View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Bournemouth University Research Online

1st International Workshop on Search and Mining Terrorist Online Content & Advances in Data Science for Cyber Security and Risk on the Web

Theodora Tsikrika
Centre for Research and Technology Hellas
theodora.tsikrika@iti.gr

Babak Akhgar
Sheffield Hallam University
B.Akhgar@shu.ac.uk

Vasilis Katos
Bournemouth University
vkatos@bournemouth.ac.uk

Stefanos Vrochidis
Centre for Research and Technology Hellas
stefanos@iti.gr

Pete Burnap
Cardiff University
burnapp@cardiff.ac.uk

Matthew L. Williams
Cardiff University
williamsm7@cardiff.ac.uk

ABSTRACT
The deliberate misuse of technical infrastructure (including the Web and social media) for cyber deviant and cybercriminal behaviour, ranging from the spreading of extremist and terrorism-related material to online fraud and cyber security attacks, is on the rise. This workshop aims to better understand such phenomena and develop methods for tackling them in an effective and efficient manner. The workshop brings together interdisciplinary researchers and experts in Web search, security informatics, social media analysis, machine learning, and digital forensics, with particular interests in cyber security. The workshop programme includes refereed papers, invited talks and a panel discussion for better understanding the current landscape, as well as the future of data mining for detecting cyber deviance.

Keywords
cybercrime; cyber security; terrorist and extremist content; data mining; security informatics

1. OVERVIEW AND MOTIVATION
Cyber deviance refers to the deliberate misuse of technical infrastructure for subversive purposes and includes (but is not limited to): the spreading of extremist propaganda [1], antagonistic or hateful commentary [2], the distribution of malware [3], online fraud, denial of service attacks, etc. Better understanding of such phenomena on the Web and social media allows for their early detection and underpins the development of effective models for predicting cyber security threats.

To this end, the 1st International Workshop on Cyber Deviance Detection (CyberDD) workshop held at WSDM 2017 in Cambridge, UK, focusses on two research tracks: (i) Detecting and Mining Terrorist Online Content and (ii) Advances in Data Science for Cyber Security and Risk on the Web. The efforts by major Web search engines and social media platforms (independently and in partnership) [4][5][6] towards addressing terrorist and violent extremist content that may appear on their services acutely demonstrate both the important challenges faced by Web Search and Data Mining practitioners, as well as the pressing need for research towards developing effective and efficient solutions. Moreover, the exploitation of the recent advances in Data Science for understanding, detecting, and forecasting cybercrime requires interdisciplinary approaches that blend them with Criminology research so as to gain true insights based on theories, methods, and data.

This workshop targets researchers and practitioners in Web search, data mining, security informatics, multimedia understanding, social media analysis, machine learning, and digital forensics, with particular interests in cyber security. It also targets industry representatives from search engines and social media platforms that aim to tackle the challenges of terrorist and violent extremist content appearing on their services, as well as criminologists and law enforcement representatives interested in recent advances in cyber deviance detection and understanding.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).
WSDM 2017, February 06-10, 2017, Cambridge, United Kingdom
ACM 978-1-4503-4675-7/17/02.
http://dx.doi.org/10.1145/3018661.3022760

2. OBJECTIVES
The main goals of this workshop are: (i) to present original research on Web search and data mining methods for the detection, extraction, and analysis of Web content related to terrorism and violent extremism, as well as methods of quantitative analysis for the purposes of better understanding and forecasting threats to cyber security emanating from the Web, (ii) to bring together researchers from the WSDM, (cyber) security informatics, and criminology communities, as well as industry representatives from search engines and social media platforms, to share ideas and experiences in designing and implementing such methods, (iii) to evaluate the effectiveness, efficiency, and maturity of such techniques, and (iv) to raise awareness of the privacy, legal, and ethical implications of the proposed methods and techniques.

3. TOPICS OF INTEREST
The two tracks of the workshop focus on different, yet complementary topics.

The track on "Detecting and Mining Terrorist Online Content" welcomes original research on detection, search, and mining methods that focus on the particularly challenging and idiosyncratic terrorist and violent extremist content on the Web (including the social media and the dark Web). Such content appears in multiple languages and media (e.g. text, images, video, and audio), it is highly volatile, often with short longevity, and it

may be covert, even when it is publicly available. The proposed methods and techniques should aim to allow for the development of effective and efficient systems and tools that are of particular interest to major search engines and social media platforms in their efforts to detect terrorist and violent extremist online content that may appear on their services, whilst striving to protect though fundamental citizens' rights. The topics include, but are not limited to, the following areas:

- Discovery and detection of terrorist online content: crawling the Web, social media, and darknets;
- Data, entity, and relationship extraction from terrorism-related multimedia content;
- Multilingual and multimedia search, mining, classification, and clustering of Web terrorist content;
- User profiling, persona modelling, and activity mining;
- Social network analysis for terrorism communities detection and key player identification;
- Search interaction log analysis for terrorism detection;
- Experiments and evaluation in Web search and data mining of terrorist online content;
- Credibility of discovered terrorist online information; and
- Predictive modelling and early warning for terrorist threats.

The track on "Advances in Data Science for Cyber Security and Risk on the Web" aims to discuss advances in Data Science and associated methods of quantitative analysis for the purposes of better understanding and forecasting threats to cyber security emanating from the Web. This essentially means any interactive socio-technical system that is underpinned by networked protocols including, but not limited to, social networking sites, command and control Web servers, SMS, Web-linked sensor devices, email, Web logs and wikis etc.; such systems have been theorised as Social Machines [7]. This track also aims to blend Criminology with Data Science for the study of cybercrime and cyber security [8]. Topics of interest include Web mining, machine learning and statistical modelling for:

- Malware classification and clustering;
- Cybercrime in distributed systems;
- Understanding interactive social systems and implications for cyber security;
- Web, IoT and cyber security;
- Modelling deviant behaviour on the Web;
- Criminological theory adapted to the Web;
- Understanding motivations to commit cybercrime; and
- Cybercrime and global politics.

4. REVIEW PROCESS

The call for papers solicited submissions in the form of long (8 pages) and short (4 pages) papers. Each submission was reviewed by at least three Programme Committee members and final decisions were made by the workshop chairs. The Programme Committee members include several experts in the field who worked diligently in reviewing the submitted papers and providing constructive feedback to the authors.

5. PROGRAMME

The program will be presented in the form of a half-day workshop that will include presentations of the accepted papers, two invited talks and a small panel. The accepted papers propose methods for discovering, identifying, and managing terrorist and extremist content on the Web. The invited talks from leading experts (researchers, industry representatives of social media platforms and search engines, or representatives of law enforcement and public services tackling cyber deviance) will focus on the current landscape of the detection and analysis of online content related to terrorism, violent extremism, and hate crime, as well on the human and social aspects of cyber deviant and cybercriminal behaviour from a criminology perspective. For the panel discussion, we intend to focus on the open challenges identified during the workshop and in particular on the privacy, ethical, and legal implications of the proposed methods and approaches.

6. ACKNOWLEDGMENTS

This workshop is partially supported by the EC H2020 project TENSOR (700024). We are also very grateful to the members of the Programme Committee.

7. REFERENCES

[1] Chatfield, A. T., Reddick, C. G., and Brajawidagda, U. 2015. Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided Twitter networks. In Proceedings of the 16th Annual International Conference on Digital Government Research. ACM. New York, NY, USA, 239-249. DOI: http://dx.doi.org/10.1145/2757401.2757408.

[2] Burnap, P. and Williams, M. L. 2016. Us and them: identifying cyber hate on Twitter across multiple protected characteristics. EPJ Data Science, Volume 5, Issue 11. DOI: http://dx.doi.org/10.1140/epjds/s13688-016-0072-6.

[3] Burnap, P., Javed, A., Rana, O. F. and Awan, M.S. 2015. Real-time Classification of Malicious URLs on Twitter using Machine Activity Data. In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2015), ACM, New York, NY, USA, 970-977. DOI: http://dx.doi.org/10.1145/2808797.2809281.

[4] Microsoft's approach to terrorist content online. Retrieved December 12, 2016, from Microsoft's official blog: https://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online.

[5] Combating Violent Extremism. Retrieved December, 12, 2016, from Twitter's official blog: https://blog.twitter.com/2016/combating-violent-extremism.

[6] Partnering to Help Curb Spread of Online Terrorist Content. Retrieved December 12, 2016, from Facebook's newsroom. http://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.

[7] Hendler, J. and Berners-Lee, T. 2010. From the Semantic Web to social machines: A research challenge for AI on the World Wide Web, Artificial Intelligence, Volume 174, Issue 2, Pages 156-161, ISSN 0004-3702, DOI: http://dx.doi.org/10.1016/j.artint.2009.11.010.

[8] Choo, KKR. 2011. The cyber threat landscape: Challenges and future research directions, Computers & Security, Volume 30, Issue 8, Pages 719-731, ISSN 0167-4048, DOI: http://dx.doi.org/10.1016/j.cose.2011.08.004.