

Open Source Intelligence produced from Online Social Networks: A proactive cyber-defense tool

Dimitris Gritzalis

July 2014

13th European Conference on Cyber Warfare and Security (ECCWS-2014)

July 2014, Piraeus, Greece

Keynote address

Open Source Intelligence produced from Online Social Networks: A proactive cyber-defense tool



Dimitris A. Gritzalis

Professor and Director

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece

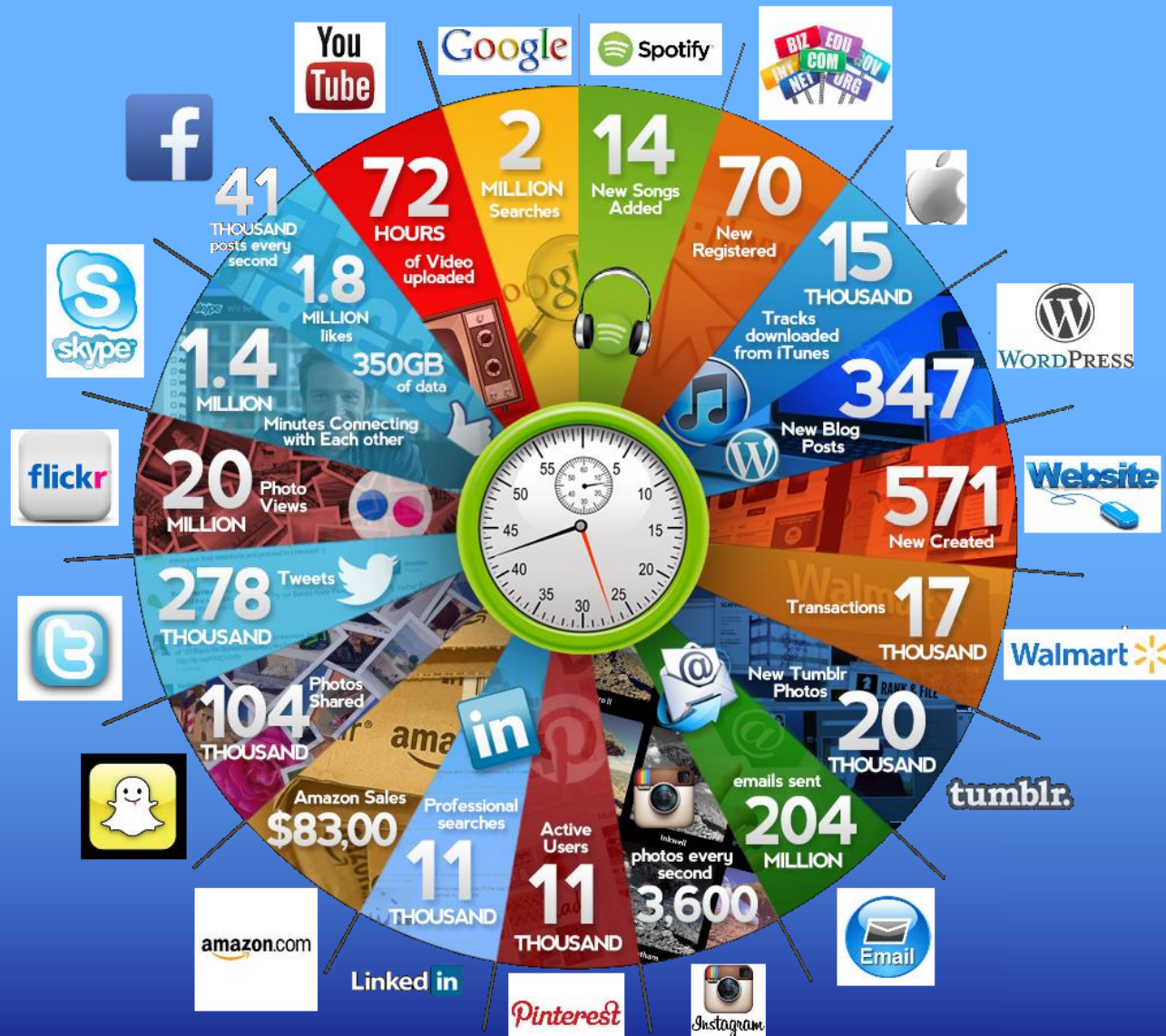
Outline

- Online Social Networks (OSN)
- Open Source Intelligence
- Insider threat and threat parameters
- Exploiting data from OSN
- Behavior prediction capabilities
 - Case 1:** Success story - Insider detection based on Narcissism
 - Case 2:** Success story - Predisposition towards law enforcement
 - Case 3:** Horror story - Identifying political beliefs
- Ethical and legal issues
- Conclusions

Online Social Networks

- OSN and Web 2.0 enable users add online content
- Content can be crawled and utilized for:
 - Personalized advertising
 - Personalized content promotion
 - User/usage profiling
- Can content be crawled and utilized for:
 - Behavior prediction?
 - Psychosocial characteristics extraction?
 - Proactive cyber defense?

What happens online in 60 sec

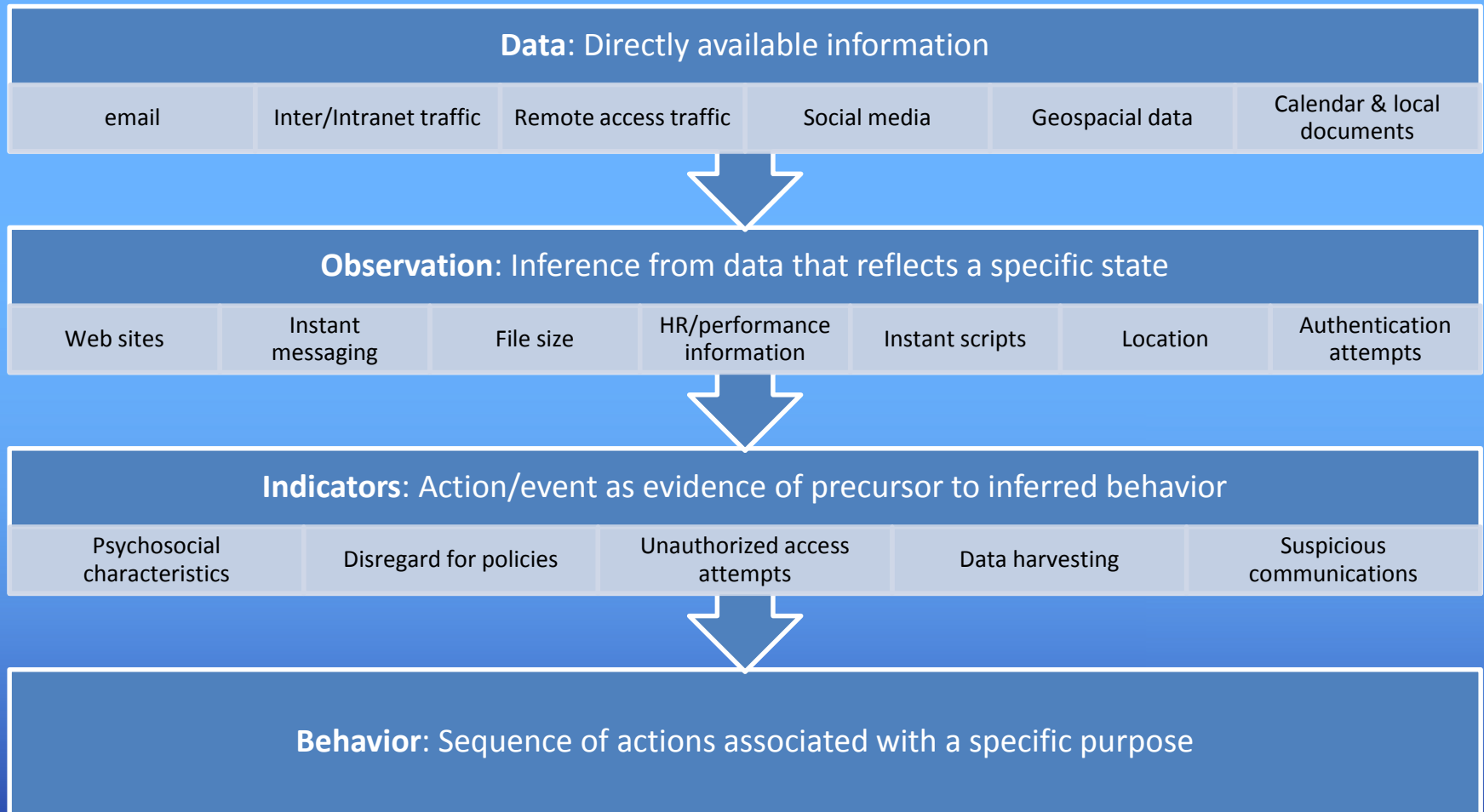


Open Source Intelligence (OSINT)



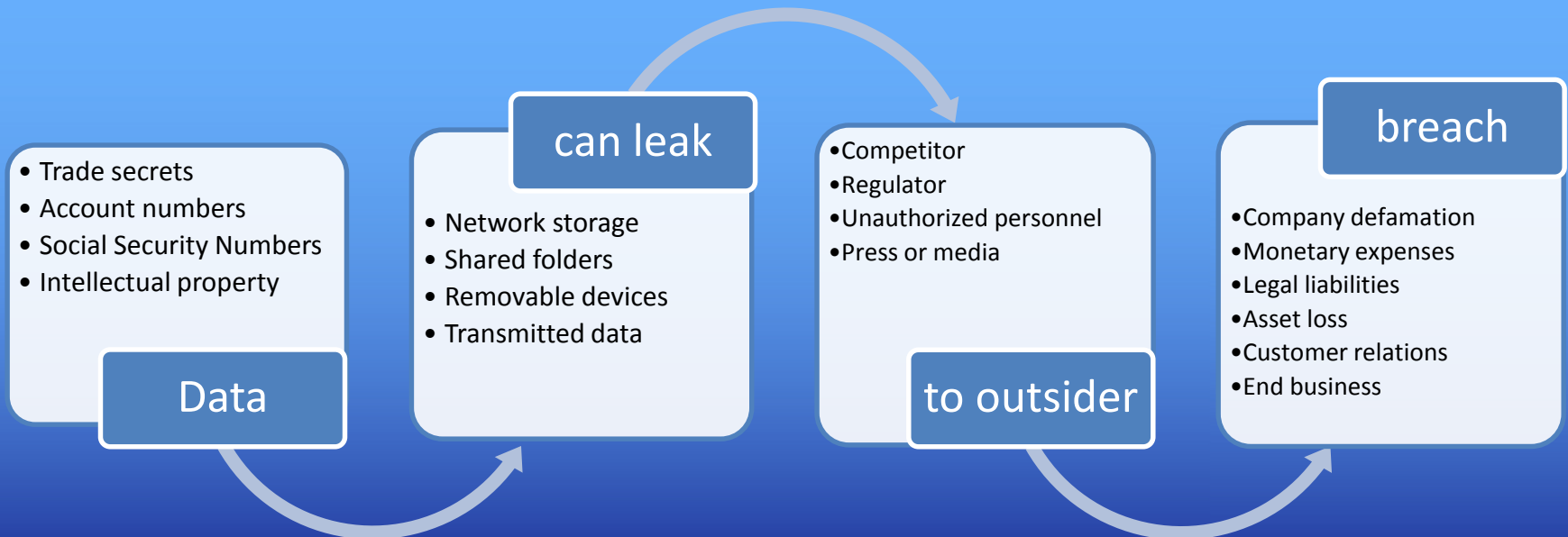
- OSINT (US Dept. of Defense) is produced from **publicly available** information, that is:
 - collected, exploited and disseminated in a **timely** manner
 - offered to an **appropriate** audience
 - used for the purpose of addressing a specific **intelligence requirement**
- Publicly available information refers to (not only):
 - traditional media (e.g. television, newspapers, radio)
 - web-based communities (e.g. social networking sites, blogs)
 - public data (e.g. government reports, official data, hearings)
 - amateur observation and reporting (e.g. amateur spotters, radio monitors)

A generic model for predicting threats



Insider Threat

- A serious threat is the “insider threat”
- Severe problem in cyber/corporate security
- Insider threat originates from persons who:
 - are legitimately given access rights to IS
 - misuse privileges
 - violate security policy

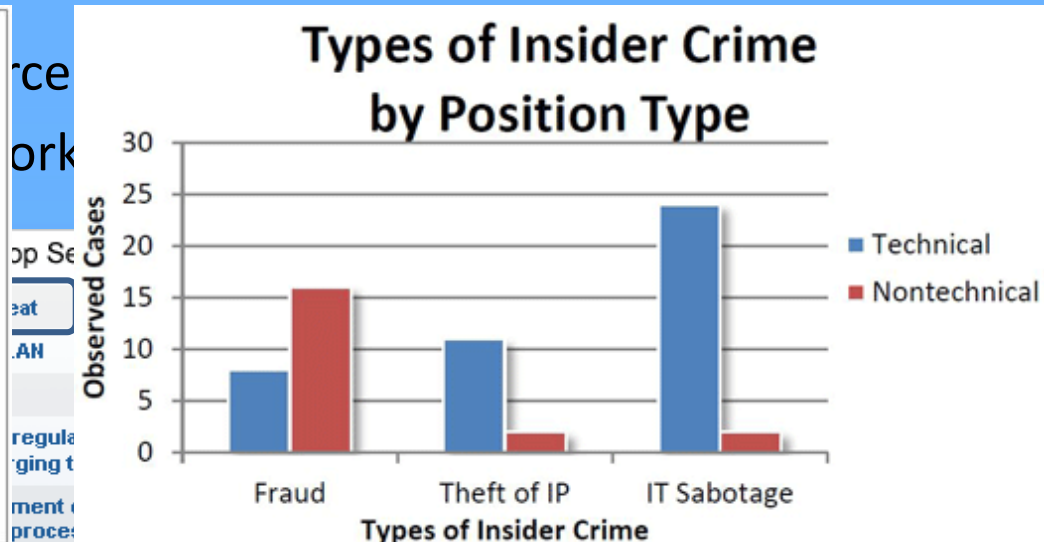
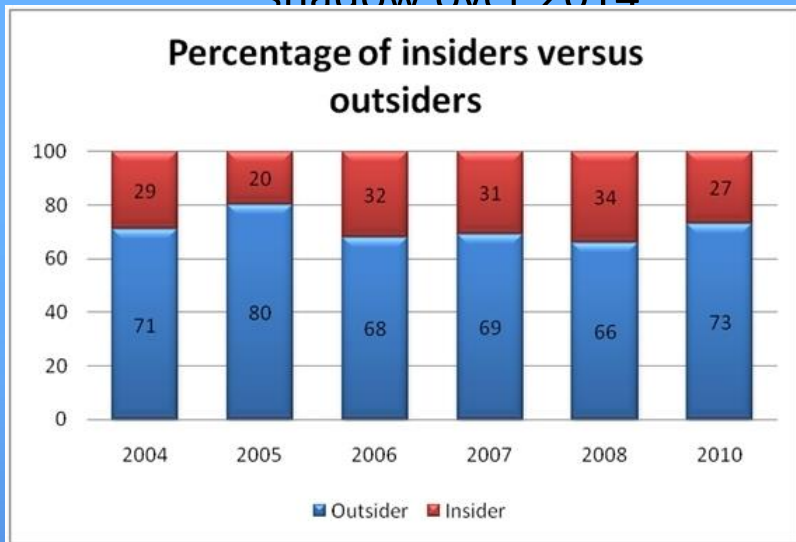


Insider Threat: When is its impact high?

Internal process knowledge Technical literacy	High	Low
High	Highest impact	Insignificant (though demonized) impact
Low	Potentially significant impact	Insignificant impact

Insider Threat severity

- Recognized as one of the most important security issues for 2014
 - The case of former US Government contractor E. Snowden is casting a shadow over 2014



Sources:

<http://www.securityweek.com/ep-10-issues-the-threat-to-2014/> Carnegie Mellon University, USA
<http://www.zdnet.com/asia/it-priorities-survey-2008-09/> ZDNet Asia IT Priorities Survey 2008/09

Threat parameters

- We have a threat if:
 - At least one actor is motivated.
 - **Opportunity** exists.
 - At least one vulnerability exists.
 - Attackers have the skills to exploit the vulnerability.
- Given a threat, a system is vulnerable.

Threat
consists of:

- **Motive**
- Opportunity
- Vulnerability
- Skills

Malevolent user characteristics

- Malevolent users needs:
 - **Opportunity** to unleash prepared attack
 - Egosyntonic¹ or egodystonic² motive
 - In case of egodystonic motive, he further needs ability to **overcome inhibitions**
 - **Approach** and **impulse**
- Under these conditions every user is vulnerable to diversion of loyalty.

Malevolent
user requirem's:

¹ Psychological tendencies that are in harmony with or acceptable to the ego's self-image.

² The opposite of egosyntonic, that are in conflict, or dissonant, with the ego's self-image, or, further, in conflict with a person's ideal self-image.

Personal factors (Shaw)

- According to research most insiders share:

- **Inward turning**, or focused more on internal thoughts, feelings and mood

- Social isolation, **loss of individual will.**

- **Turn** towards depression, reduced productivity, over

- **Lack** of social and personal frustrations

- **Lack** of computer dependency

- Exhibit **ethical “flexibility”**

- **adm**inistrative arrogance

- **Lack** of **Entitlement – Narcissism**

- Lack of empathy

- Are r... state **Predisposition towards law enforcement**

Personal factors

Source: Shaw E., Ruby R., Post S., “The insider threat to information systems: The psychology of the dangerous insider”, *Security Awareness Bulletin*, Vol. 98, No. 2, pp. 1-10, 1998.

Personal factors (FBI)

- According to the FBI model
 - Inordinant
 - Sentimentality
 - for revenge
 - **Problems**
 - **Acceptance**
 - Insecure
 - Deep
 - Prone
 - **Narcissism**
 - **Established** effort.
 - **Performance** (e.g. without leading to an
 - **Problems with relative**
- Greed/financial need
- **Anger/Revenge**
- **Problems at work**
- **Ideology/Identification**
 - **Divided loyalty**
 - Adventure/Thrill
- Vulnerability to blackmail
- **Ego/self-image (Narcissism)**
 - Ingratiation
 - Compulsive and destructive behavior
 - Family problems

Source: FBI, 2012. The Insider Threat: An in

The threat

- **Motive**
- Opportunity
- Vulnerability
- Skills

- Opportunity
- **Motive**
- **Ability to overcome inhibitions**
- Stimulus/impulse

Threat consists of:

Malevolent user requirem's:

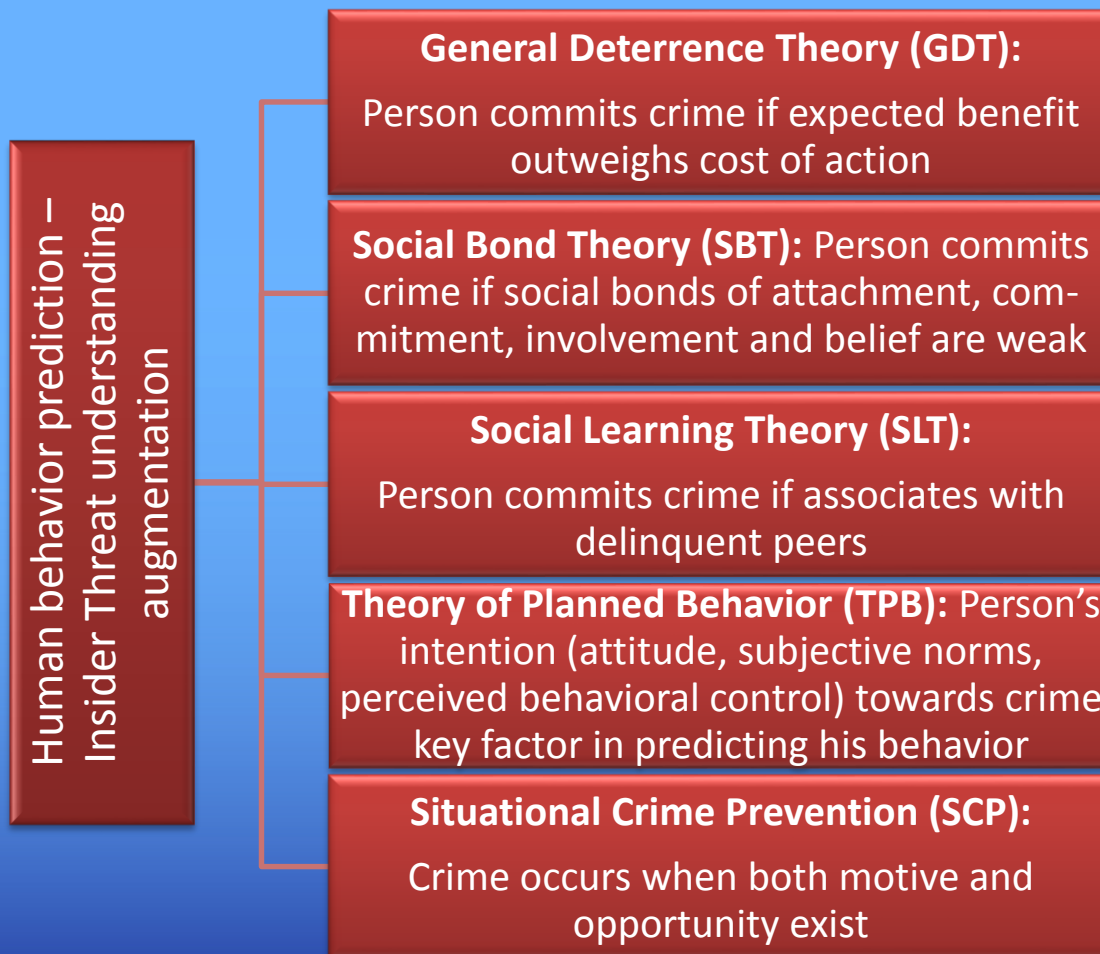
- **Introversion**
- **Social and personal frustrations**
- Computer dependency
- Ethical "flexibility"
- **Reduced loyalty**
- **Entitlement-Narcissism**
- Lack of empathy
- **Predisposition towards law enforcement**

Personal factors (Shaw)

Personal factors (FBI)


- Greed/financial need
- **Anger/Revenge**
- **Problems at work**
- **Ideology/Identification**
- **Divided loyalty**
- Adventure/Thrill
- Vulnerability to blackmail
- **Ego/self-image (Narcissism)**
- Ingratiation
- Compulsive and destructive behavior
- Family problems

Delinquent behavior prediction



Case 1

Scope: Insider threat prediction based on Narcissism

OSINT		OSN: Twitter 
Tools used for the analysis		
Science	Theory	
Computing	Graph Theory	
Sociology	Theory of Planned Behavior	
	Social Learning Theory	

Case 1: Insider threat prediction based on Narcissism



Narcissistic behavior detection

Study: Motive, ego/self-image, entitlement

Means: Usage Intensity, Influence valuation, Klout score

Analyze each user:

- Under the prism of usage deviation
- With graph theoretic tools

Narcissistic behavior is detected through social media popularity and usage intensity

Trait of narcissism is related to delinquent behavior via analysis of:

- Sense of entitlement
- Lack of empathy
- Anger and “revenge” syndrome
- Inflated self-image

Convicted insiders do share this personality trait (narcissism)

Analysis based on:

- Theory of Planned Behavior
- Social Learning Theory



Dataset analysis

Focus on a Greek Twitter community:

- Context sensitive research
- Utilize ethnological features rooted in locality
- Extract and analyze results

Definition of content and measures of user influence

User categories:

- Follower, i.e., somebody who is followed by someone
- Following, i.e., somebody who follows someone
- Retweeter, i.e., somebody who spreads the speech of someone else via tweets

1.075.859 distinct users. 7.125.561 connections among them

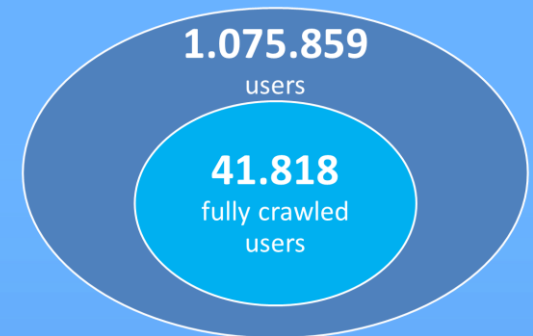
Graph:

- 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)



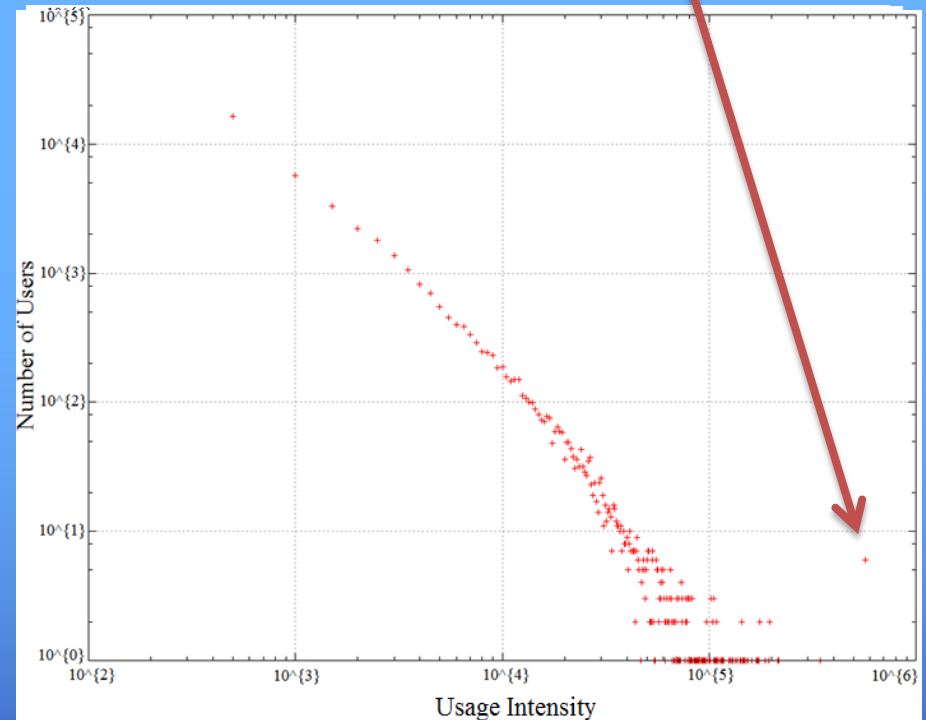
7.125.561 connections
among them

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, followings, tweets, retweets, mentions, favorites, lists}

Important cluster of users






Narcissism detection

- Majority of Greek users make limited use of Twitter
 - A lot of “normally” active users
 - Very few users are popular
- There is a threshold above which:
 - User become quite influential/perform intense medium usage
 - User turns from “normality” to a “mass-media persona” status
- Individuals tend to transfer offline behavior online
 - **Extravert** individuals form large groups and communicate easier
 - **Introvert** individuals communicate less
 - **Excessive usage** of social media connects to **narcissism**

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

Case 2

Scope: Revealing negative attitude
against law enforcement

OSINT		OSN: YouTube 	
Tools used for the analysis			
Science		Theory	
Computing		Machine Learning	
		Data Mining	
Sociology		Social Learning Theory	

Case 2: Revealing negative attitude against law enforcement



Law enforcement predisposition

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

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

- Extract results over users' predispositions
- Analyze each user under the prism of attitude towards law enforcement and authorities
- Individuals tend to transfer offline behavior online
 - Such behavior can be detected through social media
- Trait of negative attitude towards law enforcement is closely related to delinquent behavior via:
 - Sense of entitlement
 - Lack of empathy
 - **Anger and revenge syndrome**
 - Inflated self-image
- Analysis based on Social Learning Theory

Dataset analysis



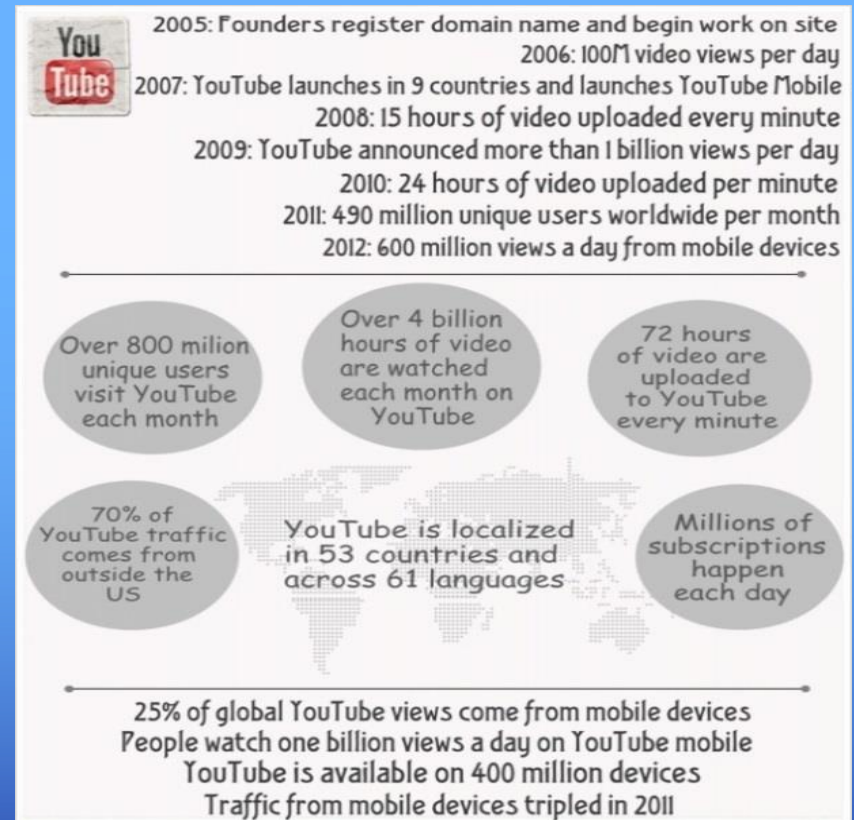
- Crawled YouTube and created dataset consists solely of Greek users
- Utilized YouTube REST-based API (developers.google.com/youtube/)
 - Only publicly available data collected
 - Quote limitations (posed by YouTube) respected
- Gathered data classified into three categories:
 - User-related information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



- Time span of collected data covered 7 years (Nov 2005 - Oct 2012)
- Basic anonymisation layer added to the collected data
 - MD5 hashes instead of usernames

Graph Theoretical and Content Analysis

- **Small World Phenomenon**
 - Every user of the community is 6 hops away from everyone else
- **Indegree Distribution**
 - Presentation of statistical distribution of incoming edges per node
- **Outdegree Distribution**
 - Presentation of statistical distribution of outgoing edges per node
- **Tag Cloud**
 - Axis of content of the collected data via tag cloud analysis
- **YouTube's nature**
 - Popular social medium, emotional-driven responses, audio-visual stimuli, alleged anonymity, users interact with each other, contains political content



Implemented approaches

Examined new
using two ap

- Comment
- Examined
- Performance
- Examined

Approach	Metrics			
	Machine Learning		Flat Data	
Classifier	Logistic Regression		Naïve Bayes	
Classes	P	N	P	N
Precision	86	76	72	93
Recall	74	88	92	73
F-Score	80	81	81	82
Accuracy	81		81	

- Flat Data

– Addressing the problem from a different perspective

- Both approaches achieve similar results

– Design an assumption-free and easy-to-scale method

- Flat data approach behaves slightly more efficiently (better f-score) than machine learning

– Prove (or not) the correctness of machine learning method

- Flat data performs faster than machine learning

- Verifies the results extracted by the Machine Learning approach

ing content
a

their comments

Machine Learning Approach (1)

- Comment classified into categories of interest
 - Process performed as **text classification**
 - Machine trained with **text examples** and **category** they belong to
 - Excessive support by **field expert** (Sociologist)
- Created test set 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
- Significant percentage of comments written in Greek
 - Users write Greek words using Latin alphabet ("**greeklish**")
 - Analyze them as two different languages
 - A converter ("word-by-word") could be also used
- Training sets (greeklish, greek) were merged - One classifier was trained
- Two categories of content were defined:
 - **P**redisposed negatively (P)
 - **N**on-predisposed negatively (N)

Machine Learning Approach (2)

- **Comment classification using:**
 - Naïve Bayes (NB)
 - Support Vector Machines (SVM)
 - Logistic Regression (LR)
- **Compared each classifier efficiency**
 - Metrics (on % basis): Precision, Recall, F-Score, Accuracy
- **Logistic Regression**
 - Model classifies a comment with 81% accuracy
 - Use of precision, recall and f-score to examine classifiers' efficiency

Precision: Measures the classifier exactness. Higher and lower precision means less and more false positive classifications, respectively.

Recall: Measures the classifier completeness. Higher and lower recall means less and more false negative classifications, respectively.

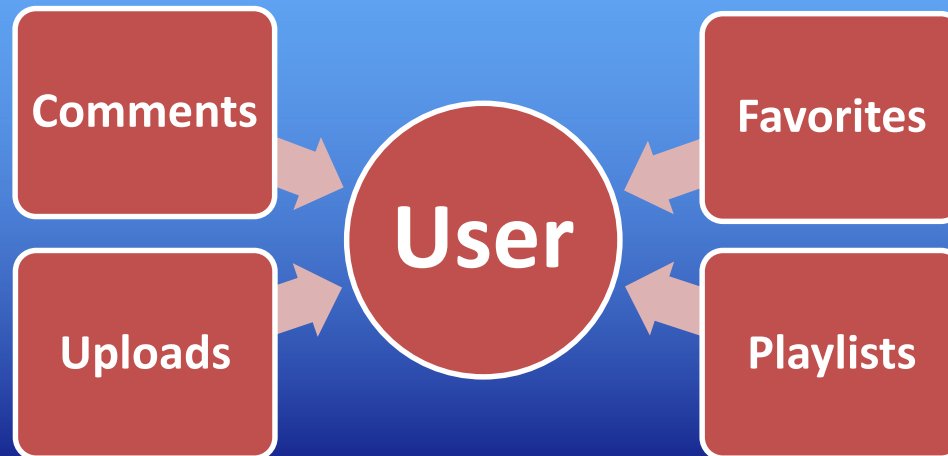
F-Score: Weighted harmonic mean of both metrics.

Accuracy: No. of correct classifications performed by the classifier. Equals to the quotient of good classifications by all data.

Classifier	Metrics					
	NBM		SVM		LR	
Classes	P	N	P	N	P	N
Precision	71	70	83	77	86	76
Recall	72	68	75	82	74	88
<u>F-Score</u>	71	69	79	79.5	80	81
Accuracy	70		80		81	

Machine Learning Approach (3)

- **Video classification**
 - Examination of each video based on its comments
 - Voter process to determine category classification (threshold cut-off at 72% to enhance the possibility that the comment does express the predicted content)
- **(Video) Lists classification**
 - Voter system to determine category classification (same threshold)
- **Conclusions over the user's behavior**
 - At least one category P attribute
 - User is assigned into category P



Example of conclusion extraction (1/2)

- Each comment falls into a category (P or N) based on the classifier's prediction.
- Each video falls into a category based on its comments.

Video "Example"			
Comment	Classifier's output	Likes	Dislikes
#1	P	0	2
#2	P	9	1
#3	N	0	5
#4	P	5	2
#5	N	4	13
#6	P	0	3

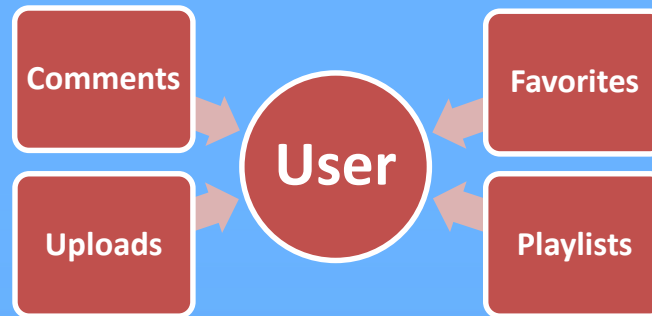
Only comments #2 and #4 will be fed to the voter (if N, then ignore. If no likes and at least 1 dislike, then ignore).

Video contains (at least) 2 negatively Predisposed comments. Thus, it falls into category P.

- The voter decides based on the number of negatively predisposed comments (category P).
- Comments with only dislikes and no likes are excluded
 - If a comment receives only dislikes and no likes, then it is possible that the content of the video has nothing to do with negative attitude towards law enforcement and should not be calculated in the video classification process
- The same approach to extract conclusions applies to list of videos (instead of comments), i.e. user's uploaded videos, favourite videos and playlists.

Example of conclusion extraction (2/2)

- To decide over the user's behaviour the following parameters are examined.



- The voter decides based on a vector that contains the categorization of each one of the above 4 attributes.
- Security Officer may determine threshold cut-off, as well as minimum number of category P comments taken into consideration by voter.
- False positive case: User is classified as P although she is not
 - Such cases mean that there might be an indication that further examination is needed so as to decide whether a user shares this psychosocial characteristic or not.

Flat Data approach (1)

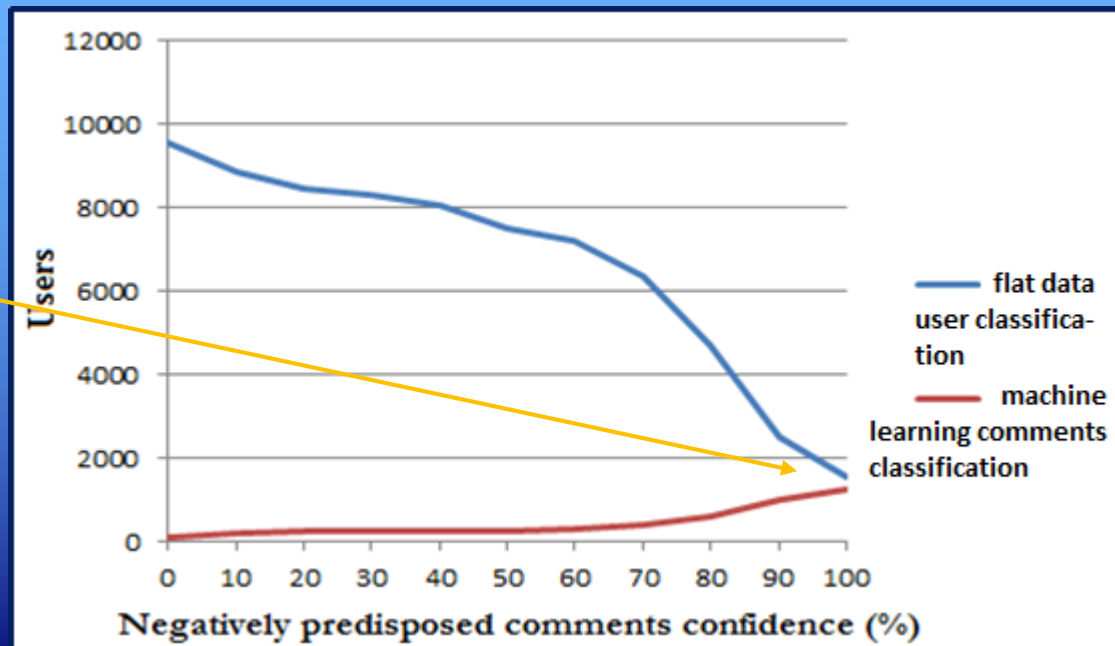
- Addressing the problem from a different perspective
 - Assumption-free and easy-to-scale method
 - Prove (or not) the correctness of the Machine Learning method
 - Machine trained by a set of users of both categories (P, N)
- Data transformation
 - User represented by a (8-)tuple (username, content of comment, video ID the comment refers to, country, age, genre, # of subscribers, # of video views)
- Machine trained by a set of specific users (Sociologist served as field expert)

Naïve Bayes metrics		
Classes	P	N
Precision	72	93
Recall	92	73
F-Score	81	82
Accuracy	81	

Flat Data approach (2)


- Relation between users of category P and confidence of comments belonging to category P
 - Blue** line: Users of category P classified on the basis of the comment-oriented tuple (**Flat Data**)
 - Red** line: Users of category P classified on the basis of their comments-only (**Machine Learning**)
- Confidence level indicates the no. of users who are classified into category P with a specific level of certainty that their comments are classified as P.

1721 users are almost certainly negatively predisposed towards law enforcement!



Case 3

Scope: Identifying Political Beliefs (?)

OSINT		OSN: YouTube 
Tools used for the analysis		
Science	Theory	
Computing	Machine Learning	
	Data Mining	
Political Sociology		

Case 3: Horror story – Identifying Political Beliefs



Divided loyalty

Study: Motive, ideology,
divided/reduced loyalty,
predisposition towards
law enforcement

Means: Machine
Learning, Content
Analysis, comment
classification

Same dataset

Political profiling conclusion extraction


Three (indicative, local context) clusters:

Radical - Neutral - Conservative

Machine Learning and Content Analysis
of the dataset

Analysis based on:

- Social Learning Theory
- General Deterrence Theory



Horror
story

Methodology

- Three (indicative) categories: **Radical**, **Neutral**, **Conservative**
 - Assumptions are context-dependent (Greece, 2007-12)
 - Test case consists of an indicative subset of the Greek community
 - Reflection of the generic political context in Greece
- Defined pairings:
 - **R**adical political affiliation: center-left, left, far-left
 - **N**eutral political affiliation refers to neutral or non-specific political content disclosed
 - **C**onservative political affiliation: center-right, right, far-right
- Classify comments into categories of political affiliation:
 - Comment classification performed as text classification
 - Machine trained with text examples and category they belong to
 - Label assignment required assistance of field expert (Sociologist)

Analysis of results

- **Comment** classification using:
 - Naïve Bayes Multinomial (NBM)
 - Support Vector Machines (SVM)
 - Multinomial Logistic Regression (MLR)
- Comparing each classifier's **efficiency**
 - Metrics (%): Precision, Recall, F-Score, Accuracy
- Multinomial Logistic Regression was chosen
 - MLR classifies appropriately a comment with 87% accuracy
 - Use of precision, recall and f-score to further examine classifiers' efficiency

Precision: Measures the classifier exactness. Higher and lower precision means less and more false positive classifications, respectively.

Recall: Measures the classifier completeness. Higher /lower recall means less/ more false negative classifications, respectively.

F-Score: Weighted harmonic mean of both metrics.

Accuracy: No. of correct classifications performed by the classifier. Equals to the quotient of good classifications by all the data.

Classifier	Metrics								
	NBM			SVM			MLR		
Classes	R	N	C	R	N	C	R	N	C
Precision	65	93	55	75	91	74	83	91	77
Recall	83	56	85	80	89	73	77	93	78
<u>F-Score</u>	73	70	60	76	89	73	80	92	77
Accuracy	68			84			87		

Conclusions (1/2)

- Each **comment** falls into a category, based on the classifier's prediction
- Each **video** falls into a category based on its **comments**

Video "Example"			
Comment	Political affiliation	Likes	Dislikes
#1	R	90	10
#2	C	15	20
#3	R	30	5
#4	N	5	2
#5	R	10	3
Total		150	40

All comments are taken into account.

Like means "approve" and dislike means "not approve"

$$R = (1+90/150-10/40) + (1+30/150-5/40) + (1+10/150-3/40) = 4.1$$

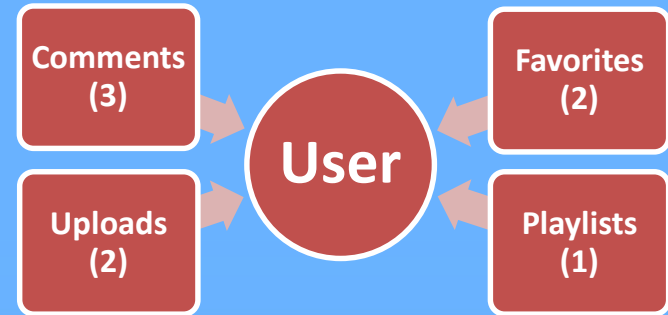
$$C = (1+15/150-20/40) = 0.6$$

$R > C$ then the video is classified as R

- Two sums are calculated (i.e. R,C).
- For every comment in a video we calculate: $1 + \{(likes/(total_likes)) - (dislikes/(total_dislikes))\}$
- The greater sum indicates the category the video falls into
- Same applies to list of videos, i.e. user's uploaded videos, favourite videos and playlists

Conclusions (2/2)

- User content is now classified. Then, four parameters (comment, upload, favorite, playlist) are calculated by the voter in order to identify the user's beliefs.



- Each parameter gets a weight from the voter (as user comments forms the most direct way to express opinions).
- Search for indications of direct political affiliation expression in the uploaded and favourite videos and in the playlists

User classification example:

User "Example"		
	Political beliefs	Weight
Comments	R	3
Uploaded videos	N	2
Favorite videos	R	2
Playlists	C	1

$$R = 3 + 2 = 5$$

$$C = 1$$

$R > C$, i.e. the user belongs to category R

Observations (1/2)

2% of **comments** demonstrate political affiliation (0.7% Radical, 1.3% Conservative)

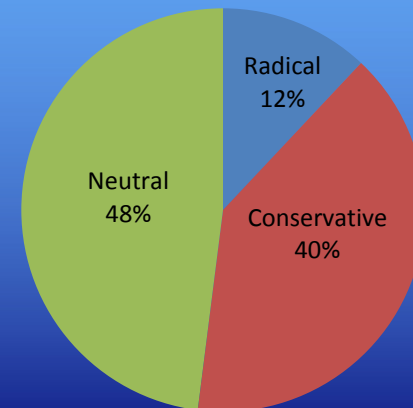
- 2% means that almost **41.000 comments** (of the 2.000.000 collected) include political content

7% of **videos** classified into one category (2% Radical, 5% Conservative)

- 7% means that almost **14.000 videos** (of the 200.000 collected) include political content

12% of **users** express **Radical** political affiliation and 40% **Conservative** affiliation

- 52% means that **6.760 users** were revealing - one way or another - their political beliefs!



Observations (2/2)

Radicals:

- 20% of their comments includes political position
- Prefer Greek alphabet (i.e., 54% comments in Greek, 33% in greeklish, 13% use both)
- Massively comment on the same videos
- Prefer videos with political content (political events, music, incidents of police brutality)
- Add to favourites documentaries and political music clips

Conservatives:

- Prefer greeklish in comments (i.e., 55% greeklish, 35% Greek, 10% both)
- Often share conspiracy-based and nationalistic content videos

Greeklish comments are usually shorter and aggressive

Greek comments are usually explanatory, polite and longer

The more aggressive a comment, the more misspelled

7% of videos published under Creative Commons license

- 55% uploaded by Radicals, 10% by Conservatives, 35% by Neutrals

Exploitation paths

- **Insider threat prediction**
 - Adopting Shaw and FBI psychosocial indicators (narcissism, anger and revenge syndrome, etc.)
- **Delinquent behavior prediction**
 - Analysis of psychosocial characteristics (narcissism, anger and revenge syndrome, etc.)
 - Predisposition analysis (graph theory and content analysis through social learning theory, etc.)
- **Forensics analysis support**
 - Suspect profiling and analysis (proactive prediction of delinquent behavior, etc.)

Ethical and legal issues

- Users are **not** aware of the actual reach of the information they reveal
- The methods used for OSINT may:
 - be associated with discrimination and prejudice risks
 - infringe human rights (freedom of speech, conception of identity, privacy, etc.).
 - cause self-censorship and self-oppression
 - cause visible problems both in the workplace and the social environment
 - pose a threat of marginalization (employers or rigid micro-societies)
- Online Social Networks offer privacy options which **do not really** help
- Private profiles are still **indirectly crawlable**
- **Laws prohibit** the process of data revealing psychosocial characteristics
- Derogations are allowed:
 - On a legal manifest of public interest
 - If given an explicit, informed, and written consent of the person concerned
 - For processing relates to data made public by the data subject

Conclusions

- ✓ Online Social Networks produce vast amounts of crawlable information
- ✓ **OSINT** may transform this information to intelligence
- ✓ **Right now** we are able to:
 - ✓ Detect narcissistic behavior, predisposition towards law enforcement, divided political loyalty, group analysis, etc.
- ✓ Exploitation of these results may :
 - ✓ Predict insider threat, predict delinquent behavior, help law enforcement
- ✓ Online Social Networks data exploitation may lead to **horror stories**
- ✓ Intrusive nature dictates **limited** usage (e.g. Critical Infrastructure)
- ✓ **Proactive cyber defense** with the use of OSINT is feasible

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* (NMITS-2014), Springer, UAE, 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, Athens, 2014.
3. 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.
4. Kandias M., Galbogni 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. Mitrou L., Kandias M., Stavrou V., Gritzalis D., "Social media profiling: A Panopticon or Omnipticon tool?", in *Proc. of the 6th Conference of the Surveillance Studies Network*, Spain, 2014.
10. Mylonas A., Kastania A., Gritzalis D., "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, pp. 47-66, May 2013.
11. Mylonas A., Meletiadiis V., Tsoumas B. Mitrou L., Gritzalis D., "Dynamic evidence acquisition for smartphone forensics", in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, pp. 245-256, Springer (AICT 267), Greece, 2012.
12. Mylonas A., Dritsas S, Tsoumas V., Gritzalis D., "Smartphone Security Evaluation - The Malware Attack Case", in *Proc. of the 9th International Conference on Security and Cryptography* (SECRYPT-2011), pp. 25-36, SciTekPress, Spain, 2011.
13. Mylonas A., Meletiadiis V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security*, Vol. 38, pp. 51-75, October 2013.
14. 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.
15. Stavrou V., Kandias M., Karoulas G., Gritzalis D., "Business Process Modeling for Insider threat monitoring and handling", in *Proc. of the 11th International Conference on Trust, Privacy & Security in Digital Business* (TRUSTBUS-2014), Springer, Germany, 2014.
16. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer Criticality Assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.
17. 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.
18. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability* (ICGS3-2011), pp. 171-178, Springer (LNICST 0099), Greece, 2012.
19. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent critical infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
20. Stachtiari E., Soupionis Y., Katsaros P., Mentis A., Gritzalis D., "Probabilistic model checking of CAPTCHA admission control for DoS resistant anti-SPIT protection", in *Proc. of the 7th International Workshop on Critical Information Infrastructures Security* (CRITIS-2012), pp. 143-154, Springer (LNCS 7722), Norway, 2012.