Using Facial Recognition to gather Social Media Intelligence

Jack Neilson

January 24, 2018

1 Literature Review

1.1 Background

1.1.1 SOCMINT

Social media intelligence (SOCMINT) is an emergent field in intelligence gathering where data is gathered from social media profiles. Massive amounts of data are added to social media services every day (Omand et al., 2012), much of it personal, making social media sites a potentially valuable resource when gathering information about groups or individuals (Ruiz, 2018). Social networks have also been used as a means of communication between persons of interest to the security services, making mining intelligence from their profiles a high priority (Omand et al., 2012)(Kilburn and Krieger, 2014).

As it stands, social media intelligence sources are woefully underutilised. After the 2011 riots in London that were organised in large part on social media, Her Majesty's Inspectorate of Constabulary stated that the police services were "insufficiently equipped" to effectively use SOCMINT in their response (Antonius and Rich, 2013). This is not to say that the value of SOCMINT is not realised however, as many intelligence agencies are investing in tools to effectively gather and analyse SOCMINT (Antonius and Rich, 2013) or are performing case studies in to potential uses (Klontz and Jain, 2013).

While traditional human intelligence (HUMINT) focuses on building rapport and a foundation of trust in order to extract information from people of interest (Russano et al., 2014), users of social networking websites are much more likely to divulge personal information due to a misplaced senes of privacy (Livingstone, 2008). This makes SOCMINT attractive when attempting to gather data with little investment. The amount of data available to gather is vast in comparison to HUMINT sources (Omand et al., 2012), making mass collection and analysis viable (Unknown, 2013). The nature of SOCMINT makes it easier to analyse than HUMINT, which relies on "tells" and small social cues (Russano et al., 2014).

1.1.2 Uses of SOCMINT

As previously stated, SOCMINT has seen some emergent use particularly in the security services. The Greek Ministry of Defence has developed a framework to identify individuals fitting certain psychiatric profiles from their social media accounts to allow for early identification of potential insider threats (Kandias and Stavrou, 2015). By identifying factors that multiple intelligence agencies agree make a person more likely to pose an insider threat or negatively influence society (See appendix A), they were able to map usage habits (intensity, content, popularity) to these factors to draw conclusions about clusters of users. So far, the research has been helpful in insider threat prevention, delinquent behaviour prediction and forensic analysis support.

Maybe write about PRISM?

1.1.3 Facial Recognition

Facial recognition is a much more mature area of research than SOCMINT with many examples of industry usage. Facebook uses facial recognition to automate "tagging" photos with the identity of the persons pictured (Becker and Ortiz, 2008), and large companies are now releasing datasets such as YouTube Faces (Cui et al., 2013) in an effort to advance the field.

This is not to say that facial recognition is not without controversy however, as many privacy advocates have pointed out that accurate face regonition could infringe on their right to privacy (Ruiz, 2018). David Wood and Lucas Introne have posed that accurate facial recognition could lead to increased levels of surveillance, with no way to "opt out" (Introna and Wood, 2002).

References

Antonius, N. and Rich, L. (2013), 'Discovering collection and analysis techniques for social media to improve public safety', **3**, 42.

Becker, B. C. and Ortiz, E. G. (2008), Evaluation of face recognition techniques for application to facebook, *in* 'Automatic Face & Gesture Recognition, 2008. FG'08. 8th IEEE International Conference on', IEEE, pp. 1–6.

Cui, Z., Li, W., Xu, D., Shan, S. and Chen, X. (2013), Fusing robust face region descriptors via multiple metric learning for face recognition in the wild, *in* 'Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition', pp. 3554–3561.

Introna, L. and Wood, D. (2002), 'Picturing algorithmic surveillance: The politics of facial recognition systems', *Surveillance & Society* **2**(2/3).

Kandias, M. and Stavrou, V. (2015), 'Personal traits analysis as a means to predict insiders'.

Kilburn, M. and Krieger, L. (2014), 'Policing in an information age: The prevalence of state and local law enforcement agencies utilising the world wide web to connect with the community', *International Journal of Police Science & Management* **16**(3), 221–227.
URL: *https://doi.org/10.1350/ijps.2014.16.3.341*

Klontz, J. C. and Jain, A. K. (2013), 'A case study on unconstrained facial recognition using the boston marathon bombings suspects', *Michigan State University, Tech. Rep* **119**(120), 1.

Livingstone, S. (2008), 'Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression', *New Media & Society* **10**(3), 393–411.
URL: *https://doi.org/10.1177/1461444808089415*

Omand, S. D., Bartlett, J. and Miller, C. (2012), 'Introducing social media intelligence (socmint)', *Intelligence and National Security* **27**(6), 801–823.
URL: *https://doi.org/10.1080/02684527.2012.716965*

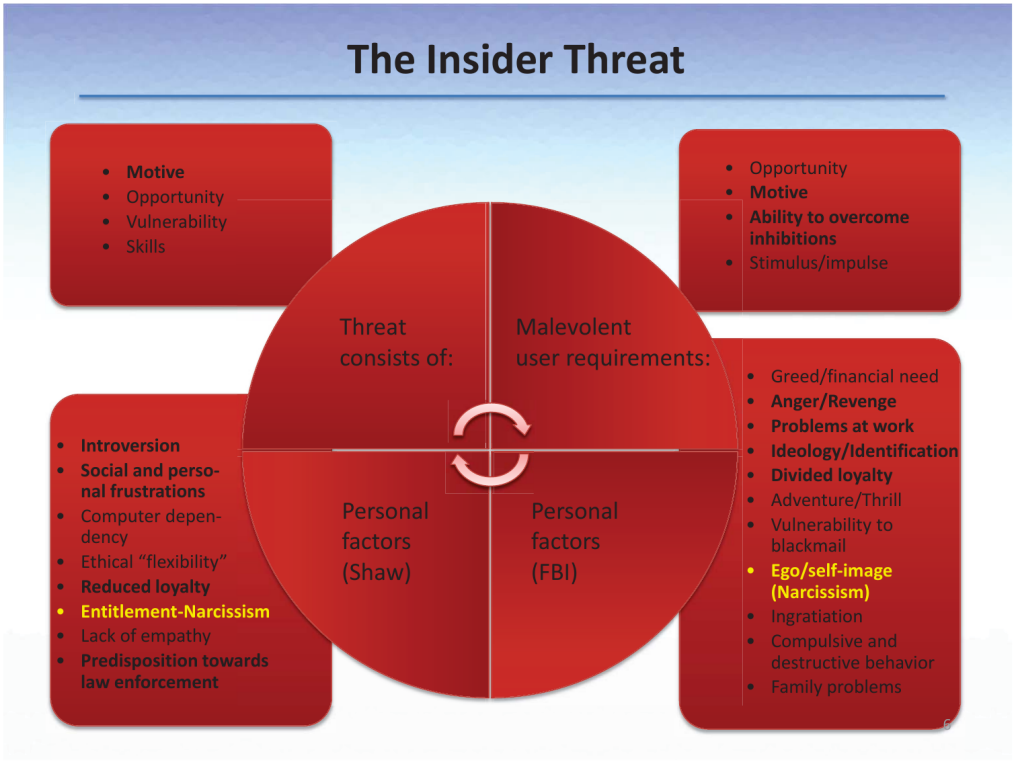
Ruiz, J. (2018), Gchq and mass surveillance, Technical report, Open Rights Group.

Russano, M. B., Narchet, F. M., Kleinman, S. M. and Meissner, C. A. (2014), 'Structured interviews of experienced humint interrogators', *Applied cognitive psychology* **28**(6), 847–859.

Unknown (2013), 'Prism slides', Leaked to several newspapers by Edward Snowden in late 2013.

Appendices

A Threat Graph



Graph of insider threat factors (Kandias and Stavrou, 2015).