

Open Source and Social Media Intelligence at Your Service



ΣΕΘΑ
Σχολή Εθνικής Άμυνας



ΟΠΑ
ΑΥΕΒ

Καθηγητής Δημήτρης Γκριτζαλης

Διευθυντής Εργαστηρίου Ασφάλειας Πληροφοριών &
Προστασίας Κρίσιμων Υποδομών (INFOSEC Laboratory)
Τμήμα Πληροφορικής | Οικονομικό Πανεπιστήμιο Αθηνών



InfoSec

Ποιοί είμαστε και ποια ζητήματα ερευνούμε

Ακαδημαϊκή Μονάδα:

Εργαστήριο Ασφάλειας Πληροφοριών & Προστασίας Κρίσιμων Υποδομών
(INFOSEC Laboratory)

Τμήμα Πληροφορικής | Οικονομικό Πανεπιστήμιο Αθηνών
www.infosec.aueb.gr

Περιοχές Έρευνας & Τεχνολογικής Ανάπτυξης:

Ασφάλεια Πληροφοριών | Προστασία Κρίσιμων Υποδομών

Ψηφιακά Κοινωνικά Δίκτυα | **Open Source Intelligence**

Προστασία Ιδιωτικότητας | Ψηφιακά Τεκμήρια

Ένα motto μας:

«Αἱ τιμαὶ μεγάλαι, ἂν ἀποκτείνῃ τις οὐ κλέπτην ἀλλὰ τύραννον»

Αριστοτέλης



Τι θα παρουσιάσουμε στη σημερινή συνεργασία

Εισαγωγή

Big Data

Online Social Networks

Data Analytics - Visualization

Open Source and Social Media Intelligence

Ελπίδα

Προστασία ζωής και δικαιωμάτων πολιτών: Αποτροπή αυτοκτονιών

Φόβος

Αποκάλυψη προσωπικών δεδομένων: Πολιτικές πεποιθήσεις

Ελπίδα

Ενίσχυση δημοκρατικής συμμετοχής: Διαδικτυακές/ηλεκτρονικές εκλογές

Ελπίδα

Αντιμετώπιση απειλών: Η «εκ των έσω» απειλή

Ελπίδα & φόβος

Χειραγώγηση/έκφραση απόψεων πολιτών: The Moneyball case

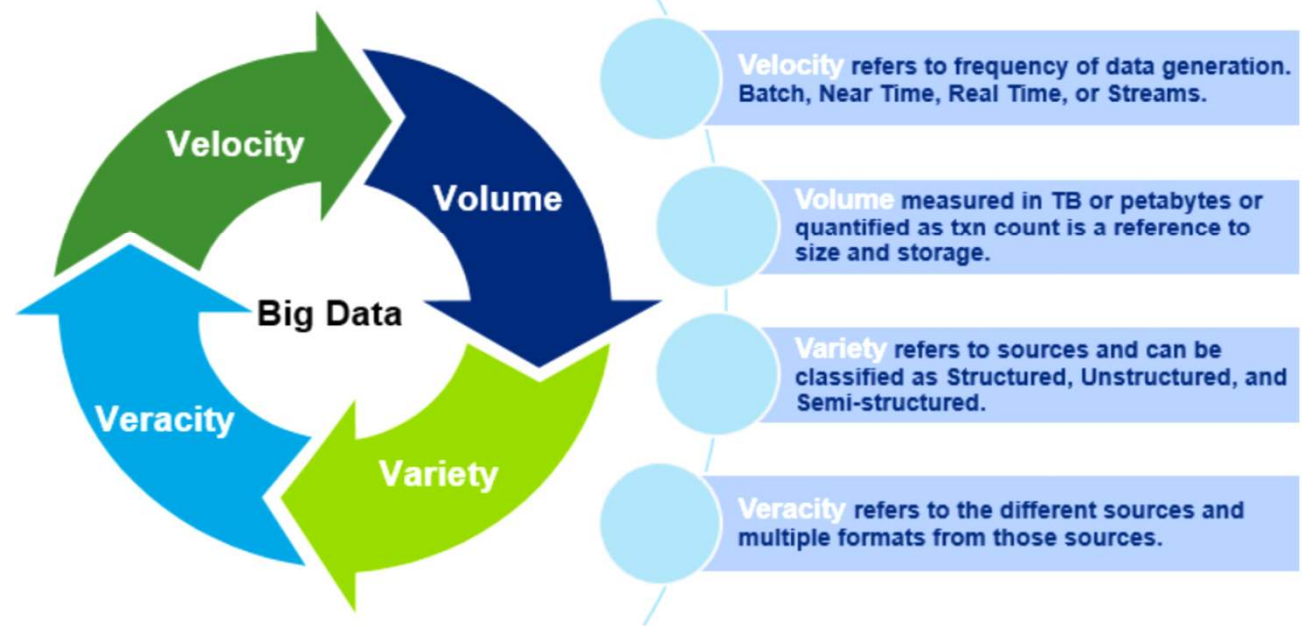
Συμπεράσματα



Big Data: Ένας Πακτωλός με ...4V



A whole new class of inputs driven by an explosion in the volume of data being created by social media, machines, intelligent devices, and other applications that is creating new challenges and opportunities.

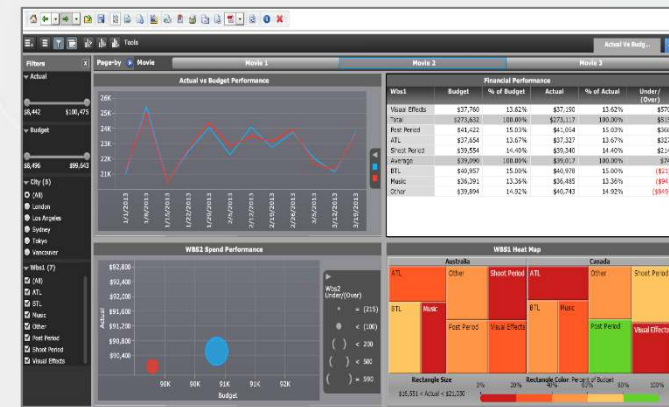
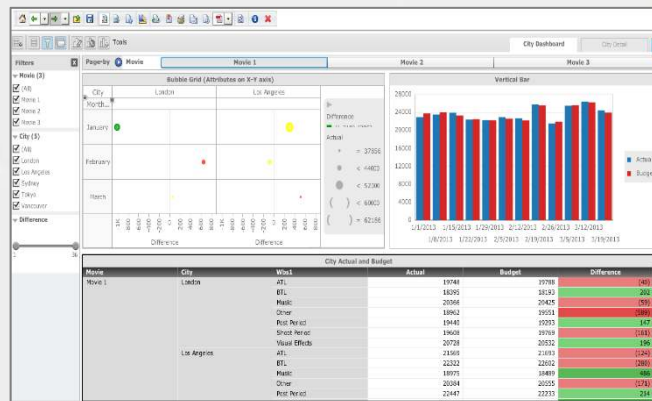
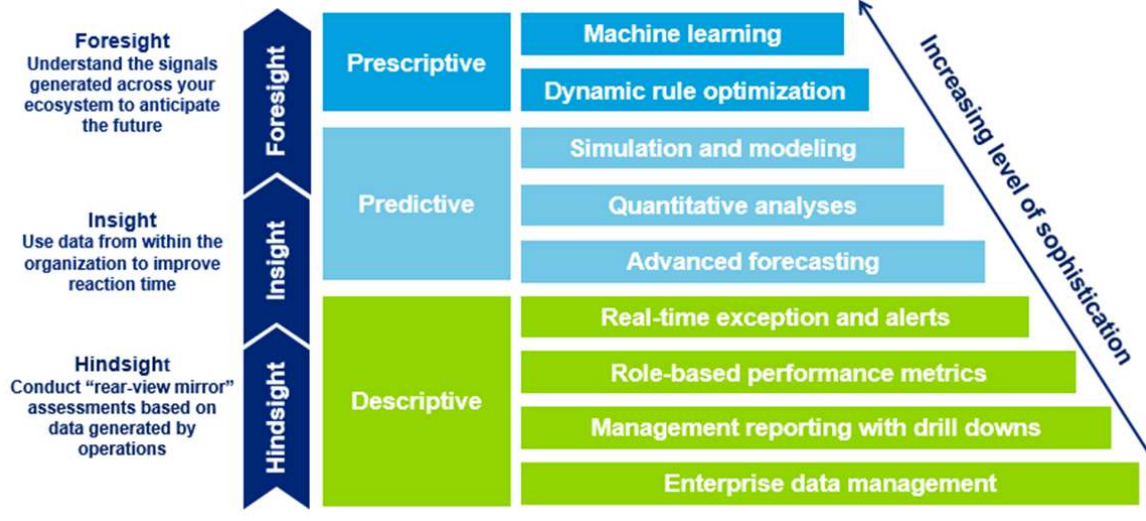


4V: Velocity (Ρυθμός), **Volume** (Όγκος), **Variety** (Ποικιλία), **Veracity** (Εγκυρότητα)

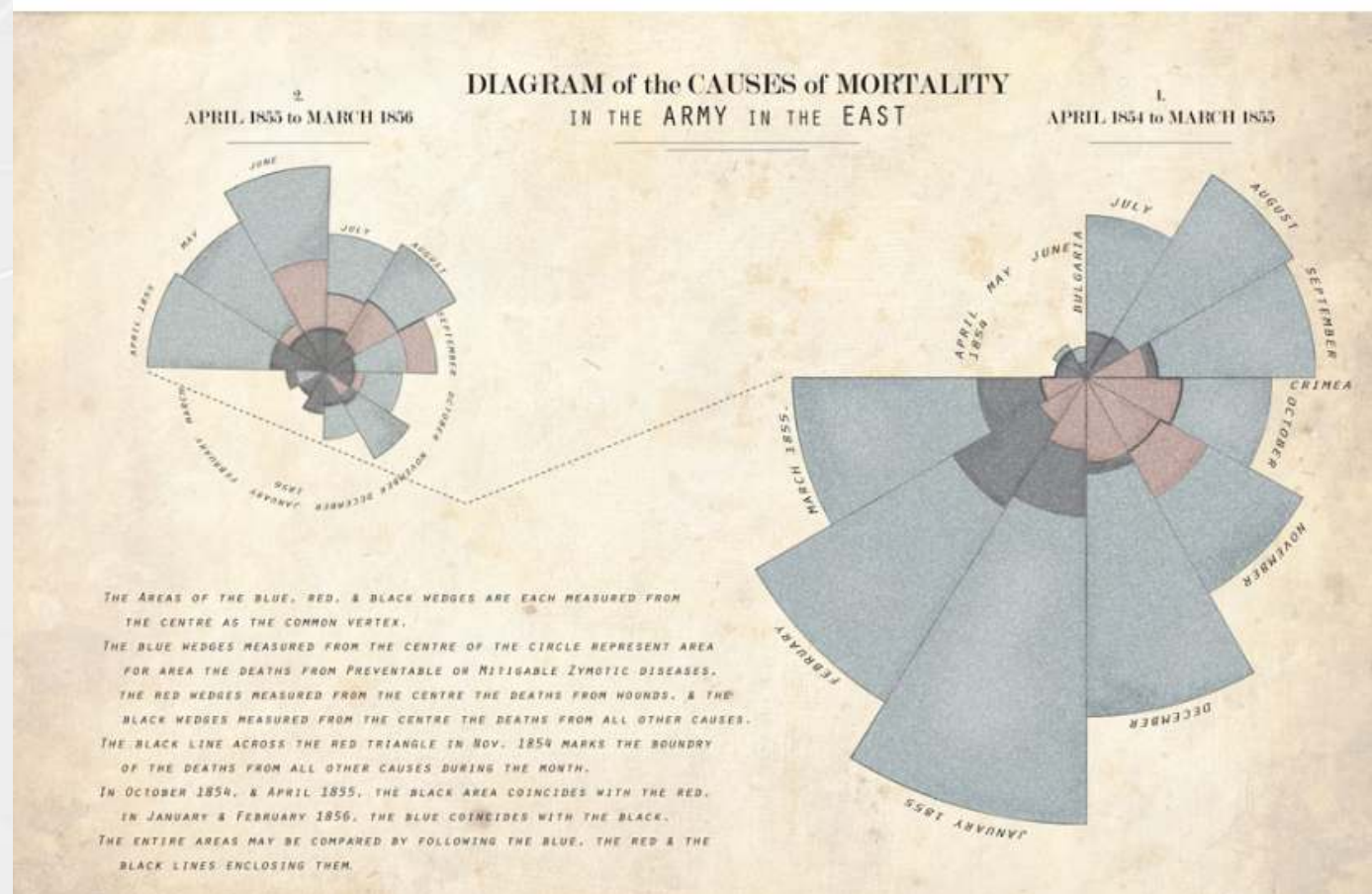


Data Analytics - Open Source Intelligence - Visualization: Πεδίον δόξης (;) λαμπρόν

Analytics is using data to make smarter decisions that support effective management, improve performance, and drive business transformation.



Data Analytics - Open Source Intelligence - Visualization: Παρόντα, εδώ και πολλά χρόνια



Visualization of Causes of Mortality (F. Nightingale, 1855)



Open Source Intelligence (OSINT): Ανάλυση δημόσια διαθέσιμων δεδομένων

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

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

Publicly available information (mainly) refers to:

- 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 reporting (e.g. amateur spotters, radio monitors)

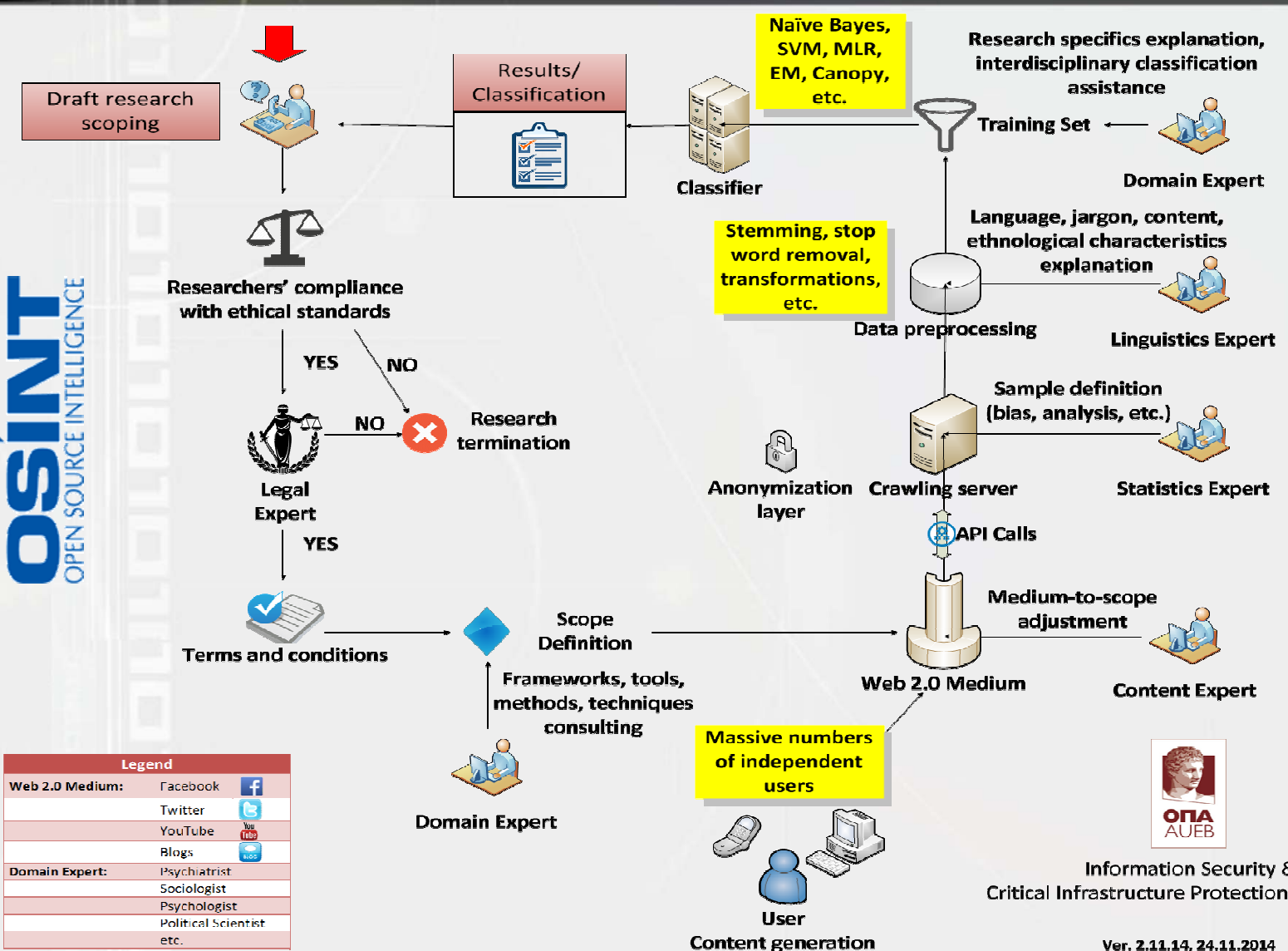
OSINT defined by US Dept. of Defense (Public Law 109-163, Sec. 931, "National Defense Authorization Act for Fiscal Year 2006")

Social Media Intelligence (SOCMINT) is produced from Online Social Networks and the Web 2.0



Open Source Intelligence: Ανάλυση δημόσια διαθέσιμων δεδομένων

OSINT
OPEN SOURCE INTELLIGENCE



Legend	
Web 2.0 Medium:	Facebook
	Twitter
	YouTube
	Blogs
Domain Expert:	Psychiatrist
	Sociologist
	Psychologist
	Political Scientist
	etc.



Information Security & Critical Infrastructure Protection Laboratory



Η ελπίδα:

Προστασία (ζωής & δικαιωμάτων) πολιτών

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα

Αναρτήσεις σε δικτυακούς τόπους και OSN

Πρόσφορο πεδίο εφαρμογής

Έκφραση αρνητικού συναισθήματος, έκφραση επιθετικότητας, εκδήλωση λεκτικών επιθέσεων, συναισθηματική φόρτιση κλπ.

Μέθοδοι ανάλυσης

Βάση Δεδομένων (με σχετική τεκμηρίωση)

Ανάλυση περιεχομένου (Opinion Mining, Machine Learning)

Ανάλυση νέφους ετικετών (Tag Cloud Analysis)





Προς επίρρωση της ελπίδας: Αποτροπή αυτοκτονιών

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα

Απειλές αυτοκτονίας (με αναλυτική σχετική τεκμηρίωση)

Προϋποθέτει άδεια/συνεργασία με αρμόδιους θεσμικούς εταίρους

Πρόσφορο πεδίο εφαρμογής

Έκφραση αρνητικού συναισθήματος, απειλή αυτοκτονίας

σχολιασμός σχετικών αναρτήσεων, συναισθηματική φόρτιση

Μέθοδοι ανάλυσης

Βάση Δεδομένων (με σχετική τεκμηρίωση)

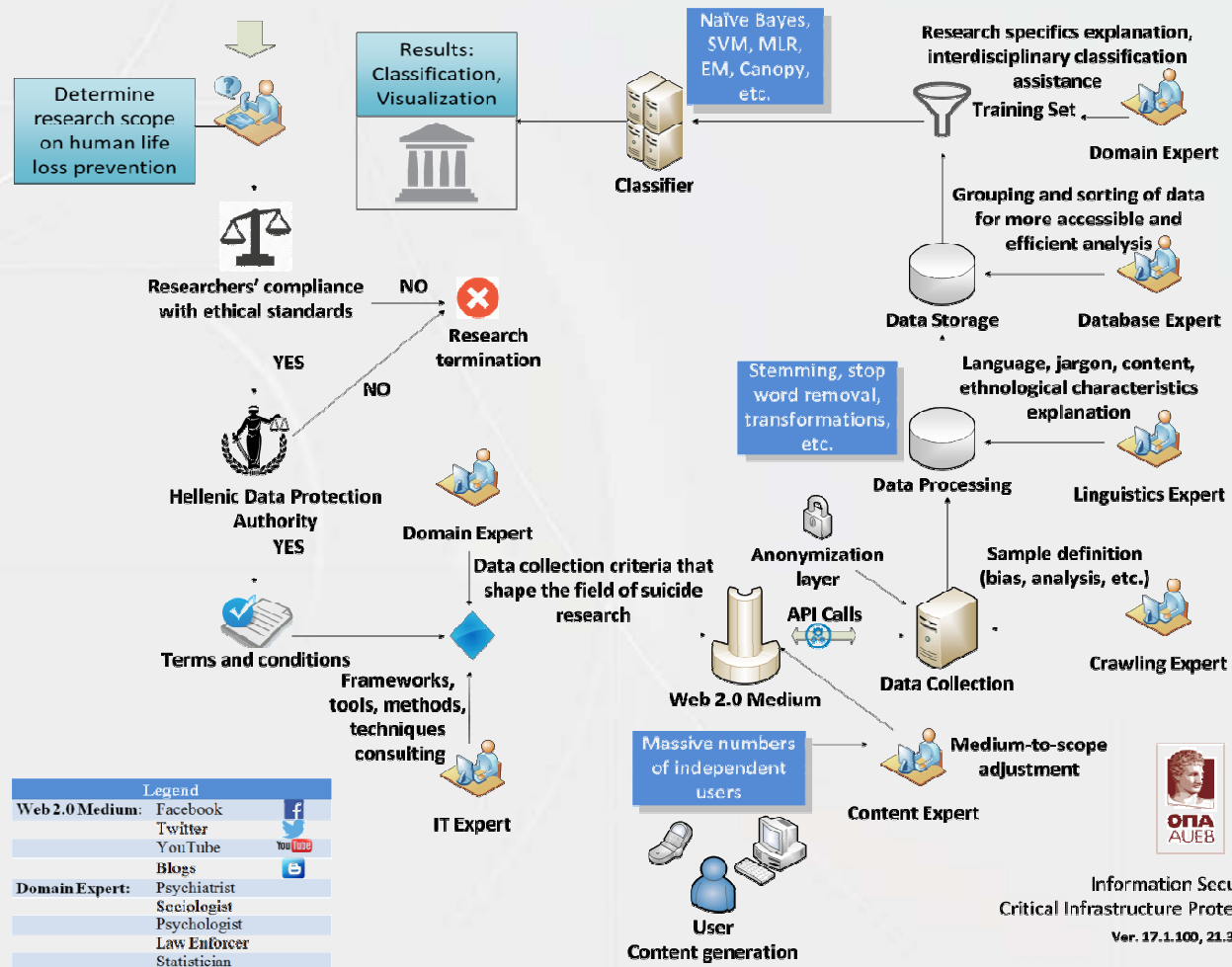
Ανάλυση περιεχομένου (Opinion Mining, Machine Learning)





Προς επίρρωση της ελπίδας: Αποτροπή αυτοκτονιών

INFOSEC Lab: Social Media Intelligence methodology





Ο φόβος:

Αποκάλυψη προσωπικών δεδομένων

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα (Ελλάδα, 11/2005 - 12/2012)

12.964 χρήστες, 207.377 βίντεο, 2.034.362 σχόλια

Πρόσφορο πεδίο εφαρμογής

Πολιτικό περιεχόμενο, οπτικοακουστικά ερεθίσματα, συναισθηματική φόρτιση, ευρεία συμμετοχή χρηστών

Μέθοδοι ανάλυσης

Γραφοθεωρητική Ανάλυση (Small World Phenomenon, Indegree/Outdegree Distribution, Node Loneliness)

Ανάλυση Περιεχομένου (Opinion Mining, Machine Learning)

Ανάλυση Νέφους Κλάσεων (Tag Cloud Analysis)





Προς επίρρωση του φόβου: Αποκάλυψη πολιτικών πεποιθήσεων

Αλγόριθμος: Multinomial Logistic Regression (MLR)

Πολιτική επιλογή Μετρικές	Κεντροαριστερά - Αριστερά	Ουδετερότητα - Μη ένταξη	Δεξιά - Κεντροδεξιά
Precision	83%	91%	77%
Recall	77%	93%	78%
F-Score	80%	92%	77%
Accuracy	87%		

Precision: Χρήστες που κατηγοριοποιήθηκαν σωστά, δια του πλήθους των χρηστών της κατηγορίας αυτής.

F-Score: Σταθμισμένος αρμονικός μέσος **Precision** και **Recall**.

Recall: Χρήστες που κατηγοριοποιήθηκαν σωστά δια του πλήθους όλων των χρηστών της κατηγορίας αυτής.

Accuracy: Ποσοστό ορθών κατηγοριοποιήσεων (πηλίκο ορθών κατηγοριοποιήσεων δια του συνόλου).





Η ελπίδα:

Ενίσχυση δημοκρατικής συμμετοχής

Internet & Web 2.0



Χρήστες

Φυσικά πρόσωπα που επιθυμούν να συμμετάσχουν (από απόσταση) σε δημοκρατικές διαδικασίες ή σε άλλες διαδικασίες έκφρασης γνώμης.

Φυσικά πρόσωπα με ειδικές ανάγκες ή με δυσκολία φυσικής προσπέλασης σε χώρους όπου εκφράζονται επιλογές/απόψεις

Πρόσφορο πεδίο εφαρμογής

Γενικές/περιφερειακές/τοπικές εκλογές, δημοψηφίσματα, δημοσκοπήσεις κλπ.

Μέσα/μέθοδοι έκφρασης γνώμης

Διαδίκτυο & Παγκόσμιος Ιστός
Ειδικές Ψηφιακές Τεχνολογίες





Προς επίρρωση της ελπίδας: Διαδικτυακές/ηλεκτρονικές εκλογές

Internet & Web 2.0



Χρήστες

Πολίτες, δημότες, τοπικές κοινωνίες, άτομα με ειδικές ανάγκες, εργαζόμενοι, παραγωγοί, καταναλωτές κλπ.

Πρόσφορο πεδίο εφαρμογής

Γενικές/περιφερειακές/τοπικές εκλογές, δημοψηφίσματα, δημοσκοπήσεις, έκφραση γνώμης κλπ.

Μέσα & μέθοδοι έκφρασης γνώμης

Ψηφιακά μέσα ψηφοφορίας
Ψηφοφορία μέσω Διαδικτύου

Ειδικές συνθήκες & απαιτήσεις

Ανάγκη ισχυρών εγγυήσεων (ασφάλεια, αξιοπιστία κλπ.)
Επίδραση «ψηφιακού χάσματος» (digital divide)





Προς επίρρωση της ελπίδας: The insider threat

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα (Ελλάδα, 2012-13)

1.075.879 χρήστες, 41.818 fully crawled χρήστες, 7.125.561 user connections

Συλλεγόμενα δεδομένα

Name, ID, personal description, URL, language, geolocation, profile state, lists, # of following/followers, tweets, # of favorites, # of mentions, # of retweets

Μέθοδοι ανάλυσης

Γραφοθεωρητική Ανάλυση (Small World Phenomenon, Indegree/Outdegree Distribution, Node Loneliness)

Ανάλυση Περιεχομένου (Opinion Mining, Machine Learning)

Επιρροή Χρηστών & Ένταση Χρήσης (User Influence & Usage Intensity)





Προς επίρρωση της ελπίδας: Insider threat?

Insiders are persons who:

- are **legitimately** given access rights to an information system or critical infrastructure
- **misuse** their privileges and **violate** security policy

The Insider Threat

		Internal Process Knowledge	
		High	Low
Technical Literacy	High	Greatest Threat	Demonized But Insignificant
	Low	Significant Threat	Insignificant

Source: GartnerGroup
Report 5605





Προς επίρρωση της ελπίδας: Εντοπισμός insiders

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

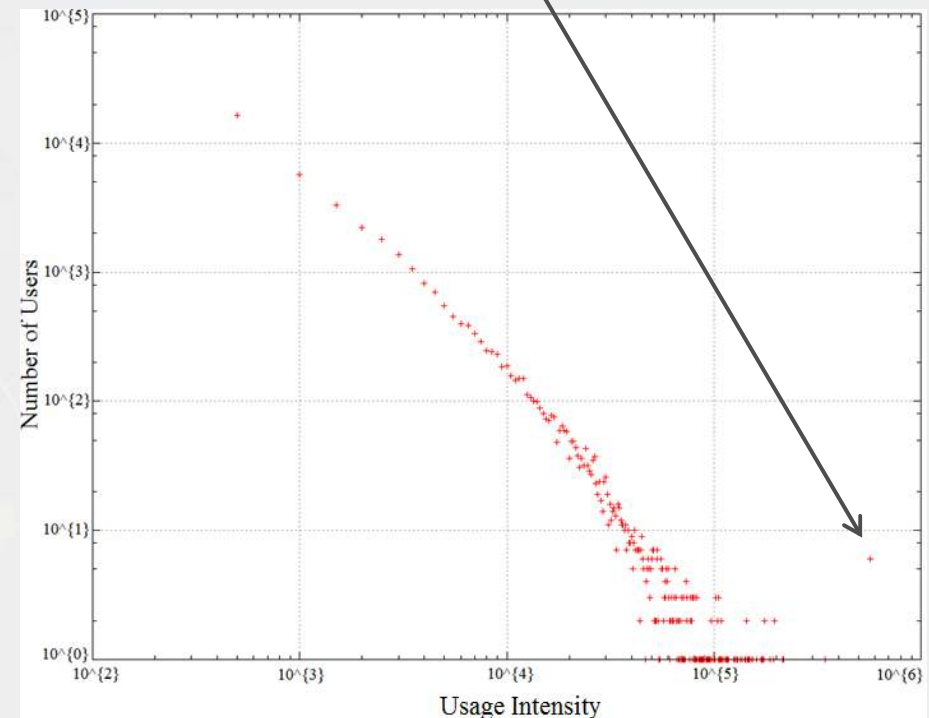
Outdegree Distribution:

of users each user follows
Average 11 followers/user

Usage Intensity Distribution:

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

Cluster of users with narcissistic behavior



Theoretical basis:

- (1). Narcissists tend to turn into insiders.
- (2). Individuals tend to transfer offline behavior online





Φόβος/Ελπίδα: Χειραγώγηση/έκφραση απόψεων πολιτών

Internet & Online Social Networks



Μεθοδολογίες ανάλυσης



Δεδομένα

Αναρτήσεις (σχόλια) πολιτών-ψηφοφόρων

Πρόσφορο πεδίο εφαρμογής

Πολιτικές επιλογές πολιτών, (αν)επιθυμητές πολιτικές αποφάσεις, οπτικοακουστικά ερεθίσματα, διατύπωση αιτημάτων/απόψεων

Μέθοδοι ανάλυσης

Ανάλυση Περιεχομένου (Opinion Mining, Machine Learning)

Control & Treatment Groups (testing messages to voters)

Database Querying





Προς επίρρωση φόβου/ελπίδας: Moneyball: Maximizing votes per \$

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα

Απόψεις ψηφοφόρων (ΗΠΑ, Obama-2012, Big Data in Politics, 100M\$)

Πρόσφορο πεδίο εφαρμογής

Στοχευμένες επιλογές πολιτικής δράσης (ανά Πολιτεία, πόλη, κοινωνική ομάδα, επαγγελματική ομάδα, φύλο, φυλή κλπ.)

Μέθοδοι ανάλυσης

CATALIST Database (& for-profit Venture) (2 PetaBytes)

Ανάλυση Περιεχομένου (Opinion Mining, Machine Learning)

Time/effort Maximization Algorithms (i.e. "don't knock on that door")

Control & Treatment Groups (testing messages to voters)

Decentralized-over-the-phone volunteers (VoIP)



Open Source and Social Media Intelligence at Your (whose?) Service

- ✓ **Ελπίδα και Φόβος**
- ✓ **Άμυνα και Απειλή**
- ✓ **«Άγια Ανησυχία» (Σήμα Κινδύνου, Α. Σαμαράκης)**
- ✓ **Ταξικότητα των ΤΠΕ (;)**



References

1. Gritzalis D., *Secure Electronic Voting*, Springer, USA, 2003.
2. 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.
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. 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, Greece, 2014.
5. 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.
6. 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, 2013.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures in Critical Infrastructures", in *Proc. of the 7th IFIP Inter-national Conference on Critical Infrastructure Protection (CIP-2013)*, pp. 171-182, Springer (AICT 417), USA, 2013.
13. 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.
14. 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)*, pp. 119-131, Springer (LNCS 8647), Germany, 2014.