

Online Social Networks: Enhancing Social Welfare and Supporting National Defense



Dimitris Gritzalis

April 2016

Ψηφιακά Κοινωνικά Δίκτυα: Ελπίδα ή Απειλή για την Εθνική Άμυνα και την Κοινωνική Ευημερία;



CONFERENCE 2016
EXPOSEC
DEFENSEWORLD

April 12 & 13, Athens Ledra Hotel
Greece at the center
of geopolitical changes
and migration flows
Security in Southeastern Europe



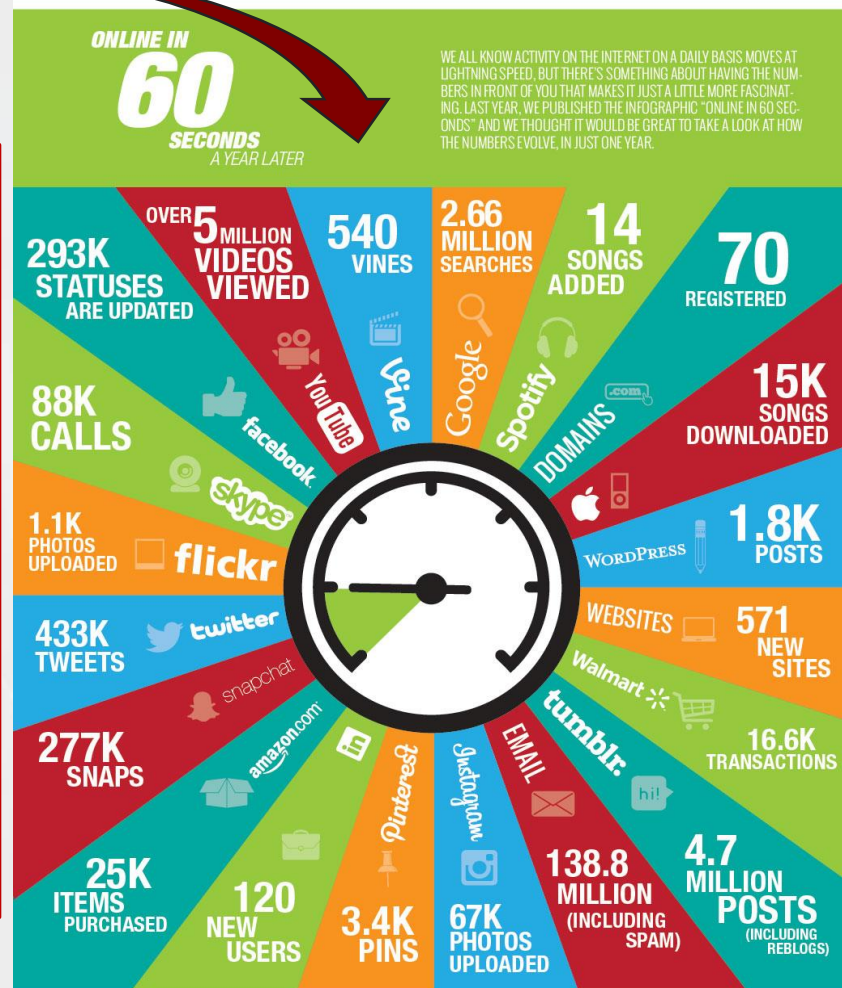
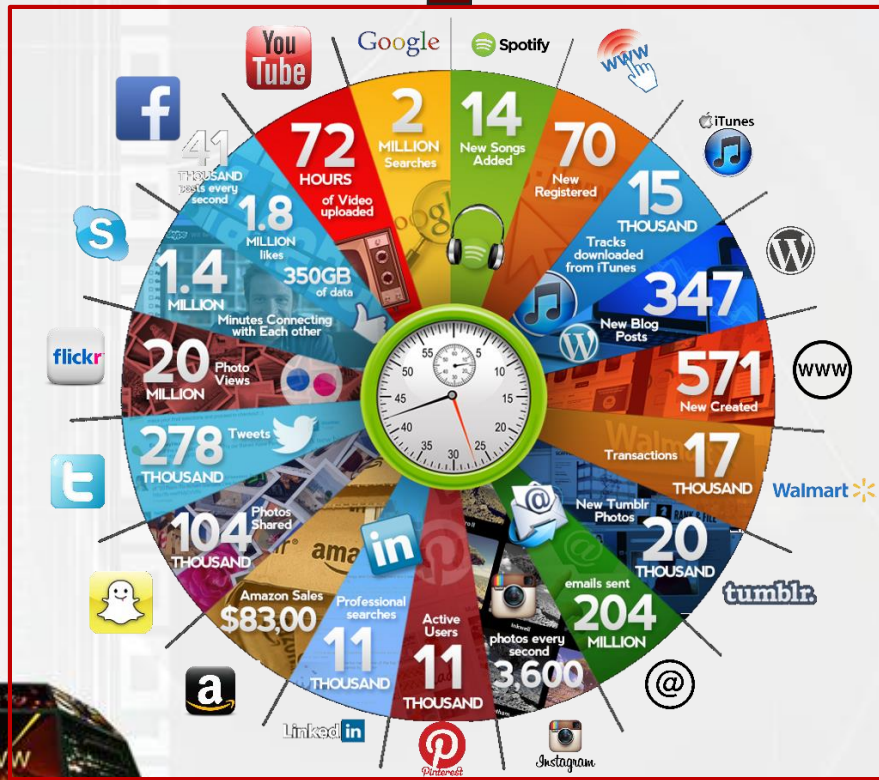
Καθηγητής Δημήτρης Γκριτζαλης

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



Internet, Web 2.0 & Online Social Networks (OSN): Πεδία δημόσιας (;!) έκφρασης και επικοινωνίας

qmee.com

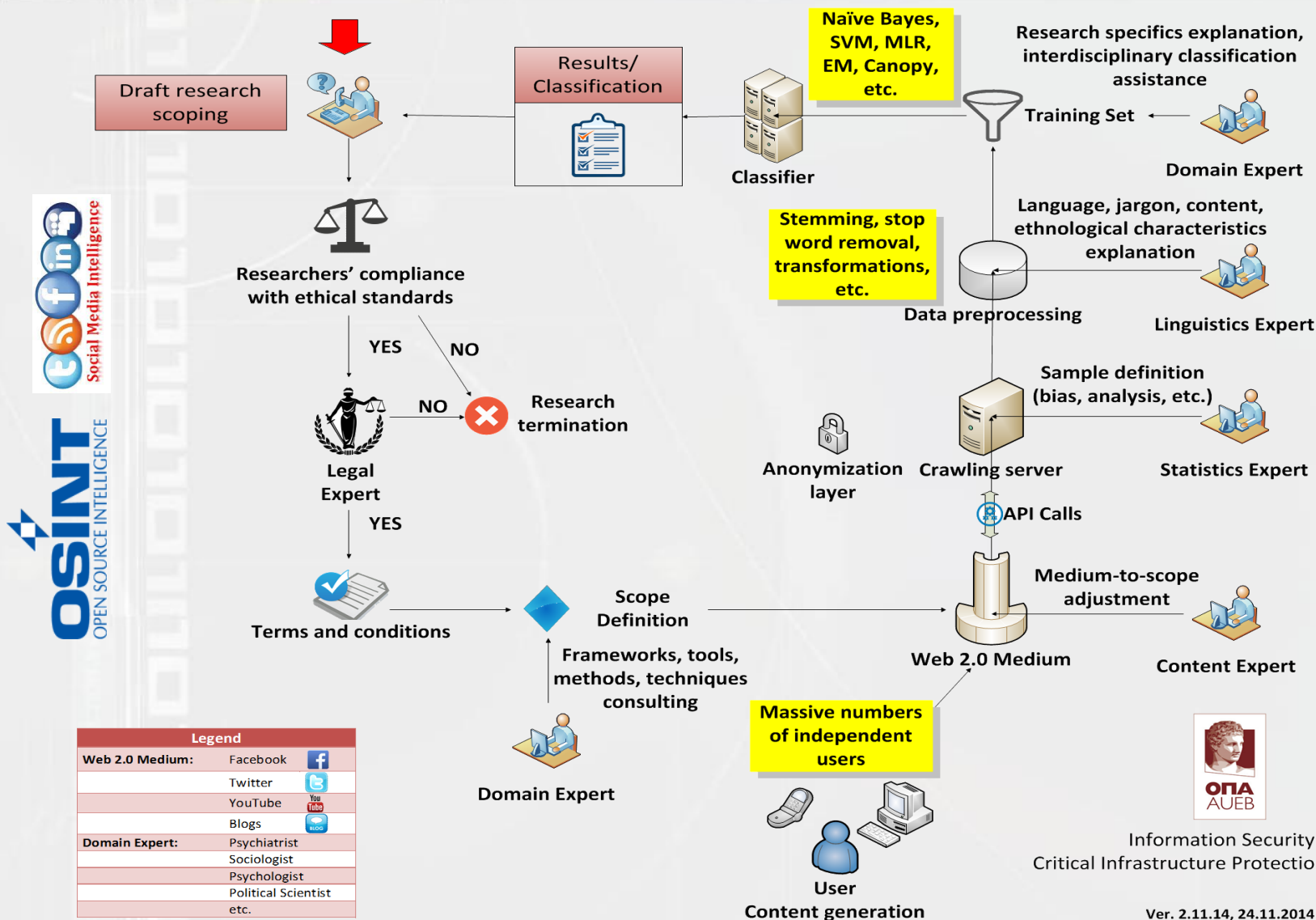


qmee

DATA
www.internetstats.com
www.thesocialstory.com
www.tumblr.com
www.guru.com
www.amazon.com
www.cnn.com
www.wired.com
www.flickr.com
www.wired.com
www.mashable.com

DESIGN BY NoLimitAgency

Open Source (or Social Media) Intelligence: Συλλογή & ανάλυση δημόσια διαθέσιμων δεδομένων





Προς επίρρωση της **ελπίδας** (1/2): 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

Συλλεγέντα 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, Node Loneliness, Indegree/Outdegree Distribution)

Ανάλυση Περιεχομένου (Opinion Mining, Machine Learning)

Επιρροή Χρηστών και Ένταση Χρήσης (User Influence, Usage Intensity)



Προς επίρρωση της **ελπίδας** (2/2): Συμβολή στον εντοπισμό **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

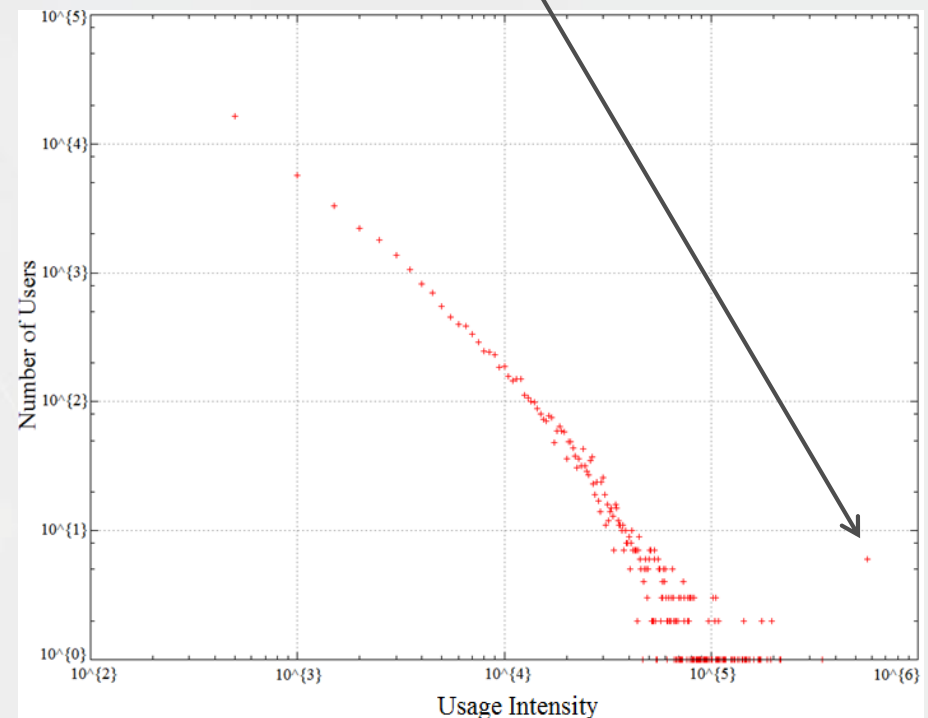
Outdegree distribution

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**



Προς επίρρωση της **απειλής** (1/2): Εκμετάλλευση 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, Node Loneliness, Indegree/Outdegree Distribution)

Ανάλυση Περιεχομένου (Opinion Mining, Machine Learning)

Ανάλυση Νέφους Κλάσεων (Tag Cloud Analysis)



Προς επίρρωση της απειλής (2/2): 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).



Προς επίρρωση της **ελπίδας** (1/2): Ενίσχυση της 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** (2/2): Ψηφιακή/Διαδικτυακή ψηφοφορία

Internet & Web 2.0



Χρήστες

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

Πρόσφορο πεδίο εφαρμογής

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

Μέσα και μέθοδοι έκφρασης γνώμης

Ψηφιακά Μέσα/Τεχνολογίες Ψηφοφορίας
Ψηφοφορία μέσω Διαδικτύου

Ειδικές συνθήκες και απαιτήσεις

Ανάγκη ισχυρών εγγυήσεων (ασφάλεια, αξιοπιστία κλπ.)
Επίδραση «Ψηφιακού Χάσματος» (“Digital Divide”)



Προ επίρρωση **απειλής/ελπίδας** (1/2): **Χειραγώγηση/έκφραση** απόψεων πολιτών

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα

Αναρτήσεις και 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 **απειλής/ελπίδας** (2/2): “Moneyball”: Maximizing votes per \$

Internet & Online Social Networks



Μεθοδολογία ανάλυσης



Δεδομένα

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

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 max Algorithms (i.e. “don’t knock on that door”)

Control & treatment Groups (testing messages to voters)

Decentralized-over-the-phone volunteers (VoIP)



Ψηφιακά Κοινωνικά Δίκτυα

- ✓ **Υβριδικό** μέσο (ελπίδα 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 (NMTS-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. 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.
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 on Trust, Privacy & Security in Digital Business (TRUSTBUS-2014)*, pp. 119-131, Springer (LNCS 8647), Germany, 2014.