Exploiting the dark triad for national defense capabilities

Dimitris Gritzalis

May 2015
Exploiting the dark triad for national defense capabilities

Professor Dimitris A. Gritzalis (dgrit@aueb.gr)

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business
The problem:
An insider as a severe threat to national defense

The theory:
Narcissists tend to turn insiders

The defense:
Reveal narcissists

The data source:
Online Social Networks and the Web 2.0

The tool:
NEREUS Framework
The problem: The Insider threat

Insider threat was the **top priority to protect** for 2014

Insiders are persons who:
- are legitimately given access rights to a Critical Infrastructure
- misuse their privileges and violate security policy

Insiders consist the **top source** of data breaches

**Source:**
The theory: The Dark Triad

- **Dark Triad personality traits**
  - **Narcissism**: Inflated self-view and focus on themselves
  - **Machiavellianism**: Manipulative personality
  - **Psychopathy**: High impulsivity and thrill-seeking, along with low empathy and low anxiety

- Dark Triad traits are used to extend Five Factor Model (FFM) to represent **socially malevolent behavior**

- The wealth of data provided by OSN users has opened the door to a new way of **analyzing personality**

- Ability to **exploit narcissism** personality trait
  - Narcissism trait is also examined by Shaw and the FBI

**Sources:**
The defense: Open Source Intelligence

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


**SOCMINT** is produced from Online Social Networks & the Web 2.0
The data source: Web 2.0 & Online Social Networks

Source: [http://socialmediatoday.com/](http://socialmediatoday.com/)
## The tool: The NEREUS Framework

### Tools used for the open data analysis

<table>
<thead>
<tr>
<th>Science</th>
<th>Theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informatics</td>
<td>Graph Theory</td>
</tr>
<tr>
<td></td>
<td>Content Analysis</td>
</tr>
<tr>
<td>Sociology</td>
<td>Theory of Planned Behavior</td>
</tr>
<tr>
<td>Psychology</td>
<td>Social Learning Theory</td>
</tr>
</tbody>
</table>

**Application:** Insider threat detection/prediction, influential users detection, means of communication evaluation, etc.
The **NEREUS** Framework in a nutshell

### Predicting & identifying potential insiders

- Twitter Users
- Content generation

### Researchers’ compliance with ethical standards

- LEGAL EXPERT
- YES

- CRITICAL INFRASTRUCTURES
  - National security
  - Public interest

### Information Security & Critical Infrastructure Protection Laboratory

#### Legend

<table>
<thead>
<tr>
<th>Category</th>
<th>Influence valuation</th>
<th>Klout score</th>
<th>Usage valuation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loners</td>
<td>0 - 90</td>
<td>3.55 - 11.07</td>
<td>0 - 500</td>
</tr>
<tr>
<td>Individuals</td>
<td>90 - 283</td>
<td>11.07 - 26.0</td>
<td>500 - 4,500</td>
</tr>
<tr>
<td>Known users</td>
<td>283 - 1,011</td>
<td>26.0 - 50.0</td>
<td>4,500 - 21,000</td>
</tr>
<tr>
<td>Mass Media &amp; Personas</td>
<td>1,011 - 3,604</td>
<td>50.0 - 81.99</td>
<td>21,000 - 56,900</td>
</tr>
</tbody>
</table>

#### Diagram

- Twitter
- Crawling & storing
- Our crawling server
- Klout score queries
- User classification according to categories
- Content Aggregator
  - Usage intensity valuation
- Indegree/oudegree aggregator
- Influence valuation
- Klout score collector

---

Ver. 2.11.14, 24.11.2014
The dataset utilized

- Focus on a Greek **Twitter** community:
  - Context sensitive research
  - Utilize ethnological features rooted in locality
  - Extract and analyze results
- Analysis of **content** and measures of **user influence** and **usage intensity**
- User Categories: Follower, Following, Retweeter
- Graph:
  - Each user is a node
  - Every interaction is a directed edge
- **41.818 fully crawled users** (personal & statistical data)
  - Name, ID, personal description, URL, language, geolocation, profile state, lists, # of following/followers, tweets, # of favorites, # of mentions, # of retweets

Twitter (Greece, 2012-13)

1,075,859 users
41,818 fully crawled users
7,125,561 connections among them
Graph theoretical and content analysis

Strongly connected components:
- There exists 1 large component (153.121 nodes connected to each other) and several smaller ones

Node Loneliness:
- 99% of users connected to someone

Small World phenomenon:
- Every user lies <6 hops away from anyone else

Indegree Distribution:
- # of users following each user
- Average 13.2 followers/user

Outdegree Distribution:
- # of users each user follows
- Average 11 followers/user

Usage Intensity Distribution:
Weighted aggregation of: {# of followers, # of followings, tweets, retweets, mentions, favorites, lists}
Conclusions

✓ Web 2.0 produces vast amounts of crawlable information and OSINT can transform it into intelligence.

✓ OSINT can assist in detecting the Dark Triad traits (narcissistic behavior, etc.).

✓ OSINT can help in predicting insiders, in predicting delinquent behavior, and in enhancing national defense.

✓ OSINT intrusive nature dictates use for specific purposes, according to law.


