RiskTrack: a new approach for risk assessment of radicalisation based on social media data

David Camacho**, Irene Gilpérez-López, Antonio Gonzalez-Pardo, Alvaro Ortigosa, and Carlota Urruela

Computer Science Department
Universidad Autónoma de Madrid, Spain,
AIDA research group: http://aida.ii.uam.es
{david.camacho, irene.gilperez, antonio.gonzalez, alvaro.ortigosa, carlota.urruela}@uam.es

Abstract. The RiskTrack project aims to help in the prevention of terrorism through the identification of online radicalisation. In line with the European Union priorities in this matter, this project has been designed to identify and tackle the indicators that raise a red flag about which individuals or communities are being radicalised and recruited to commit violent acts of terrorism. Therefore, the main goals of this project will be twofold: On the one hand, it is needed to identify the main features and characteristics that can be used to evaluate a risk situation, to do that a risk assessment methodology studying how to detect signs of radicalisation (e.g., use of language, behavioural patterns in social networks...) will be designed. On the other hand, these features will be tested and analysed using advanced data mining methods, knowledge representation (semantic and ontology engineering) and multilingual technologies. The innovative aspect of this project is to not offer just a methodology on risk assessment, but also a tool that is build based on this methodology, so that the prosecutors, judges, law enforcement and other actors can obtain a short term tangible results.

Keywords: Radicalisation, Risk assessment, Social Networks Analysis, Terrorism prevention

1 Introduction

The West entered in a new era of perpetual danger for its people and its way of living since 2001, when the 11-S jihadist attack happened in the USA. This tragic event marked a before and an after in the West, because it unchained a series of attacks by national and international extremist groups, in the name of the Islamic State [18].

The European Union has as one of its top priorities to fight together terrorism in all its forms to protect the fundamental rights of its citizens and to

** Corresponding author: david.camacho@uam.es

maintain their safety. In order to do so, in 2005 an EU Counter-terrorism strategy was stablished by the European Council; the strategy is sustained by four pillars: prevent, protect, pursue and respond. This strategy was revised in 2014 by the European Council and it came out with guidelines of measures for EU member states to follow and put into effect [17,29].

The new jihadist terrorism has characteristics in common with other types of terrorism; despite this, it has an idiosyncratic nature, particularly the way to radicalise its militants. When it comes to understanding this peculiarity and the series of stages that it takes for a person to become radicalised, it is mandatory to look into the unique traits of jihadist terrorism. This could give essential information to detect and prevent radicalisation. Great efforts are needed to prevent radicalisation and develop efficient counter-terrorism measures: the size of the violence perpetrated, the psychological consequences for Western citizens and the constant innovation of these terrorists to carry out their attacks make this matter a top urgency for governments and counter-terrorism institutions [18].

Jihadist radicalisation has its own process, and also their militants have many vulnerability factors that made them adequate targets. The United Nations Office of Drugs and Crime [40] sustains that such factors are related to demographic and socio-economic situations. Nevertheless, this kind of explanation is very limited [15,16]. It has to be taken into account that Muslim religion has more than 1300 believers across the planet who suffer, as well as jihadists, the same serious political, social and economic problems; and yet, jihadism is not as widespread as can be expected, and a very small percentage of these faithful Muslims agree with this extremist perspective, although jihadists denounce clear and loud the difficulties Muslim countries and Muslim people undergo.

In this way, radicalisation is triggered by not only socio-demographic factors, but also by personal life experiences and situations and basic needs, emotions and feelings. In fact, these people usually start its radicalisation by entering themselves in this dynamic, auto-exploring radical ideologies and getting in touch with extremist individuals or circles, longing to fulfil these needs. The entrance and the stay in radical networks, and also the appearance of determined behaviours, can be encouraged by the social recognition and feel of belonging they can provide. Humiliation, indignation, anger, guilt, hatred and frustration are the most related emotions and feelings to jihadist radicalisation [4,36].

The RiskTrack project will have its base on these radicalisation factors, focusing studying, understanding and identifying them on the Internet. Although there are complex software tools that make it hard to track private communications among radicals, such as anonymising software and encryption tools [40], there is a huge amount of information published by these radicalised individuals in public social media which can be traced.

Thus, the most used social networks, such as Twitter, Facebook, YouTube, Tumblr and Instagram, have become a new and dynamic scenario for the jihadist cause: they serve as propaganda sharing platforms, psychological warfare, live forums and recruitment assets. As in 2012 the message that "any Muslim who tries the jihad against the enemy by electronic means is considered one way or another a Mujahid" was spread through the Al-Fida and Shumukh al-Islam forum, generations of youths have listened and the use of social media, with which they are familiar, as a new place for the Jihad [22]. Thus, according to the UNODC document "The use of the Internet for terrorist purposes" [40], terrorists make use of the Internet and social media to spread their propaganda, accompanied by instructions, justifications and explanations, promoting their acts with virtual messages, such as presentations, video files, among others; and also, as mentioned above, to make connections with potential radicals. But not only are the already named social networks used for these purposes: jihadists use massively the Internet through forums, web pages, blogs, chats, multimedia publications, messages and emails, virtual communities, among others [13]. Consequently, the Network allows vulnerable individuals to get sensitive information or get in touch with other people with their same restlessness or already radicalised people, who could give positive feedback among each other about their extremist ideas and encourage the radicalisation process. Also, the powerful feeling of belonging is present, as the Network favours the international communications which give the sensation of being part of a transnational movement [38,39]. And finally, radicalised individuals or terrorists have a wide way of communication with others to collaborate together or to radicalise: by getting the attention of other groups, cells or radicalised individuals through their Network activity while in the process of radicalisation, or leaders or 'recruiters' to contact potential new members.

The importance of online connections is supported by the fact that self-radicalisation or no social interaction at all is unlikely or practically impossible; even individuals who seem that they were alone in the process, they had from the beginning strong influences of other people, who had already contact with radical environment or were members of a terrorist group, by getting in touch with them on the Internet [37]. Furthermore, usually the process involves that, while gradually drifting apart from friends or reference peer groups, the subjects get closer to other individuals to radicalise or be radicalised [15]. Nevertheless, these communications with people who are already radicalised or active members of terrorist groups can sometimes be unexpected and a result of chance [33].

This project will focus on the extraction of radicalisation factors on social media and their detection through a cyber-tool of own creation. There are many tools to extract information of online sources, but there is a lack of a specific and specialised tool for online radicalisation, and this is a problem for Law Enforcement Agencies, Probation Services, Intelligence Services and also for researchers and industry. Examples of suitable technologies for knowledge extraction are, for example, Big Data [9,25], Artificial Intelligence [24] and Data Mining [10],

which set the bases for the development of a new specialised tool, nourished with adequate psychologist methodologies in order to process and make an extraction of pertinent information with which model the behaviour of human users [6,8]. Because of the previously exposed, it is imperative a project of this kind, to analyse radicalisation on the Internet and being able to develop and use solid tools which would detect radicalisation and prevent it.

2 Risk assessment for radicalisation in social media

The survey conducted by Agarwal and Sureka [1] showed that over the past 10 years there has been many studies about detecting radicalisation by mining textual data from public social media sources. Microblogs such as Twitter and Tumblr were the most common websites used for this purpose, but studies with YouTube, the most often used platform for jihadist propaganda, were not found. About the tools used for detecting and predicting online radicalisation in social media, the researches claim that the most popular techniques are Clustering (Blog Spider), Topical Crawler/Link Analysis (Breadth First Search, Depth First Search, Best First Search), KNN (K Nearest Neighbor), Keyword Based Flagging (KBF), Decision Tree, Support Vector Machine, Exploratory Data Analysis (EDA), Rule Based Classier and Naive Bayes. Some examples of the latest studies regarding the development of a tool for radicalisation risk assessment are the following.

Monahan questioned in the study '*The Individual Risk Assessment of Terrorism*' [26] the challenges that should be faced in order to carry out a trustworthy risk assessment for violent extremists. The research revised identified indicators for potential criminal behaviour and compared them to the findings of literature dedicated to terrorism, concluding that they were not proper for risk assessment of terrorism. Thus, the work explained, as a result of literature review, that potential adequate candidates for specialised indicators are grievances, ideologies, affiliations and moral emotions. Also, different approaches to make an assessment were compared – unmodified clinical risk assessment, modified clinical risk assessment, structured professional judgement, modified actuarial risk assessment and unmodified actuarial risk assessment – to finally state that the most useful approach for terrorism risk assessment may be structured professional judgement. About the issue of the validation of a risk assessment tool of terrorism, the author maintains that this tool should be validated through ex post facto studies, with already registered terrorists and non-terrorist subjects from the same population, as it would be unlikely to do it prospectively.

The work of Pressman and Flockton [30] explored the possibility of making a VERA 2 (parting from the original VERA - Violent Extremist Risk Assessment protocol) for terrorists, violent extremists and unlawful violent offenders impelled by political, social or religious ideologies. They highlighted the need of using specific indicators for assessing terrorists' behaviour, as they strongly

differ from violent criminals in general. As they state, an approach to build this specialised tool is viable by a structured professional judgment once appropriate risk indicators are identified, as the VERA 2 does.

In this line, the book Combating Violent Extremism and Radicalization in the Digital Era [21] includes a chapter which proposes the application of the VERA 2 in social media [31]. The authors focus on cyber-language, imagery elements, online social context and behaviour to create the CYBER-VERA or CYBERA risk assessment tool, to use it in addition to VERA 2 or other instruments or techniques already in use by security and intelligence agencies, as well as professionals such as psychologists or communication analysts. The protocol was tested successfully with a case of cyber-radicalisation.

3 Methods and frameworks for Social Data Analysis

As it has been previously said, the majority of the jihadist radicalisation takes part in the social media. This is because the number of connected users through Social Networks (SN) is increasing every day [28]. For this reason, it is extremely important the development of methods and frameworks to analyze the Social Data.

The area of Social Networks, and the possibility to analyse huge amounts of data, has attracted the attention to research areas as Machine Learning, Big Data, Statistics or Physics among others. Traditionally, the problem of community finding has been studied from Graph-based computing, Machine learning as Clustering or Computational Intelligence. The area of Social Network Analysis [34] provides methods, algorithms, frameworks and systems that allows to analyse the information stored in this SNs to obtain useful information for users. This section will be focused on the two key concepts related to the Social Network Analysis: Community Finding and EgoNetworks.

3.1 Community Finding

Community finding is one of the most important task when studying networks. The network is composed by a set of nodes that represents the objects of the network, and the interactions among these objects appear as the edges of the network.

The goal of any community finding method is to group the different nodes in several clusters in such a way the nodes belonging to the same cluster share some properties. There is a plethora of applications that gravitates around the community finding problem. For example, it is used to discover functionally related objects [41], to study the different interactions between the objects [3], or

to predict unobserved connections [12] among others.

In these networks, there are two different sources of data that can be used to perform community finding tasks. The first one is related to the information stored in the different nodes that compose the network; whereas the second one is extracted from the set of network connections.

The decision of what kind of data will be used in the community finding problem is an important task that will affect to the performance of the proposed algorithm. On the one hand, using the information contained in the network will be useful to cluster those nodes with similar characteristics, but those nodes without this specific information will not be correctly clustered. On the other hand, the results obtained using the information extracted from the network will represent the different relationships among the nodes but it will fail with nodes with few connections.

3.2 Ego Networks

The number of users registered in the different Social Networks, and the volume of information generated by them are increasing every day. This fact makes extremely difficult any analysis over the whole network without the application of an approach based on the well-known Big Data paradigm [7]. In order to extract the knowledge from the network, some relevant works have focused the attention to Ego Networks [19].

An Ego Network is a social network composed by one user centering the graph (called 'Ego'), being all the users connected to this Ego (called 'Alters') and all the relations among the alters. Given a specific Social Network composed by N different users, there are N different Ego Networks associated with the given network (one Ego Network for each user). Figure 1(a) provides an example of a Social Network composed by 8 users, whereas Figure 1(b) shows the Ego Network for the selected user (coloured node) from Figure 1(a).

One of the most extended algorithms in this area is the **Clique Percolation Method** (CPM) [20]. It is based on the concept that different communities exhibit high density, i.e. the nodes of the community are highly connected. Initially this algorithm looks for all the cliques of size k. Then, a reduced graph is created by considering a node each of the k-cliques previously identified. Two nodes belong to the same community if their corresponding k-cliques share $k-1$ members. Other approaches use the topology of the network to detect the different communities by dividing the network based on the different links or edges [5]. Other popular algorithm is the one proposed by Clauset et al. [14]. The **Clauset-Newman-Moore** [35] algorithm is based on the **Edge Betweenness** algorithm [27]: given a dataset composed by N elements, this algorithm starts considering N isolated nodes that represent the elements of the dataset. Then,

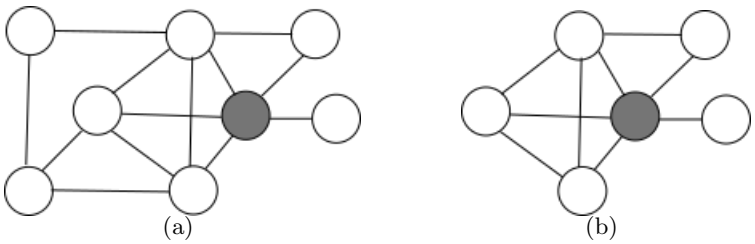

Fig. 1. a) Representation as a graph of a Social Network composed by 8 users. b) Ego Network whose ego is the coloured node from the left SN.

the algorithm starts iteratively adding links of the original graph to produce the largest possible increase of the modularity at each step. **Label Propagation** is an algorithm proposed in [32] that it is used to perform the community finding task. The algorithm is based on the propagation of different labels through the edges of the network in order to define the clusters. In this algorithm, a cluster is defined as the set of nodes that shares the same label among them. Initially, each node is given a specific label from the set of k labels. When all the nodes are labelled, the algorithm, iteratively, changes the labels of the nodes. For a specific node, the new label will be the one that is most common among its neighbours. Finally, the different clusters are composed by those groups densely connected with a unique label. Other hierarchical agglomerative algorithm is the **Walktrap** algorithm [11]. In the first step of this algorithm, N different clusters are created for the N elements that will be analyzed. Then, two clusters are merged taking into account the number of random walks that connect the elements of both clusters. The key concept of this algorithm is based on the premise that elements belonging to the same cluster share many connection, or edges, whereas there are few connections between the elements from different clusters. In the literature can also be found the **Infomap** algorithm [2]. Initially, each element is assigned to only one cluster composed by the node itself. Then, iteratively, nodes are moved to a neighbouring cluster that results in the largest decrease of the map equation. This map equation measures the trade-of between the compression of data and the extraction of patterns within those data. The algorithm is executed until there are not any movement that decreases the value of the map equation.

Finally, there are other works that uses different probabilistic approaches in order to estimate the community membership of the different elements [23].

4 Next steps and future work

The achievements of the RiskTrack project will be developed in two parallel phases. The first one will be handle by a team of behaviour scientists composed

by terrorism and risk assessment experts: they will provide the basic features to identify the radicalisation and how to make an accurate assessment. On the other hand, two engineering teams will be the responsible to generate both, an ontology and data representation to adequately process the information extracted from a set of selected Web sites (as Twitter), and a set of data-analitics tools, able to apply previous radical features provided from the terrorism experts over the data gathered from the Web.

The initial steps to carry out in this project will be the following: the identification of radicalisation indicators, designing the methodology to evaluate these indicators and generating a set of data benchmarks that will be used later to design a radicalisation ontology, and the set of data mining algorithms to process them.

Acknowledgments

This work has been supported by the RiskTrack project: "Tracking tool based on social media for risk assessment on radicalisation" under the EU Justice Action Grant: JUST-2015-JCOO-AG-723180.

References

1. Swati Agarwal and Ashish Sureka. Applying social media intelligence for predicting and identifying on-line radicalization and civil unrest oriented threats. *arXiv preprint arXiv:1511.06858*, 2015.
2. Y.-Y. Ahn, J. P. Bagrow, and S. Lehmann. Link communities reveal multiscale complexity in networks. *Nature*, 466(7307):761–764, 2010.
3. E. M. Airoldi, D. M. Blei, S. E. Fienberg, and E. P. Xing. Mixed membership stochastic blockmodels. *Journal of Machine Learning Research*, 9:1981–2014, June 2008.
4. Scott Atran. *Talking to the enemy: Faith, brotherhood, and the (un) making of terrorists*. Harper Collins, 2010.
5. R. Balasubramanyan and W. W. Cohen. Block-lda: Jointly modeling entity-annotated text and entity-entity links. In *Handbook of Mixed Membership Models and Their Applications*, pages 255–273. Chapman and Hall/CRC, 2014.
6. David F Barrero, Antonio González-Pardo, David Camacho, and María D. R-Moreno. Distributed parameter tuning for genetic algorithms. *Computer Science and Information Systems*, 7(3):661–677, 2010.
7. G. Bello-Orgaz, J. J. Jung, and D. Camacho. Social big data: Recent achievements and new challenges. *Information Fusion*, 28:45–59, 2016.
8. Gema Bello-Orgaz, David F Barrero, María D R-Moreno, and David Camacho. Acquisition of business intelligence from human experience in route planning. *Enterprise Information Systems*, 9(3):303–323, 2015.
9. Gema Bello-Orgaz, Jason J Jung, and David Camacho. Social big data: Recent achievements and new challenges. *Information Fusion*, 28:45–59, 2016.

10. Gema Bello-Orgaz, Héctor D Menéndez, Shintaro Okazaki, and David Camacho. Combining social-based data mining techniques to extract collective trends from twitter. *Malaysian Journal of Computer Science*, 27(2):95–111, 2014.
11. V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre. Fast unfolding of communities in large networks. *Journal of statistical mechanics: theory and experiment*, 2008(10):P10008, 2008.
12. J. Chang and D. M. Blei. Hierarchical relational models for document networks. *Ann. Appl. Stat.*, 4(1):124–150, 03 2010.
13. Frank Cilluffo, Gregory Saathoff, Jan Lane, Sharon Cardash, and Andrew Whitehead. NETworked Radicalization: A Counter-Strategy. Technical report, The George Washington University Homeland Security Policy Institute & The University of Virginia Critical Incident Analysis Group, 2007.
14. A. Clauset, M. E. J. Newman, and C. Moore. Finding community structure in very large networks. *Phys. Rev. E*, 70:066111, Dec 2004.
15. Luis De la Corte Ibáñez. *La lógica del terrorismo.* Madrid: Alianza Editorial, 2006.
16. Luis De la Corte Ibáñez and Javier Jordán. *La yihad terrorista.* Madrid: Síntesis, 2007.
17. European Commission. Radicalisation, 2016.
18. David Garriga Guitart. *Yihad, ¿qué es?* Barcelona: Comanegra, 2015.
19. Antonio Gonzalez-Pardo, Jason J. Jung, and David Camacho. Aco-based clustering for ego network analysis. *Future Generation Comp. Syst.*, 66:160–170, 2017.
20. S. Günnemann, B. Boden, I. Färber, and T. Seidl. Efficient mining of combined subspace and subgraph clusters in graphs with feature vectors. In *Advances in Knowledge Discovery and Data Mining: 17th Pacific-Asia Conference, PAKDD, Proceedings, Part I*, volume 7818 of *Lecture Notes in Computer Science*, pages 261–275, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
21. Majeed Khader, Loo Seng Neo, Gabriel Ong, Eunice Tan Mingyi, and Jeffery Chin. *Combating Violent Extremism and Radicalization in the Digital Era.* IGI Global, Hershey, PA (USA), 1st edition, 2016.
22. Eguskiñe Lejarza Illaro. Terrorismo Islamista En Las Redes – La Yihad Electrónica. Technical report, Instituto Español de Estudios Estratégicos, 2015.
23. J. Mcauley and J. Leskovec. Discovering social circles in ego networks. *ACM Trans. Knowl. Discov. Data*, 8(1):4:1–4:28, February 2014.
24. Héctor D. Menéndez, David F Barrero, and David Camacho. A genetic graph-based approach for partitional clustering. *International journal of neural systems*, 24(3):1–19, 2014.
25. Héctor D. Menéndez, Fernando Esteban Barril Otero, and David Camacho. Extending the sacoc algorithm through the nystrom method for dense manifold data analysis. *International Journal of Bio-Inspired Computation*, 2015.
26. John Monahan. The individual risk assessment of terrorism. *Psychology, Public Policy, and Law*, 18(2):167–205, 2012.
27. S. Moon, J.-G. Lee, and M. Kang. Scalable community detection from networks by computing edge betweenness on mapreduce. In *Big Data and Smart Computing (BIGCOMP), 2014 International Conference on*, pages 145–148. IEEE, 2014.
28. K. Musiał and P. Kazienko. Social networks on the internet. *World Wide Web*, 16(1):31–72, 2012.
29. Council of the European Union. The european union strategy for combating radicalisation and recruitment to terrorism. Technical report, Brussels: European Parlament, 2005.

30. D. Elaine Pressman and John Flockton. Calibrating risk for violent political extremists and terrorists: the VERA 2 structured assessment. *The British Journal of Forensic Practice*, 14(4):237–251, 2012.
31. D. Elaine Pressman and Cristina Ivan. Internet Use and Violent Extremism: A Cyber-VERA Risk Assessment Protocol. In Majeed Khader, Loo Seng Neo, Gabriel Ong, Eunice Tan Mingyi, and Jeffery Chin, editors, *Combating Violent Extremism and Radicalization in the Digital Era*, chapter 19, pages 391–409. IGI Global, Hershey, PA (USA), 1st edition, 2016.
32. U. N. Raghavan, R. Albert, and S. Kumara. Near linear time algorithm to detect community structures in large-scale networks. *Phys. Rev. E*, 76:036106, Sep 2007.
33. Marc Sageman. *Understanding terror networks*. Philadelphia: University of Pennsylvania Press, 2004.
34. J. Scott. *Social network analysis*. Sage, 2012.
35. S. Sobolevsky, R. Campari, A. Belyi, and C. Ratti. General optimization technique for high-quality community detection in complex networks. *Physical Review E*, 90(1):012811, 2014.
36. Anne Speckhard. *Talking to Terrorists: Understanding the Psycho-social Motivations of Militant Jihadi Terrorists, Mass Hostage Takers, Suicide Bombers & "martyrs"*. McLean, VA: Advances Press, 2012.
37. Mario Toboso Buezo. El "lobo solitario" como elemento emergente y evolución táctica del terrorismo yihadista. *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*, 2013(14), 2013.
38. Manuel R. Torres. *El eco del terror: Ideología y Propaganda en el Terrorismo Yihadista*. Madrid: Plaza y Valdés, 2009.
39. Stephen Ulph. A guide to jihad on the web. *Terrorism Focus*, 2(7), 2005.
40. United Nations Office On Drugs and Crime. The use of the Internet for terrorist purposes. Technical report, Vienna, 2012.
41. J. Yang and J. Leskovec. Overlapping community detection at scale: A nonnegative matrix factorization approach. In *Proceedings of the Sixth ACM International Conference on Web Search and Data Mining*, WSDM Í3, pages 587–596, New York, NY, USA, 2013. ACM.