Personal traits analysis as a means to predict Insiders

Miltos Kandias, Vasilis Stavrou

January 2015

2014 National Cybersecurity Exercise Briefing
Ministry of Defense, Athens, Greece
January 2015

Personal traits analysis as a means to predict Insiders

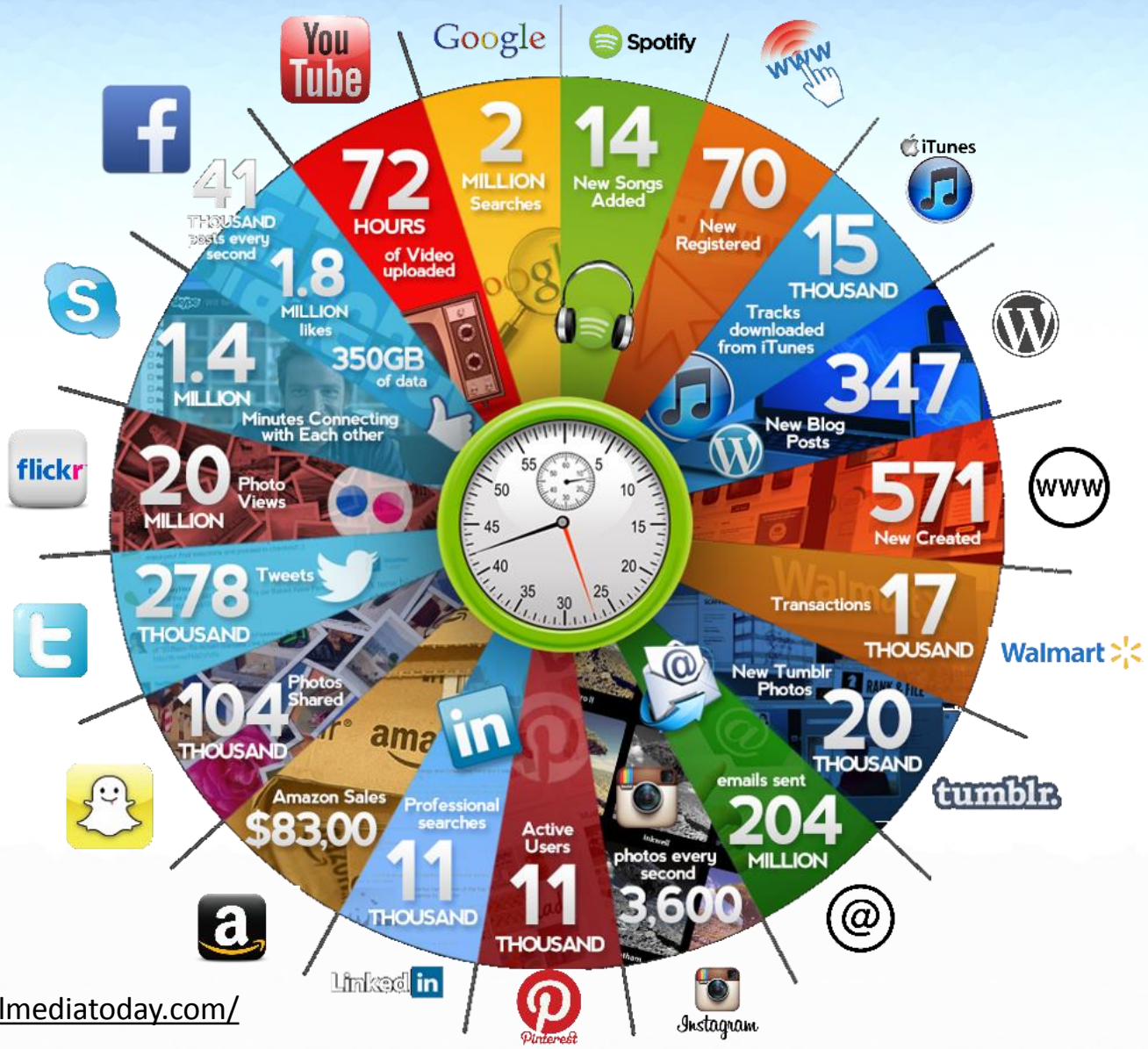
Miltos Kandias, Vasilis Stavrou

Information Security & Critical Infrastructure Protection (INFOSEC) Lab
Dept. of Informatics, Athens University of Economics & Business

Presentation outline

- Web 2.0 and Online Social Networks dynamics
- Open Source (& Social Media) Intelligence
- The Insider threat
- The **NEREUS** Framework
- Insider threat prediction via Narcissism
- Conclusions

Web 2.0 and Online Social Networks (OSN)

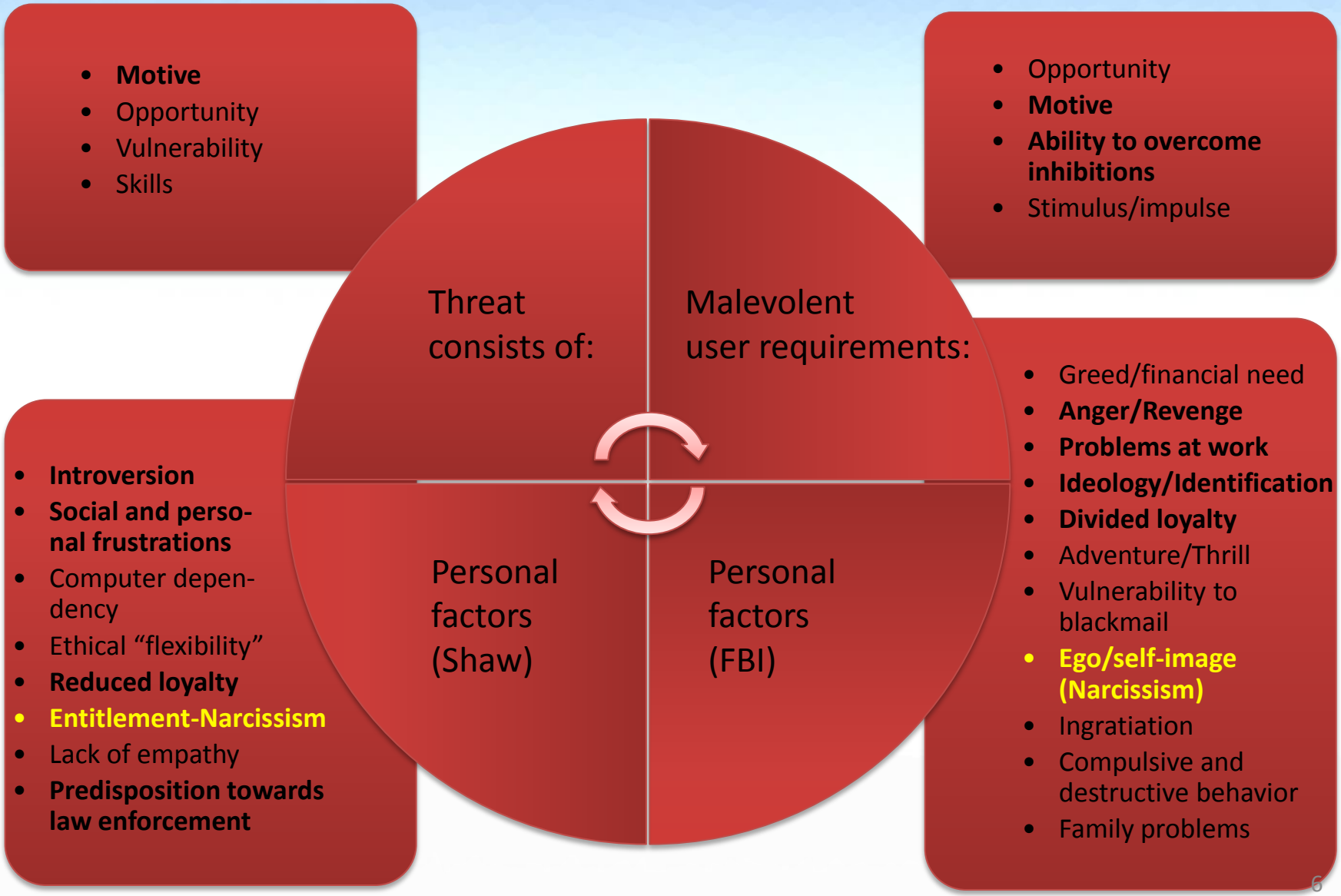


Source: http://socialmediatoday.com/

Open Source (& Social Media) Intelligence (OSINT/SOCMINT)

- 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)
- 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 and the Web 2.0

The Insider Threat

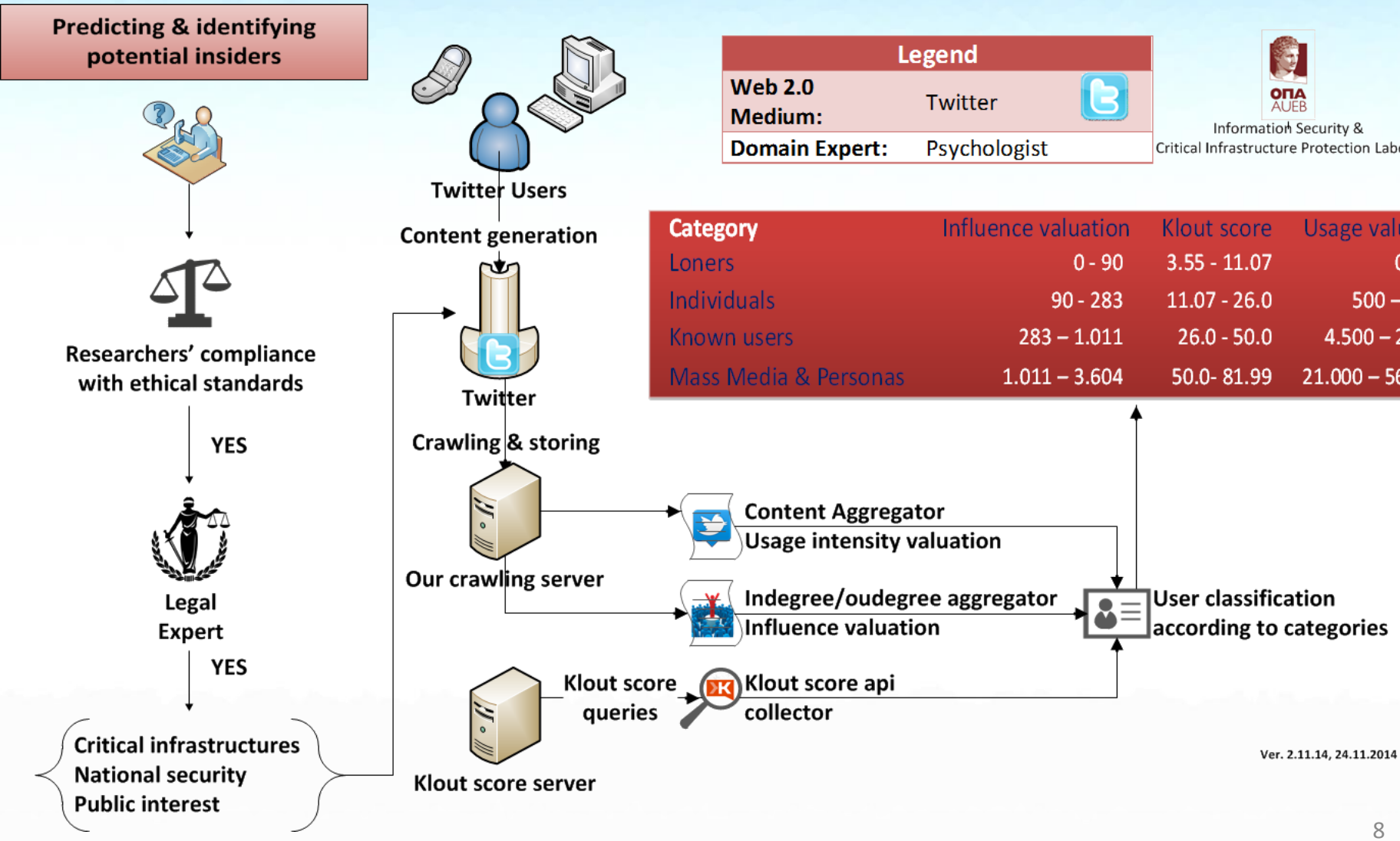


NEREUS Framework (Function 1)
Insider threat prediction based on *Narcissism*

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.	

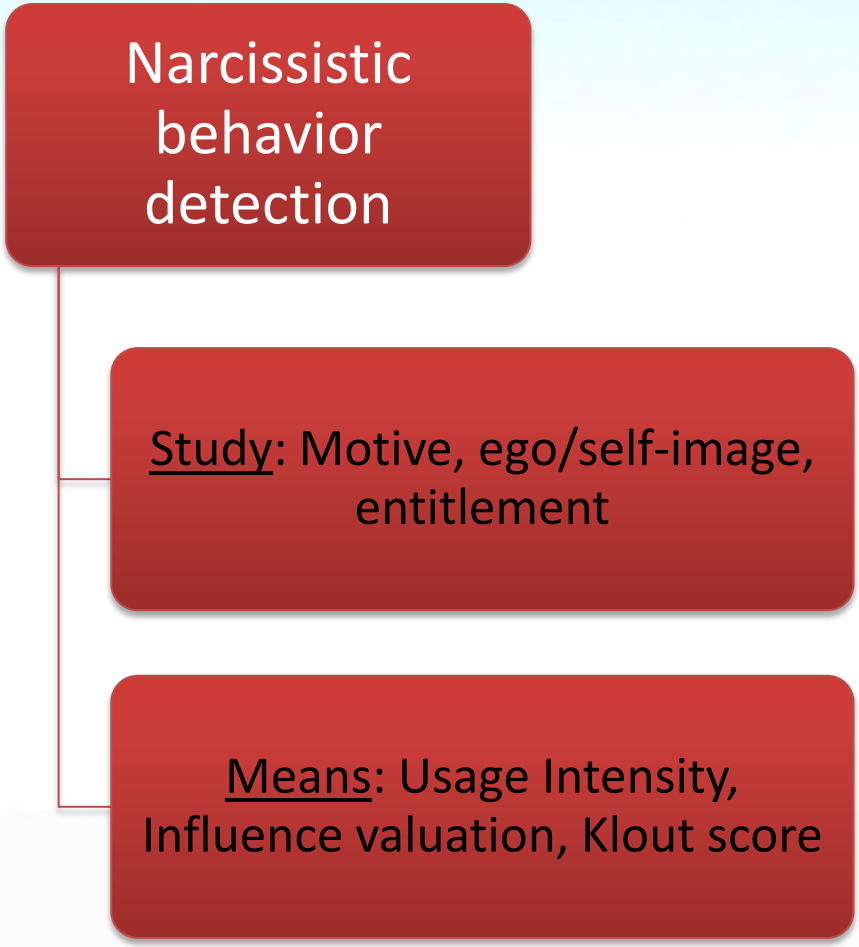
NEREUS Framework (Function 1)

The 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

NEREUS Framework (Function 1)
Insider threat prediction based on Narcissism

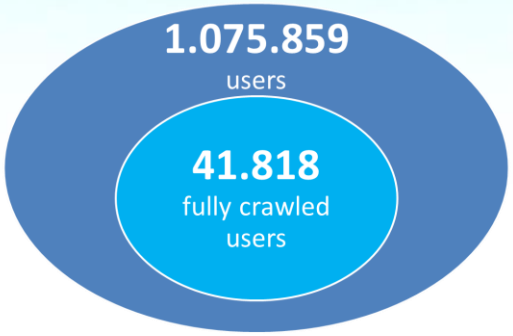


- Individuals tend to transfer offline behavior online.
- Trait of narcissism directly relates to **insider threats**, **OSN popularity** and **influence**.
- Utilize graph theoretic tools to perform analysis.
- Valuation of social media **popularity** and **usage intensity**.
- Twitter data to become open.
- Trait of narcissism relates to delinquent behavior via :
  - sense of entitlement
  - lack of empathy
  - anger and “revenge” syndrome
  - inflated self-image

Dataset description

- 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 and 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)

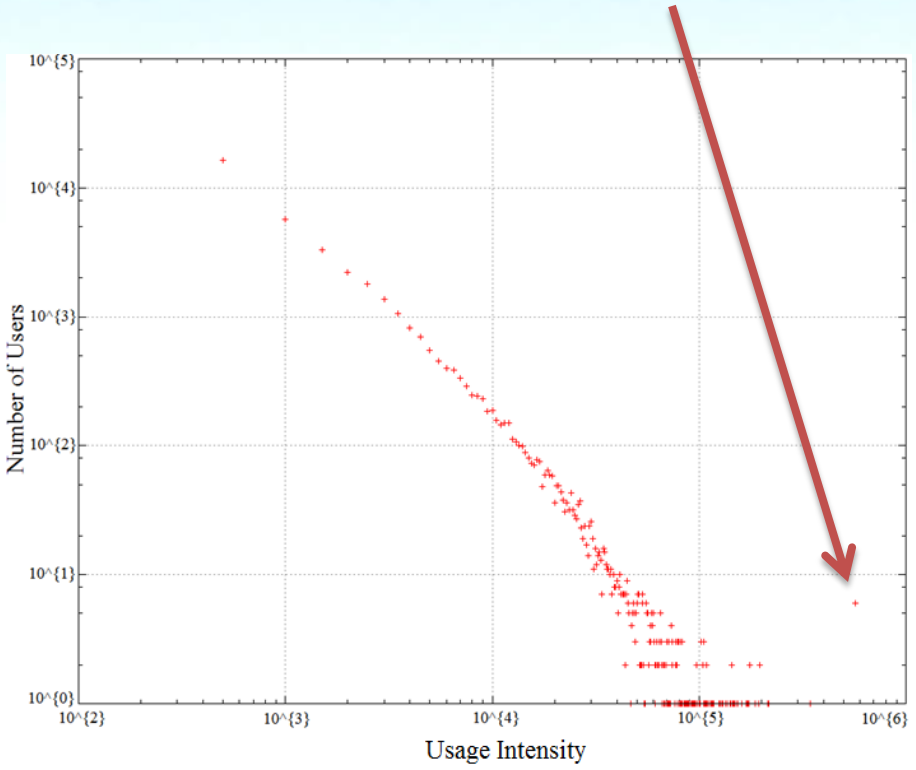


7.125.561 connections among them

Graph Theoretical approach

- **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
- **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}



Narcissism detection

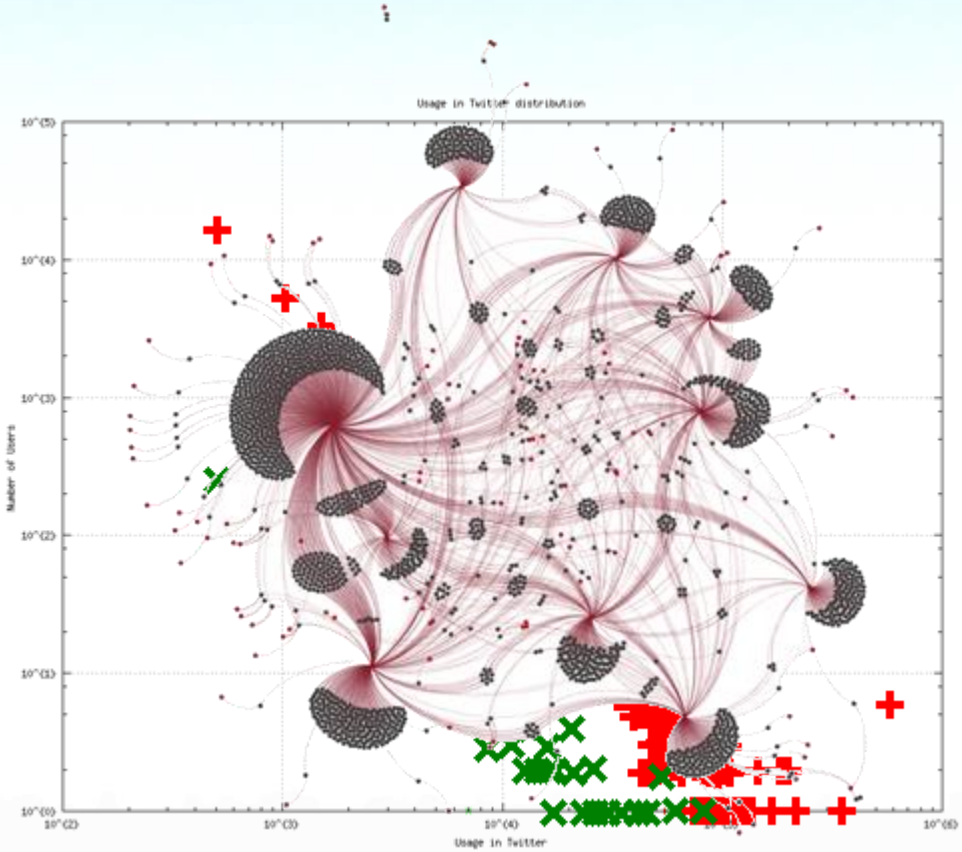
- Majority of users make limited use of Twitter
  - A lot of “normally” active users and very few “popular” users
  - Users classified into four categories, on the basis of specific metrics (influence valuation, Klout score, usage valuation)
- Above a threshold:
  - User becomes **quite influential/perform intense** medium use
  - User get a “**mass-media & persona**” status

The excessive use of Twitter by persons who are not mass-media or personas could connect to narcissism and identify narcissists, i.e. persons who - inter alia - tend to turn insiders

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

Group dynamics

- Create reliable graphs of interconnection, i.e. visualization of groups of people according to their **relationships** and **common interests**
- Compare deviating usage behavior according to a set of parameters, **maximize efficiency**



NEREUS Framework:
Web 2.0 data exploitation capabilities

- Insider threat prediction
  - Applying Shaw and FBI psychosocial indicators (narcissism, anger syndrome, revenge syndrome, 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.)

Preliminary conclusions

- ✓ Web 2.0 produces vast amounts of crawlable information and OSINT/SOCMINT can transform it into intelligence.
- ✓ OSINT/SOCMINT can assist in detecting narcissistic behavior, predisposition towards law enforcement, personal stress level variations, etc.
- ✓ OSINT/SOCMINT can help in predicting insiders, in predicting delinquent behavior, in supporting law enforcement, in enhancing national defense, etc.
- ✓ OSINT/SOCMINT intrusive nature dictates specific uses for legitimate only purposes.

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* (NMTS-2014), Springer, UAE, 2014.
2. 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.
3. 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, Athens, 2014.
4. 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* (SECRYPT-2013), pp. 98-110, Iceland, 2013.
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* (NSS-2013), pp. 220-235, Springer (LNCS 7873), Spain, June 2013.
6. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Conference on Critical Infrastructure Security* (CRITIS-2011), pp. 93-103, Springer (LNCS 6983), United Kingdom, 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* (ATC-2013), pp. 347-354, IEEE Press, Italy, 2013.
8. Kandias M., Stavrou V., Bosovic N., Mitrou L., Gritzalis D., “Proactive insider threat detection through social media: The YouTube case”, in *Proc. of the 12th Workshop on Privacy in the Electronic Society* (WPES-2013), pp. 261-266, ACM Press, Germany, 2013.
9. Kandias M., Virvilis N., Gritzalis D., “The Insider Threat in Cloud Computing”, in *Proc. of the 6th International Workshop on Critical Infrastructure Security* (CRITIS-2011), Bologna S., et al (Eds.), pp. 93-103, Springer (LNCS 6983), Switzerland, 2011.
10. 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* (TrustBus-2010), pp. 26-37, Springer (LNCS-6264), Spain, 2010.
11. 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.
12. 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* (ECCWS-2014), Greece, 2014.
13. Stavrou V., Kandias M., Karoulas G., Gritzalis D., "Business Process Modeling for Insider threat monitoring and handling", in *Proc. of the 11th International Conference*Theoharidou M., Kotzanikolaou P., Gritzalis D., "Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection* (CIP-2009), Springer, USA, 2009.
14. Theoharidou M., Papanikolaou N., Pearson S., Gritzalis D., “Privacy risks, security and accountability in the Cloud”, in *Proc. of the 5th IEEE Conference on Cloud Computing Technology and Science* (CloudCom-2013), pp. 177-184, IEEE Press, UK, 2013.
15. Virvilis N., Gritzalis D., “Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?”, in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing* (ATC-2013), pp. 396-403, IEEE Press, Italy, 2013.