Behavioural Analytics: A Preventative Means for the Future of Policing

Alireza Daneshkhah, Hamid Jahankhani, Homan Forouzan, Reza Montasari, Amin Hosseinian-Far

Original citation:
'Behavioural Analytics: A Preventative Means for the Future of Policing', in *Policing in the Era of AI and Smart Societies*, ed. by H. Jahankhani, B Akhgar, B Cochrane and P Dastbaz, pub 2020 (ISBN 978-3-030-50613-1)

Publisher: Springer

Behavioural Analytics: A Preventative Means for the Future of Policing

Alireza Daneshkhah[1], Hamid Jahankhani[2], Homan Forouzan[3], Reza Montasari[4], Amin Hosseinian-Far[5]

[1]Coventry University, UK, [2]Northumbria University, London, UK, [3]University of Northampton, UK, [4]Huddersfield University, UK, [5]University of Northampton UK

Abstract. Without sufficient intelligence, police response to crimes occurs in the form a reactive retort. This is even more so in the case of cyberspace policing, as digital platforms increase the complexities involved in the overall police incident response development. In this paper, we briefly introduce cybercrime and the necessities that police forces have to deal with. We argue that there is an urgent need for development and adoption of proactive and preventive techniques to identify and curb cyber and cyber-enabled crimes. We then present topic modelling as one of effective preventive techniques for predicting behaviours that can potentially be linked to cybercrime activities on social media.

Keywords: Future of Policing, Topic Model, Information Security, Machine Learning, Predictive Inference, Behavioural Analytics

1. Introduction

More and more people and organisations are relying on electronic devices and the Internet to store personal information, and this consequently increases also increase the opportunity for crime. Cyber criminals have no jurisdiction as they can operate from anywhere in the world. The complicity of investigation of such crimes is extremely challenging, if staff are not adequately trained or educated on the subject matter in being able to identify the offenders and bring them to justices (Jahankhani & Hosseinian-Far, 2014). As technology has become a pivotal point in our society, the dependency is intensified and critical for all, ranging from people to business and instead a larger scale to the government organisations becoming more cyber resilient. In addition, it is vital to have in place measures and processes in place that

are adequate and sufficient in securing information security across all technological platforms. Such processes will provide safeguarding of data, information, network and devices from any form of hacking, breach or attack. Moreover. it is important that the police forces and cyber security specialists valuing, protecting and processing available information and intelligence with confidentiality, integrity and availability (CIA), as this would have a direct impact on the public's trust and confidence on those parties (Forouzan et al, 2018). If the security of this information protection is breached, this could have a detrimental effect on the service that police forces deliver, public confidence and the organisations reputational values. Therefore, it is extremely imperative that the right level of training and education be provided to police officers to be able to protect and safeguard the information on their Information Communications and Technology (ICT) systems.

2. Technology & Crime

The term cybercrime describes acts, which incorporates the unlawful usage of computer technology and the Internet (Gillespie, 2019). The question that is raised here is how aware, educated and knowledgeable the police services are in safeguarding their information and preventing a cyber-attack on their infrastructures.

As cyber criminals can operate from anywhere around the world with no jurisdiction this makes it extremely difficult for the law enforcement agencies to track and bring to justice those responsible. Such investigations are very complex and resource intensive for the police. What is key here is that the police services need to be aware, educated and trained to be able to identify their weaknesses and vulnerabilities to prevent their devices being subject to a breach or an attack. Previously cybercrime was not on the government and law enforcement agencies agenda, however more recently due to the rapid rise of cyber-enabled crime within the UK in 2010 the UK Government have classified cybercrime as a 'Tier 1' threat by The Government's 2010 National Security Strategy (Cabinet Office, 2010). The Government's 2010 National Security Strategy has grouped threats into three tiers, where 'Tier 1' threat is classified as the highest threat. Within the report, it has been highlighted that companies, industries and government organisations need to protect their devise and prevent potential attacks within the UK (Forouzan, et al. 2018). Tackling the risks and the impacts associated with cyber and cyber enabled crimes can be more challenging for Small to Medium Enterprises (SME) compared to larger organisations, due to the lack of relevant resources (both human and financial).

As the society is seeing a surge in the use of technology and the dependency is becoming greater day by day, it is vital that there is an adequate and secure information security to safeguard the information, data, network and devices from any form of attack (Schjolberg, 2014). The term cybercrime is used to

describe acts, which incorporates the unlawful usage of computer technology and the Internet. The question that could be asked here is how equipped, trained and educated are the police forces in tackling such a vast growing crime. Cyber criminals have no jurisdiction as they can operate from anywhere in the world the complicity of investigation of such crimes will make it difficult if the police are not adequately trained or educated on the subject matter in being able to identify the offenders and bring them to justices.

The Office for National Statistics (ONS) Survey of Crime in England and Wales report In March 2016 (Flatley, 2016), noteworthy saw an important change in cybercrime. Due to the surge in cyber enabled crimes the ONS devoted a cybercrime and fraud section on the report for a very first time. This illustrated the importance of cybercrime and the need for government and law enforcement agencies needing to take cybercrime more seriously than ever before. The report highlighted the fact that an estimate of 5.8 million cyber enabled crime and fraud had been committed in England and Wales. The data estimated out of the 12 million crimes committed across England, Wales nearly over half of those crimes were cyber enabled, and fraud related (Ford, 2016). Such statistics were an eye opener to the government and the law enforcement agencies as traditional crimes was making a significant shift towards cyber enabled crime. The question that might be considered is the fact that are police forces across England and Wales adequately trained, educated and equipped to tackle cyber enabled crime to bring those responsible to justice and to serve justice for the victims of those crimes. Due to the advancement of technology, criminals are using the cyber space more and more in carrying out their criminal conducts, the governments national statistics has highlighted that cyber enabled crime victims are on an increase year by year (Wall, 2013).

3. Traditional Crime VS Cyber Crime

Typically, criminals who intended to gain personal information from others would have committed identify theft by intercepting the intended targets post, looking at their trash and trying to piece their office shredded documents together. With the advancement of technology and the social dependency for people to interact with the Internet, more and more personal information has become readily accessible for criminals. As people are using their smart phones, tablets, TV's and computers more to purchasing goods of the internet, paying their bills via applications, using social media applications to engage with others and to share personal information.

Traditional Personal identity theft tactics have not changed but what has changed is their method in which they are acquired. As previously criminals used to physically trawl through the trash of others now through hacking, breaches and attacks they search the systems recycle bin for deleted items, cache memory, temporary files and cookies for recent accessed data and so

on. There are many more methods that criminals use to obtain personal or financial information from others for example the use of phishing emails to get the intended victim to provide their personal or financial information to the criminal. Benefits of obtaining personal information could be financial, revenge, personal or to misrepresent that person and to commit a criminal conduct (Forouzan, et al. 2018, Clough, 2015).

Both traditional crime and cybercrime have one thing in common and that is the word 'crime' which includes an unlawful act or conduct. One uses the Internet and or a computer device to carry out the criminal conduct, where the perpetrator has no jurisdiction and can operate from anywhere across the world in committing that crime. On the other hand, traditional crimes require the perpetrator to be present at the crime scene where the crime has been committed (Forouzan, et al. 2018, Clough, 2015, Wall, 2007).

For both traditional and cybercrime, the perpetrator will leave evidential footprints behind. For instance, for traditional crimes, the offender will leave DNA, fingerprints and physical traces of evidence behind at the crime scene. The same applies for cybercrime, cyber criminals will leave digital footprints and evidential traces behind through the use of the internet or digital devices (Forouzan, et al. 2018, Swire, 2009, Wall, 2007).

As the police services in the UK have been investigating traditional crimes since the 1890's, they have become experts and masters in identifying and bringing offenders to justice through their evolving methods and tactics. However, the police service has recently began investigating cybercrime and are still by far nowhere near in being able to master such methods and tactics. With traditional crimes the police would have looked at the physical footprints left by the perpetrator (DNA, finger prints, shoe prints etc..), review CCTV footages of the incidents, speak with witnesses and interview suspects to obtain further information. This is not always possible with cyber criminals who could be in another country, using proxy servers from another country or other genuinely devices to carry out their attack on the intended target in a third country. Due to such complexities and lack of knowledge and training by police services across the world the police are finding it very difficult to investigate such offences and bring those responsible to justice. Due to such complications and difficulties faced by the legal authorities the investigations of cyber-attacks are more resource intensive, financial very expensive and require a lot of time in order to identify and prosecute those responsible.

Traditionally perpetrators would have taken a high risk in order to commit a theft, robbery or a burglary offence in compression to the benefit that they would have obtained from committing such offences. There was a high risk that law enforcement agencies would have caught and brought them to justice. However, in the world of cybercrime similar or even higher profits are achievable with much lesser risk of being caught and prosecuted. Criminals are becoming wiser and cyber knowledgeable by balancing out the risk of being caught against the benefits (Gaidosch et al., 2019).

4. Digital Platforms and Social Media

The rise of digital platforms for business and personal use has necessitated further engagement with preventive measures in security management. The landscape of cyber crime and cyber enabled crime classification and categorisation is now very dissimilar to the earlier cataloguing as illustrated in Jahankhani et al., (2014). Social media have become an integral part of the day to day lives; furthermore, several business models nowadays leverage the potentials of data generated within social media. Twitter, Facebook, Instagram, Snapchat, and LinkedIn are some of the examples of platforms that have seen a significant increase in the number of its users from both personal and business realms. Fig. 1. illustrates the total number of Twitter users in the 9 years from 2010 until the first quarter of 2019, presenting a significant growth in the number of users in 9 years.

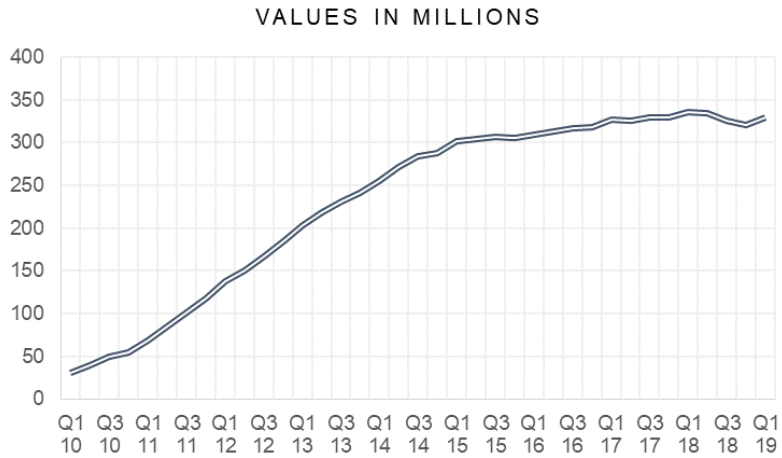

Figure 1: Number of Twitter Users from Q1 2010 to Q1 2019 - Data from (Statista, 2019)

Some perpetrators will use the internet and the social media to cause the cyber bullying, stalking and harassment either for their own pleasure or to gain financial means from them (Shinder & Cross, 2008).

Big Data (BD) that is being produced in such online platforms can potentially offer valuable insights (Hosseinian-Far et al., 2017), yet inferring and identifying perilous crimes from the data have become very challenging. The complexities arising in BD and the challenges in BD analysis are not only caused by the high volume of data, and can be due to the high velocity, variety, velocity or veracity of data generated in social media platforms (Hosseinian-Far et al., 2017). The cyber criminology of social media can occur in a reactive manner where the law enforcement teams and/or security specialists attempt to infer from the available data after the cyber crime has occurred. In the contrary, a predictive approach is a preferred method for envisaging a crime that is to occur prior to it happens (Farsi et al., 2018). In

the section below, we examine behavioural analytics as an emerging method for businesses to gain competitive advantage, and how behavioural analytics could be used for facilitating cyber criminology in social media platforms. As an instance of these crimes, we can discuss some of these in more details.

As the Internet is becoming a key part of our life's and the majority of us are becoming more and more dependent on the usage of social media in order to keep in contact with our relatives, friends, colleagues, associates or even find new friends. However, this presence on the cyberspace comes with worries:

- The majority of social media users are blind to cyber bullying and its effects on victims as they might not consider or beware that sending an inappropriate messages / pictures / comments could cause the receiver or the intended victim anxiety, humiliation, depression and ultimately lead to a suicide (Hinduja & Patchin, 2014). Cyber Bullying has a number of different types, as there are numerous ways of bullying someone online.
- Online Harassment - This involves the act of sending insulting, rude, offensive messages to the intended victim. Such messages / comments / photos are abusive or humiliating in nature (Hinduja & Patchin, 2014).
- Trickery and Outing – This involves an act when one shares another's personal information in order to trick that person or has the purpose to divulge secrets with the intention of on warding that to others. Such acts may involve private photos, images and videos too (Button & Cross, 2017).
- Cyber Stalking – This involves an act of constant messages being repeatedly send to another or a group with threatening, intimidating and abusive behaviour in nature. Such acts may also be illegal and could be treated as a criminal offence depending on the contexts that is be circulated. This would also include sending out false rumours and gossip to others on social media applications. This may also include altering images of others with the intention of posting in online for the purpose of bullying (Kowalski & Guimetti, 2014).
- Exclusion from a Group – This is an act where others deliberately leave the intended victim out of a group such as online apps, gaming sites, group messages and other online meetings. Unfortunately, this form of cyber bullying is very common among the younger generation (Hinduja & Patchin, 2014).
- Impersonation – This act involves one hacking into another's email or social networking account with the intention of using the account to send malicious and humiliating posts, images to/ about others. This act also involves the setting up of fake profiles on applications, social network sites, and online boards, such activities are very hard to get rid of (Kowalski & Guimetti, 2014).

5. Preventive vs. Reactive Policing

Ratcliffe (2003) views intelligence-led policing as a strategic effort to reduce crime and to adopt a preventive approach to tackle crimes. He defines it as "the application of criminal intelligence analysis as an objective decision-making tool in order to facilitate crime reduction and prevention through effective policing strategies and external partnership projects drawn from an evidential base". He goes on to argue that the police authorities act as the decision maker in the context and the impact made by the police within the criminal environment is influences by the intelligence provided (See Fig. 2).

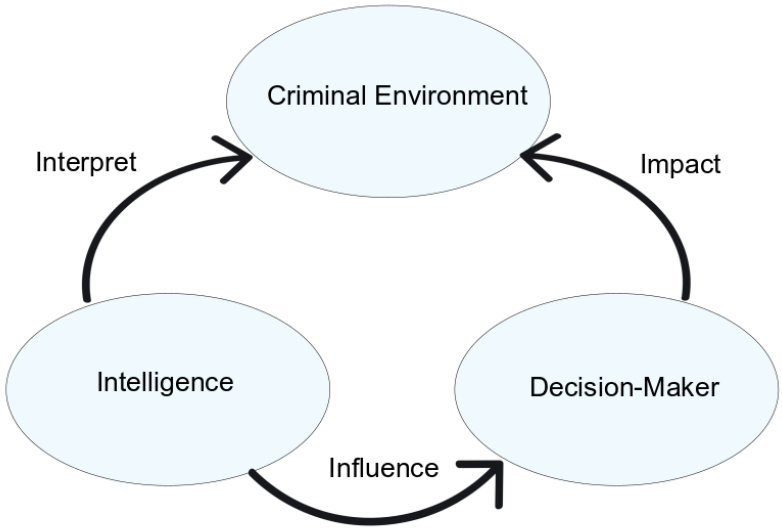

Figure 2: Intelligence-Led Policing – Redrawn with contents adapted from Ratcliffe (2003)

Lum et al. (2011) introduced a crime prevention matrix that sees reactive approaches to policing on the other side of the spectrum where the police acts after the crime has occurred or in the best scenario when the crime is taking place. The preventive approaches on the other hand, attempt to prevent a crime from occurring (Sherman & Eck, 2003). One of the dilemmas that the police will need to consider is the accuracy of ex-ante approaches to crime prevention, and to minimise bias through reasonable approaches such as risk management (Kamin & Rachlinski, 1995).

Technology can play an important role in pricing the intelligence required for implementation of preventive policing. Artificial intelligence (AI) and machine learning techniques can play a vital role in proving reliable intelligence to police forces (Farsi et al., 2018). In a social media context. the data for such techniques could be provided by the social media platforms themselves. The interactions between individuals or groups may provide some valuable input to these AI approaches. In the following sections, we discuss behavioural analytics in social media.

6. Behavioural Analytics

Behaviour Analytics emerged with the advances in Web 2.0 and the introduction of numerous online business models (Squicciarini, et al., 2017). Many technologies have been developed to assess the behaviour of the online users on different social media platforms and predict their behaviours and interests according to the current posting, liking, commenting, etc. The behaviour data can be categorised into individual and collective behaviours (Zafarani & Liu, 2014). Zafarani & Liu (2014) further define the individual behaviour as the behaviour shown by a user when interacting with another user, a community or an entity (an example of a user-entity individual behaviour is a user liking a post). The collective behaviour is the behaviour exhibited by individuals as part of group behaviour. The inherent complexity of behaviour analysis and the multifaceted interactions seem to be very challenging, however such analysis can potentially bring numerous benefits to businesses. The collected behaviour data are then fed into complex computational algorithms to market the products or services to the right audience based on the users' already shown predictive behaviour and interests. Such business intelligence and insights clearly contribute to businesses gaining competitive advantage over their competitors. Ghostery is a browser extension developed in 2009 (Ghostery, 2018) by which website visitors can gain a detailed site analysis by recognising the site trackers and analytics extensions. Some of these trackers are aimed at improving targeted advertisements by analysing the users' interests, interactions and social behaviour in the online platforms. For instance, Lotame provides such a holistic overview on the consumers behaviours collected through various online sources (Lotame, 2018). Full Circle Studies is another firm with a tracker used facilitating Internet market research by providing targeted advertisements to consumers, irrespective of the industry (Full Circle Studies, 2018). Matomo is another web analytics platform by which businesses can gain a richer perspective of their visitors through the log analytic facility provided by the technology (Matomo, 2018).

The online behaviour is representative of the behaviour that individuals embody in real life (Kularathne, et al., 2017). This would indicate that online consumer transactions and behaviour could also benefit other disciplines such as cyber threat analysis, crime data mining and prediction (Farsi, et al., 2018). The UK Cyber Security Strategy first introduced in July 2009, highlights three strands by which UK businesses could get more vigilant when combatting cybercrime. The first two elements i.e. Reduce Risk and Exploit Opportunities are directly reliant on the third strand to improve knowledge, capabilities and decision making (UK Home Office, 2011).

To make informed decisions within a context, computational and predictive techniques could be applied on behavioural data to facilitate combatting potential cyber and cyber enabled crimes. The datasets on consumer behaviour is typically generated in the form of XML and JSON (Batrinca &

Treleaven, 2015). Gephi (open source) or the Excel plug-in NodeXL are some instances of the analytics tools which then crunch the collected data and produce meaningful insights. Such an approach could be applied in the cyber defence context with a view to identify patterns of behaviour and predict potential cyber and/or cyber-enabled crimes. Below are the proposed computational techniques that can be applied on behaviour data on social media, together with some examples where the techniques are applied in different contexts.

The behaviours that are widely observed on the social media, online networks, and other intelligent systems, are very complex. It has become increasingly challenging to search and extract useful information from the collective knowledge stored digitally in the various forms including blogs, web pages, images, sounds, videos, and social networks. It would be then very important to develop appropriate tools to efficiently identify behavioural patterns between individuals, groups and population directly or indirectly producing digitised information. Retrieving information from the web search, using keywords is very tedious task and normally does not produce accurate and detailed findings. An alternative approach to the keyword search is Topic modelling. This specific machine learning approach is presented in section 7.

7. Topic Models

Topic Modelling is an unsupervised machine learning algorithm in Natural Language Processing that identifies relationships and associations within textual data. The application of Topic Modelling has been widely used on raw text data, where meaningful clusters (topics) are generated by the model. Several predictive solutions have been presented for selected research problems by means of topic models. These have been applied in a variety of subject areas namely bioinformatics, multilingual data and machine translation, sentiment analysis in social sciences, and inference for document analysis.

Topic Models were nitially introduced by Blei et al. (2003), Latent Dirichlet Allocation (LDA) has gained its popularity over the years in its success at modelling topics in discrete data. Blei described a way to uncover hidden topics from documents by determining the hidden per-document topic distribution. LDA is an unsupervised generative probabilistic model, often used for the purpose of topic modelling documents. The model assumes that topics within documents can be represented as probabilistic distributions over the words in a document and the word distributions across topics share a common Dirichlet prior (Jelodar et al., 2019). The concept behind LDA is the assumption that words from a particular topic will occur over a probabilistic distribution.

LDA assumes that documents can be represented as a mixture of latent topics, and within these documents are words that follow certain probabilities. In order to understand how topics are determined by the model, we first have to understand how a document is generated. The number of words within a document is determined possibly following a Poisson distribution. Since a document will contain a mixture of topics, the topic mixture of the document can be characterized as following a Dirichlet distribution over a fixed number of topics. Each word in the document are then selected based on the topic distribution within the document. With this process in mind, LDA uses this knowledge to break down the structure of a document to identify topics within them.

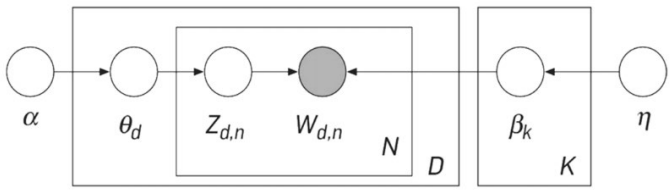

Figure 3: Plate notation of LDA (Blei 2012, p.81)

Based on Fig. 3 shown above, it can be observed that words (Wd,n) within documents (N) and the collection of documents (D). The number of topics is denoted by K, is set by the model user. The collection of documents contains several hidden topics and dependencies. The hidden topics are uncovered by the process of computing the posterior distribution of topics within a document, where the numerator is the joint distribution of all random variables:

$$p(\beta_{1:\mathrm{K}}, \theta_{1:D}, \mathrm{Z}_{1:D} | W_{1:D}) = p(\beta_{1:\mathrm{K}}, \theta_{1:D}, \mathrm{Z}_{1:D}, W_{1:D}) / p(W_{1:\mathrm{D}})$$

Topic models have been widely applied for various purposes, and slightly altered to fit the task at hand. While the models differ from one another slightly, LDA has been commonly used as the foundation of a topic model.

Topic modelling (Blei, 2012) methods learn a latent space in observed data (as a collection of documents, images, videos and other digital formats) allowing to represent them in a low-dimensional space of so-called topics. Typical activities or behaviours can be viewed as sets of features that often come together. Topic modelling can be then viewed as a method to identify these types of statistical regularities. As a result, a topic model has become a promising tool for probabilistic behaviour modelling and detecting anomaly. Although, the technique was initially developed for text mining (Hofmann, 1999; Blei, et al., 2003), it has been applied in a wide range of other fields including computer vision and social network analysis (Tang, et al., 2009). For instance, topic models can be viewed as a suite of algorithms that discovers the hidden thematic structure in the collected documents retrieved from a web search. These algorithms are very helpful in modelling the users' behaviours

based on more efficient methods of searching, browsing and summarising very large amounts of texts (or images and video clips). In other words, topic modelling ca be used as an efficient algorithm for Behaviour modelling in social networks; this is in line with the core framework of "data-to-knowledge-to-service" pipeline (see Fig 4) where behavioural data are considered as the input to support services and systems of the online social networks including precise recommendation and anomaly detection.

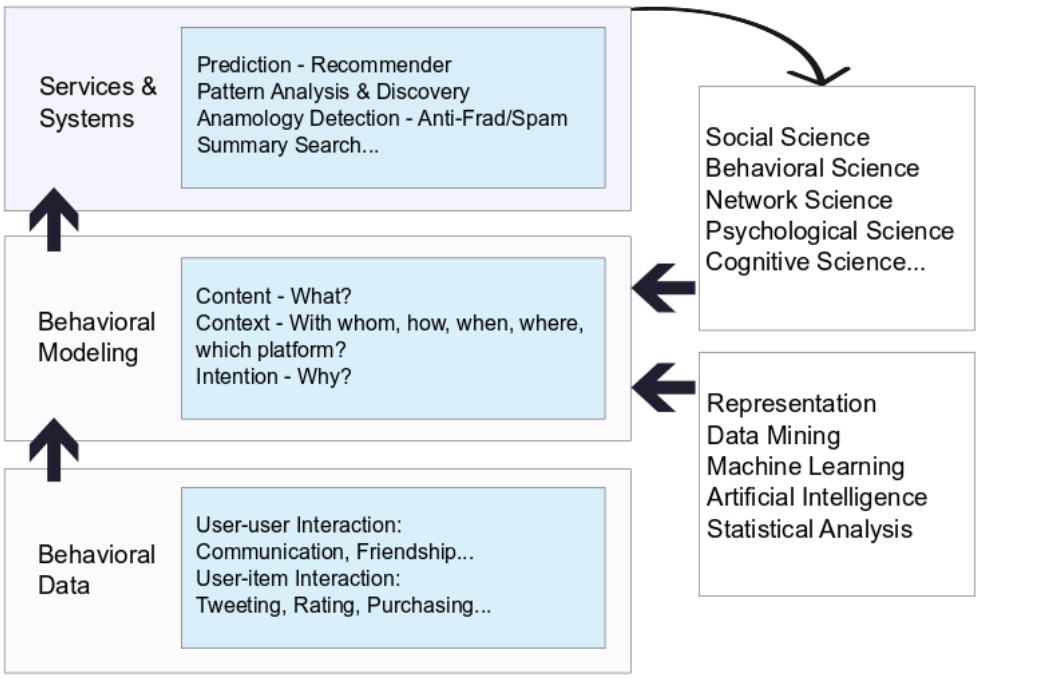

Figure 4: Behaviour modelling is a core framework of the "data-to-knowledge-to-service" pipeline – Re-drawn with contents adapted from (Jian, 2017).

Probabilistic topic modelling algorithms categorise the retrieved topics based on the themes identified by the algorithms. The models which are widely used in topic modelling, are Latent Semantic analysis (LSA), Probabilistic Latent Semantic Analysis (pLSA) and Latent Dirichlet analysis (LDA) (Hofmann, 1999). By applying these models on the search history or online data of users, valuable searched topics including any suspicious activities or anomaly behaviours can be detected. LDA can be used to automatically group documents into topics according to dependencies between words and documents (Blei, et al., 2003). This method can be extended for the personalised preference analysis (Narang, et al., 2013) with an application in discovering the topic-level social dynamics in social media text-based data (e.g., Twitter). Nevertheless, LDA suffers from the limitation that is uninterpretable and the representations are too general. As a result, mining the entities and events, the attributes and aspects related to the entities and events, and the users' sentiments will facilitate the modelling of behavioural contents and users' intentions underlying the User-generated content.

8. Proposed refinements

An alternative approach to the above method is the Hierarchical Dirichlet Process (HDP) (The et al., 2005), which is widely used in probabilistic topic modelling, where the data under consideration could be documents, clips or videos and the components would be the distributions of terms that reflect recurring patterns (or “topics”) within the collection. One limitation of HDP analysis is that the proposed Bayesian inference algorithms require multiple passes through all data (Wang et al., 2011). This would make them intractable for very large-scale applications in the social media context. A method to overcome this challenge will be to investigate various inference algorithms for the HDP, including online variational inference algorithms or Expectation Propagation algorithm (Minka, 2001) so that the resulting method can be easily applicable to massive and streaming data. The variational and Expectation Propagation algorithms have been significantly promising in analysing massive data and are considerably faster than traditional inference algorithms in the HDP. Nonetheless, their applications on behavioural modelling are very limited. Therefore, it would be essential to develop new online inference methods to efficiently analyse very large data sets, such as streaming texts, image or videos, which are very common in social media. Using probabilistic models, accurate prediction and detection of user behaviour can be evaluated online. Such methods could be used to detect the complex behavioural interactions between users/groups and predict how they are likely to act in the future, in the real time. Such a behaviour model can also effectively used for anomaly detection or any abnormal activities in social media. Our proposed topic model provides a probabilistic framework for anomaly detection. Under this framework a normality measure can be represented as the likelihood of data or the posterior probability of the specific aspect or topic of the online stream data. Anomaly detection in other data types such as images and video, is conducted differently compared to text data. For the intelligent vision systems for instance, anomaly detection can be investigated in two contexts: observing any abnormal activities as violating typical activities allowed in social media or as a rapid change in behaviour. However, the proposed behavioural modelling can be used to analyse former abnormal activities, a proper probabilistic change point detection methodology is required for the latter. We propose to develop an efficient online framework by which change points can be detected; This can be used for behaviour analysis, and anomaly detection. A change is defined as a breakpoint between normal and abnormal behaviours, and changes can be then viewed as functional breaks in input data. Existing methods (Isupova, 2018) for Gaussian Process (GP) regression over non-stationary data include clustering and change point detection algorithms. Even though these methods require significant computation, they do not provide provable guarantees in terms of accuracy and computational speed, since most algorithms only work in batch

settings (Grande, 2014). This computational complexity can be overcome by combining Bayesian online change point detection algorithm (Saatci, et al., 2010) with Gaussian processes.

9. Conclusion & Discussion

The rise of cyberspace has created a growing variety of crimes that are occurring or are enabled on digital platforms. These crimes are either occurring within the cyberspace, or the digital means are considered as an enabler of traditional crimes. With the ever-growing adoption of Internet technologies and digital cyberspace, the landscape of crimes is shifting. Social media adoption has seen a continuous growth in the past decade, and so the crimes occurring or enabled by such digital platforms. This necessitates a change in policing strategies to put more emphasis on preventive and intelligence-led policing. In this paper, we presented topic modelling as an AI based technique for analysing patterns of behaviour in social media data. Such intelligence, can potentially provide reliable intelligence to police forces to curb cyber and cyber enabled crimes.

References

1. Batrinca, B. and Treleaven, P. C., 2015. Social media analytics: a survey of techniques, tools and platforms. AI and Society, 30(1), pp. 89-116.
2. Blei, D. M., 2012. Probabilistic topic models. Communications, 55(4), pp. 77-84.
3. Blei, D. M., Ng, A. Y. & Jordan, M. I., 2003. Latent Dirichlet allocation. J. Mach. Learn. Res. 3, Journal of Machine Learning, Volume 3, p. 993–1022.
4. Button, M. and Cross, C., 2017. Technology and Fraud: The 'Fraudogenic'consequences of the Internet revolution. The Routledge handbook of technology, crime and justice. London: Routledge.
5. Cabinet Office, 2010. A strong Britain in an age of uncertainty: the national security strategy (Vol. 7953). The Stationery Office.
6. Clough, J., 2015. Principles of cybercrime. Cambridge University Press.
7. Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Chatrabgoun, O. and Montasari, R. (2018) Crime data mining, threat analysis and prediction. In: Jahankhani, H. (ed.) Cyber Criminology, Springer, pp. 183-202.
8. Flatley, J., 2016. Crime in England and Wales: year ending Mar 2016. Statistical Bulletin, 29.
9. Ford, R., 2016. Fraud doubles the number of crimes. The Times, 22.
10. Forouzan, H., Jahankhani, H. and McCarthy, J., 2018. An Examination into the Level of Training, Education and Awareness Among Frontline Police Officers in Tackling Cybercrime Within the Metropolitan Police Service. In Cyber Criminology (pp. 307-323). Springer, Cham.
11. Full Circle Studies, 2018. About Full Circle Studies. Available online at: http://www.fullcirclestudies.com/about.aspx.
12. Gaidosch, T., Adelmann, F., Morozova, A. and Wilson, C., 2019. Cybersecurity Risk Supervision. Journal Issue, 2019, p.15.
13. Ghostery, 2018. About Ghostery. Available Online at: https://www.ghostery.com/about-ghostery/.
14. Gillespie, A.A., 2019. Cybercrime: key issues and debates. Routledge.
15. Grande, R. C., 2014. Computationally efficient gaussian process changepoint detection and regression; PhD Thesis, Boston: Massachusetts Institute of Technology.
16. Hinduja, S. and Patchin, J.W., 2014. Bullying beyond the schoolyard: Preventing and responding to cyberbullying. Corwin Press.
17. Hofmann, T., 1999. Probabilistic Latent Semantic Indexing. Berkley, ACM, pp. 50-57.
18. Hosseinian-Far, A., Ramachandran, M. and Sarwar, D. eds., 2017. Strategic Engineering for Cloud Computing and Big Data Analytics. Springer.
19. Hosseinian-Far, A., Ramachandran, M. and Slack, C.L., 2018. Emerging trends in cloud computing, big data, fog computing, IoT and smart living. In Technology for Smart Futures (pp. 29-40). Springer, Cham.

20. Isupova, O., 2018. Machine Learning Methods for Behaviour Analysis and Anomaly Detection in Video. 1 ed. s.l.: Springer International Publishing A.
21. Jahankhani, H., Al-Nemrat, A. and Hosseinian-Far, A., 2014. Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164). Syngress.
22. Jahankhani, H. and Hosseinian-Far, A., 2014. Digital forensics education, training and awareness. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 91-100). Syngress.
23. Jelodar, H., Wang. Y., Yuan, C., Feng, X., Jiang, X., Li, Y. & Zhao, L. (2019) Latent Dirichlet allocation (LDA) and topic modelling: models, applications, a survey. Multimedia Tools and Applications, 78(11), pp. 15169–15211
24. Jiang, M., 2017. Behavior modeling in social networks. Encyclopaedia of Social Network Analysis and Mining, pp.1-11.
25. Kamin, K.A. and Rachlinski, J.J., 1995. Ex post≠ ex ante. Law and Human Behavior, 19(1), pp.89-104.
26. Kowalski, R.M. and Giumetti, G.W., 2017. Bullying in the digital age. In Cybercrime and its victims (pp. 167-186). Routledge.
27. Kularathne, S. D. et al., 2017. Consumer Behavior Analysis for Social Media. International Journal of Advanced Engineering, Management and Science (IJAEMS), 3(1), pp. 11-21.
28. Lotame, 2018. About Lotame. Available online at: https://www.lotame.com/about-lotame/.
29. Lum, C., Koper, C.S. and Telep, C.W., 2011. The evidence-based policing matrix. Journal of experimental criminology, 7(1), pp.3-26.
30. Matomo, 2018. What is Matomo? Available online at: https://matomo.org/what-is-matomo/.
31. Minka, T.P., 2001, August. Expectation propagation for approximate Bayesian inference. In Proceedings of the Seventeenth conference on Uncertainty in artificial intelligence (pp. 362-369). Morgan Kaufmann Publishers Inc.
32. Narang, K. et al., 2013. Discovery and Analysis of Evolving Topical Social Discussions on Unstructured Microblogs. Moscow, Springer, pp. 24-27.
33. Ratcliffe, J., 2003. Intelligence-led policing (Vol. 248). Canberra: Australian Institute of Criminology.
34. Saatci, Y., Turner, R. D. & Rasmussen, C. E., 2010. Gaussian Process Change Point Models. Haifa, IBM.
35. Schjolberg, S., 2014. the History of Cybercrime: 1976-2014. BoD–Books on Demand.
36. Sherman, L.W. and Eck, J.E., 2003. Policing for crime prevention. In Evidence-based crime prevention (pp. 309-343). Routledge.
37. Shinder, D.L. and Cross, M., 2008. Scene of the Cybercrime. Elsevier.
38. Statista. (2019) Number of monthly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019. Available online at: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

39. Squicciarini, A., Rajtmajer, S. & Griffin, C., 2017. Positive and negative behavioral analysis in social networks. ACM Transactions on the Web (TWEB), Volume 7, pp. 1-12.
40. Swire, P., 2009. No cop on the beat: Underenforcement in e-commerce and cybercrime. J. on Telecomm. & High Tech. L., 7, p.107.
41. Tang, J., Sun, J., Wang, C. & Yang, Z., 2009. Social Influence Analysis in Large-Scale Networks. Paris, ACM, pp. 807-816.
42. Teh, Y.W., Jordan, M.I., Beal, M.J. and Blei, D.M., 2005. Sharing clusters among related groups: Hierarchical Dirichlet processes. In Advances in neural information processing systems (pp. 1385-1392).
43. UK Home Office, 2011. Social and behavioural science: countering the terrorist threat. Available online at: https://www.gov.uk/government/publications/social-and-behavioural-science-countering-the-terrorist-threat.
44. Wall, D.S., 2013. Policing identity crimes. Policing and Society, 23(4), pp.437-460.
45. Wang, C., Paisley, J. and Blei, D., 2011, June. Online variational inference for the hierarchical Dirichlet process. In Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics (pp. 752-760).
46. Zafarani, R. & Liu, H., 2014. Behavior Analysis in Social Media. IEEE Intelligent Systems, 29(4), pp. 1-4.