologist)

• Test set used to evaluate efficiency of resulting classifier:
  – Contains pre-labeled data fed to machine, labeled by field expert
  – Check if initial assigned label is equal to predicted one
  – Testing set labels assigned by field expert

• Most comments written in Greek/greeklish

• Conversion of greeklish text to Greek

• Categories of content defined:
  – Users with a **negative** attitude towards law enforcement
    (**Predisposed negatively (P)**)
  – Users with a **not negative** attitude towards law enforcement
    (**Not-predisposed negatively (N)**)
• **Video classification**: Examination of a video on the basis of its comments
  - Naïve Bayes (NB)
  - Support Vector Machines (SVM)

• **(Video) Lists classification**: Voter process to determine category classification (same threshold)

• **Conclusions about user behavior**:
  - If there is at least one category P attribute then the user is classified into category P

• **Logistic Regression algorithm**:
  - Classifies a comment with 81% accuracy

**Metrics**

<table>
<thead>
<tr>
<th>Classifier</th>
<th>SVM</th>
<th>LR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes</td>
<td></td>
<td>80%</td>
</tr>
<tr>
<td>Precision</td>
<td>71%</td>
<td>77%</td>
</tr>
<tr>
<td>Recall</td>
<td>70%</td>
<td>86%</td>
</tr>
<tr>
<td>F-Score</td>
<td>71%</td>
<td>80%</td>
</tr>
<tr>
<td>Accuracy</td>
<td>70%</td>
<td>81%</td>
</tr>
</tbody>
</table>
Analysis based on flat data

- Addressing the problem from a different perspective:
  - Connection between users of category P and confidence of accuracy of comments belonging to category P.
  - Blue: Users of category P classified on the basis of the comment-oriented tuple (Flat Data).
  - Red: Users of category P classified on the basis of their comments only (Machine Learning).

- Data transformation:
  - User represented by a tuple (username, content of comment, video ID the comment refers to, country, age, genre, # of subscribers, # of video views).

- Machine trained by a set of users of categories P and N.

1721 users are (almost certainly) negatively predisposed towards law enforcement/infringement
Selected observations

- **6%** of comments (among 2,000,000 collected) express negative attitude towards respecting the law (i.e., positive to law infringement)
- **3.5%** of videos (among 200,000 collected) classified into a specific category of interest
- **14%** of users (among 13,000 collected) express negative attitude towards respecting the law (i.e., positive to law infringement)
The **NEREUS** Framework: Selected exploitation capabilities

- **(Insider) Threat prediction:**
  - Applying Shaw and FBI psychosocial indicators (narcissism, anger syndrome, revenge syndrome, etc.).

- **Influence opportunities exploitation:**
  - Analyzing communication graphs, correlating psycho-social characteristics, assessing engagement tactics, etc.

- **Delinquent behavior prediction:**
  - Analysis of psycho-social characteristics (narcissism, anger syndrome, revenge syndrome, etc.).
  - Predisposition analysis (Graph Theory and Content Analysis through Social Learning Theory, etc.).

- **Forensics analysis support**
  - Suspect profiling and analysis (prediction of delinquent behavior, etc.).
General conclusions

- SOCMINT can transform into intelligence the vast amount of data produced by Web 2.0.
- SOCMINT is an intrusive technology and could put in danger civic rights.
- SOCMINT utilization is not - and should not be considered as - a solely technical issue.
- OSINT/SOCMINT can help in predicting insiders, in predicting delinquent behavior, in supporting law enforcement and in enhancing national defense.
- OSINT/SOCMINT intrusive nature dictates specific uses for legitimate only purposes.
References


