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

What is all about?

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

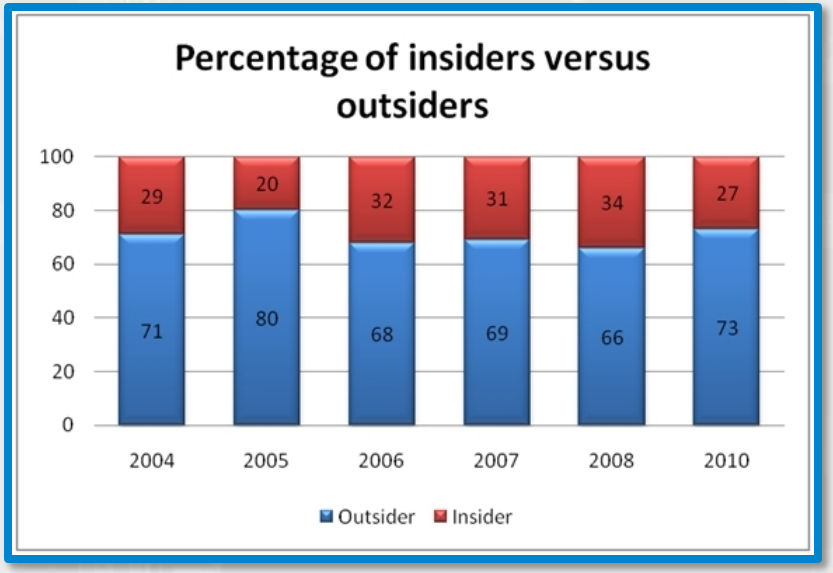
The problem: The Insider threat

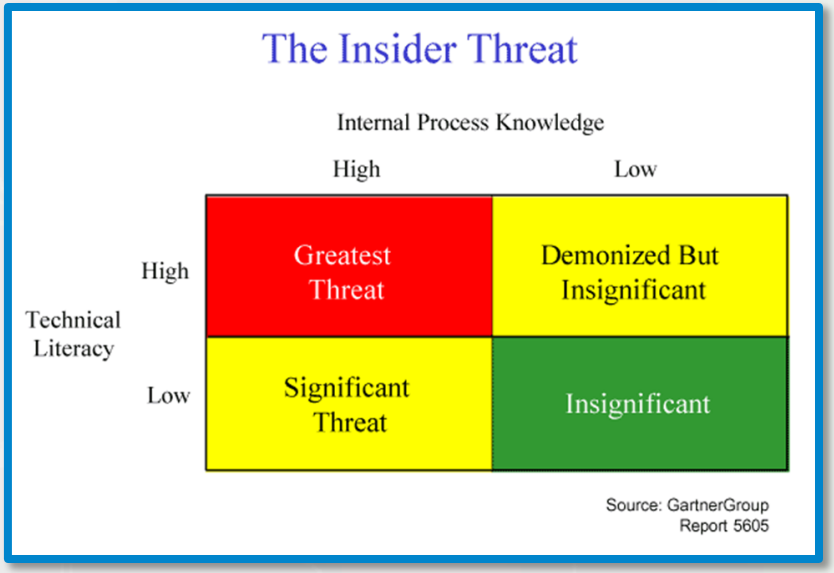
Insider threat was the **top priority to protect** for 2014

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:

CERT, *Cyber Security Watch Survey: How Bad Is the Threat?,* Carnegie Mellon University, USA, 2014.

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:

M. Maasberg, J. Warren, N. Beebe, "The Dark Side of the Insider: Detecting the Insider Threat through examination of Dark Triad personality traits".

Federal Bureau of Investigation, *The insider threat: An introduction to detecting and deterring an insider spy*", USA, 2012.

E. Shaw, K. Ruby, J. Post, "The insider threat to information systems: The psychology of the dangerous insider", *Security Awareness Bulletin*, vol. 2, no. 98, pp. 1--10. 1998.

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**

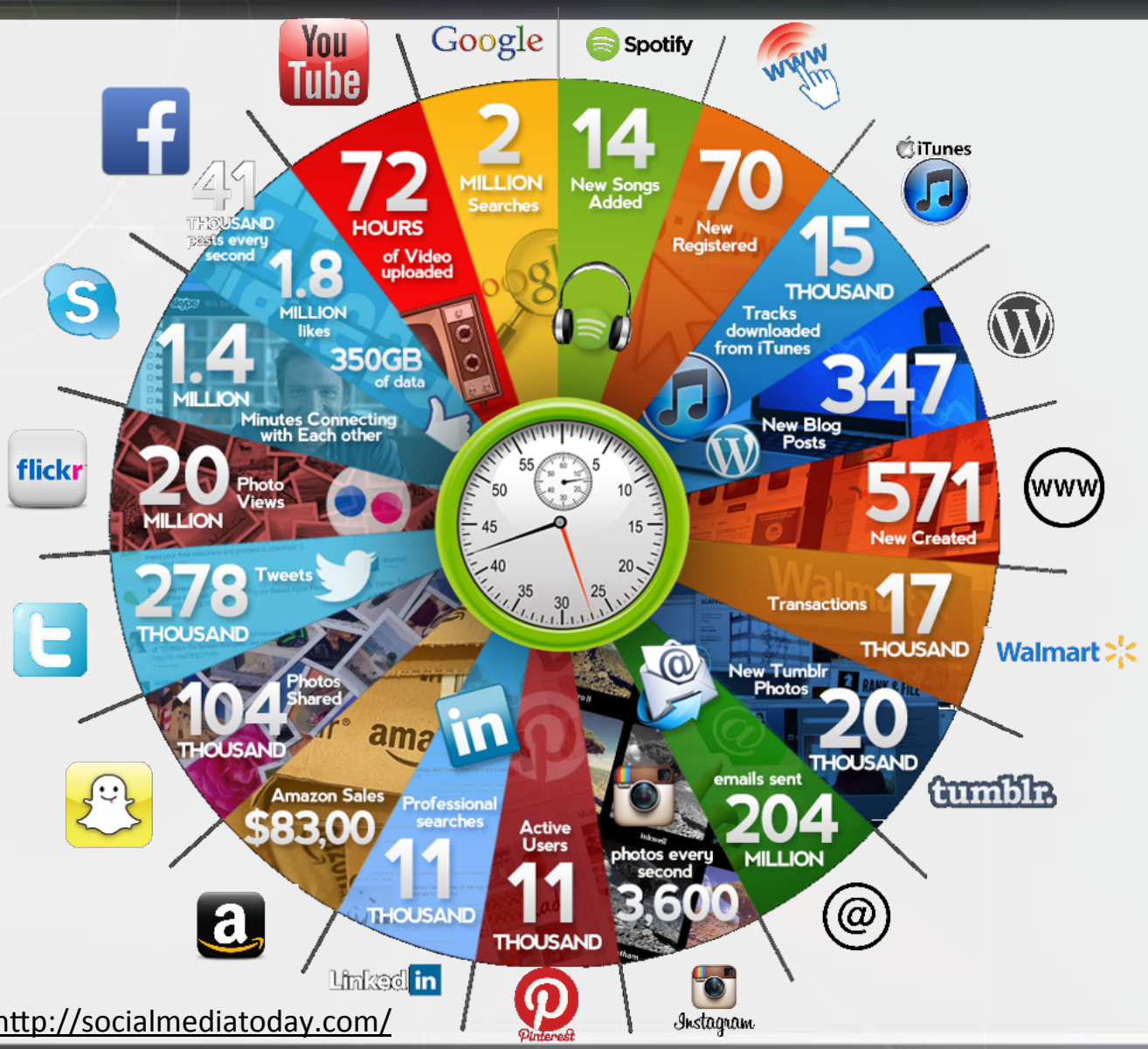
Publicly available information refers to (not only):

- 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.)

OSINT defined by US Dept. of Defense (Public Law 109-163, Sec. 931,National Defense Authorization Act for Fiscal Year 2006).

SOCMINT is produced from Online Social Networks & the Web 2.0

The data source: Web 2.0 & Online Social Networks

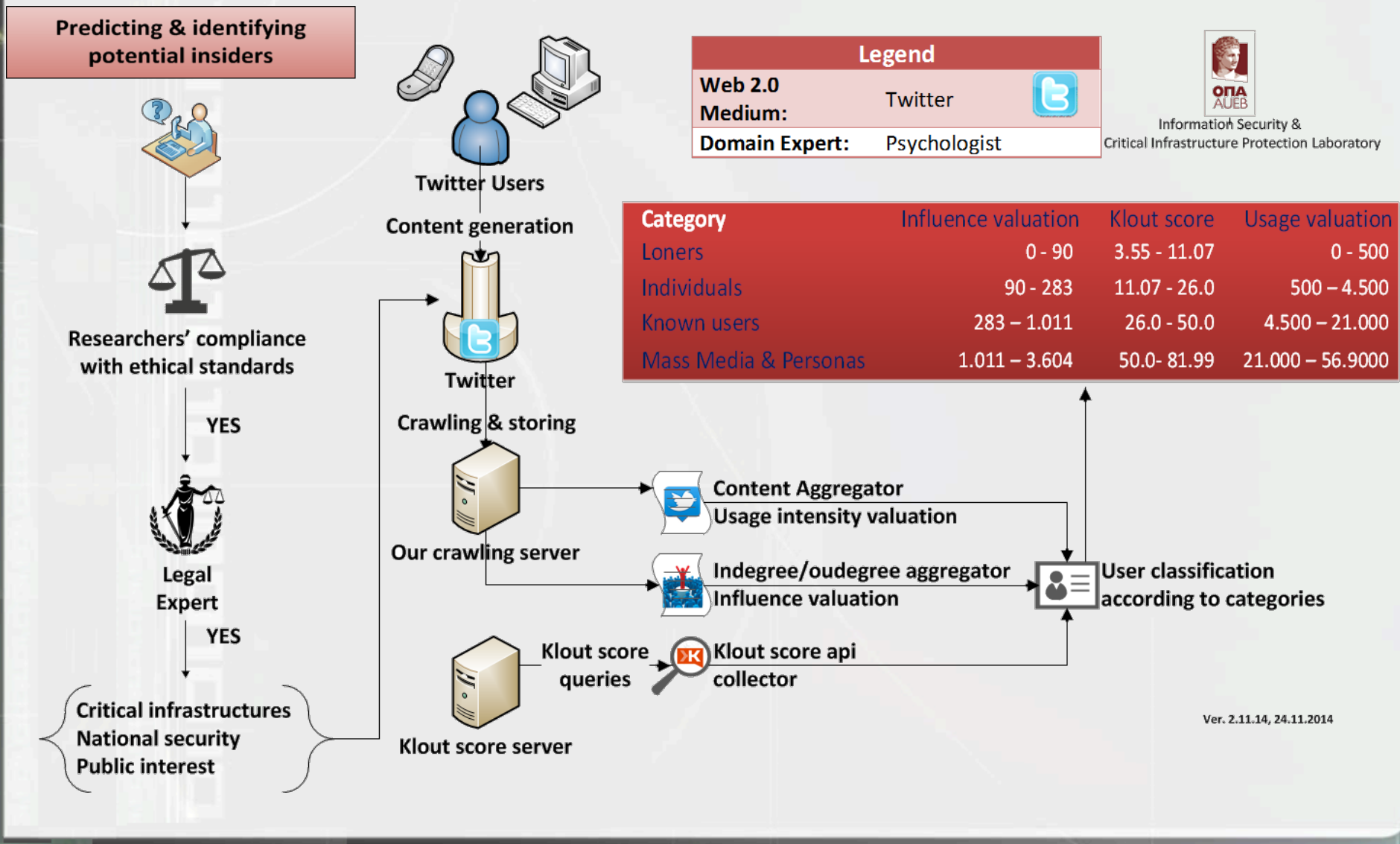


Source: http://socialmediatoday.com/

The tool: The NEREUS Framework

NEREUS Framework	OSN: Twitter
Tools used for the open data analysis	
Science	**Theory**
Informatics	Graph Theory
	Content Analysis
Sociology Psychology	Theory of Planned Behavior
	Social Learning Theory
Application: Insider threat detection/prediction, influential users detection, means of communication evaluation, etc.	

The NEREUS Framework in a nutshell

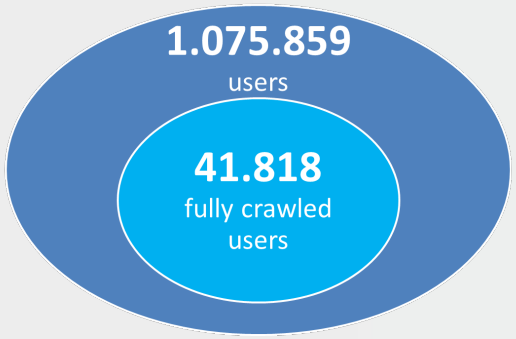


Category	Influence valuation	Klout score	Usage valuation
Loners	0 - 90	3.55 - 11.07	0 - 500
Individuals	90 - 283	11.07 - 26.0	500 – 4.500
Known users	283 – 1.011	26.0 - 50.0	4.500 – 21.000
Mass Media & Personas	1.011 – 3.604	50.0- 81.99	21.000 – 56.9000

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)



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

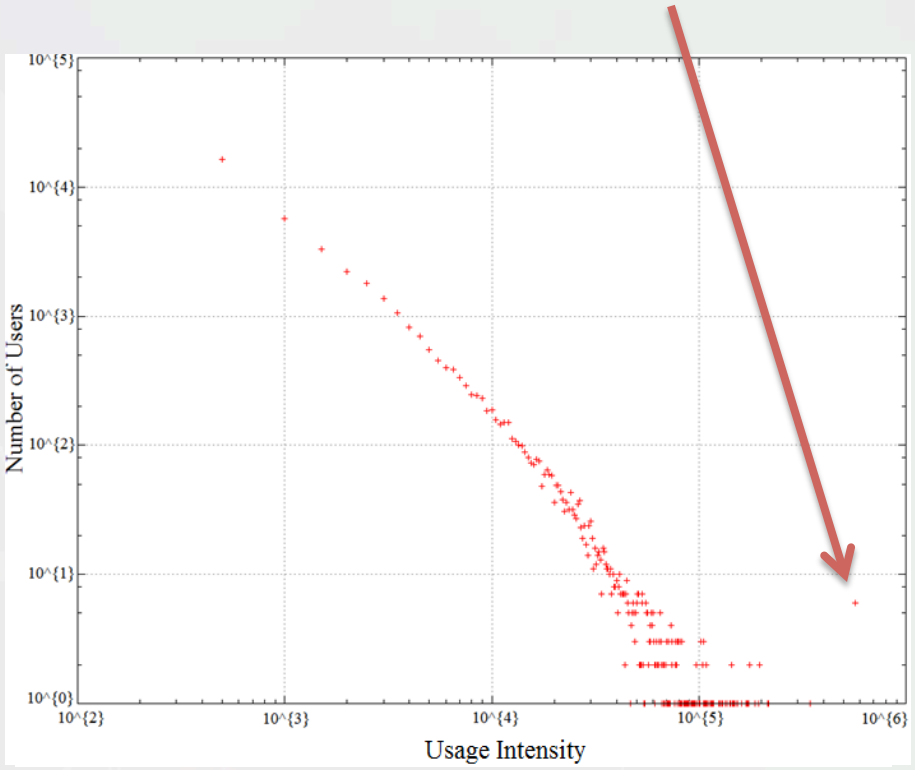
Outdegree Distribution:

- # of users each user follows
- Average 11 followers/user

Usage Intensity Distribution:

Weighted aggregation of: {# of followers, # of followings, tweets, retweets, mentions, favorites, lists}

Important cluster of users



Category	Influence valuation	Klout score	Usage valuation
Loners	0 - 90	3.55 - 11.07	0 - 500
Individuals	90 - 283	11.07 - 26.0	500 - 4.500
Known users	283 - 1.011	26.0 - 50.0	4.500 - 21.000
Mass Media & Personas	1.011 - 3.604	50.0- 81.99	21.000 - 56.9000

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.

References

1. Gritzalis D., Stavrou V., Kandias M., Stergiopoulos G., “Insider Threat: Enhancing BPM through Social Media”, in *Proc. of the 6th IFIP International Conference on New Technologies, Mobility and Security*, IEEE Press, 2014.
2. Gritzalis D., Kandias M., Stavrou V., Mitrou L., "History of Information: The case of Privacy and Security in Social Media", in *Proc. of the History of Information Conference*, Law Library Publications, 2014.
3. Gritzalis D., “Insider threat prevention through Open Source Intelligence based on Online Social Networks”, Keynote address, *13th European Conference on Cyber Warfare and Security* (ECCWS-2014), Greece, 2014.
4. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., “An Insider Threat Prediction Model”, in *Proc. of the 7th International Conference on Trust, Privacy and Security in Digital Business*, pp. 26-37, Springer (LNCS 6264), Spain, 2010.
5. Kandias M., Galbogini K., Mitrou L., Gritzalis D., "Insiders trapped in the mirror reveal themselves in social media", in *Proc. of the 7th International Conference on Network and System Security*, pp. 220-235, Springer, 2013.
6. Kandias M., Mitrou L., Stavrou V., Gritzalis D., “Which side are you on? A new Panopticon vs. privacy”, in *Proc. of the 10th International Conference on Security and Cryptography*, pp. 98-110, ScitecPress, 2013.
7. Kandias M., Stavrou V., Bozovic N., Mitrou L., Gritzalis D., "Can we trust this user? Predicting insider’s attitude via YouTube usage profiling", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, pp. 347-354, IEEE Press, 2013.
8. Kandias M., Virvilis N., Gritzalis D., "The Insider threat in Cloud Computing", in *Proc. of the 6th International Conference on Critical Infrastructure Security*, pp. 93-103, Springer, 2013.
9. Kandias M., Stavrou V., Bosovic N., Gritzalis D., “Proactive insider threat detection through social media: The YouTube case”, in *Proc. of the 12th Workshop on Privacy in the Electronic Society*, pp. 261-266, ACM, Germany, 2013.
10. Kandias M., Mitrou L., Stavrou V., Gritzalis D., "YouTube user and usage profiling: Stories of political horror and security success", in *e-Business and Telecommunications*, Springer, 2014.
11. Kotzanikolaou P., Theoharidou M., Gritzalis D., “Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer, USA, 2013
12. Mitrou L., Kandias M., Stavrou V., Gritzalis D., "Social media profiling: A Panopticon or Omniopticon tool?", in *Proc. of the 6th Conference of the Surveillance Studies Network*, Spain, 2014.
13. Pipyros K., Mitrou L., Gritzalis D., Apostolopoulos T., "A cyber attack evaluation methodology", in *Proc. of the 13th European Conference on Cyber Warfare and Security*, Athens, 2014
14. Theoharidou M., Kotzanikolaou P., Gritzalis D., “Risk-based criticality analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, 2009.