Europol's web hunt of Islamic State's Social Media Accounts

David Lowe

Liverpool John Moores University

Email: D.Lowe@ljmu,.ac.uk

Tel No; 0151 231 3918

Europol's web hunt of Islamic State's Social Media Accounts

On the 22nd June 2015 it was reported that Europol was running a new Europe-wide police unit to monitor the internet to track and block social media accounts run or linked to the terrorist group Islamic State (IS).[1] IS has been effective in their use of electronic communications, especially the various forms social media to get their message out to a global audience. One way they have done this is by decentralising their propaganda campaign by allowing its members and those living within the caliphate they formed in northern Syria and north-western Iraq to use their personal social media accounts. As it is estimated that over 25,000 foreign fighters have joined the group in the conflict zone[2] their daily messages are literally reaching a global audience as they are sent in various languages. IS social media accounts have been used to recruit foreign fighters, encourage women to travel to the region and become jihadi brides as well as encouraging families form around the world to in effect emigrate to the IS caliphate.

This increase in the number of citizens who have gone to Syria and Iraq to fight with Islamic state has led to Europol's Director, Rob Wainwright, to warn of the security gap facing EU poling agencies as they try to monitor online communications of terrorist suspects, which is compounded by the fact that by being in Syria and Iraq these suspects are effectively out of reach[3]. His concerns centre on the difficulties the security and policing agencies are currently facing in monitoring electronic communications used by terrorists. Wainwright said that hidden areas of the Internet and encrypted communications are making it harder to

---

[1] Dodd V (2015)_ 'Europol web unit to hunt extremists behind Isis social media propaganda' The Guardian 22nd June 2015 retrieved from http://www.theguardian.com/world/2015/jun/21/europol-internet-unit-track-down-extremists-isis-social-media-propaganda [accessed 23rd June 2015], BBC News 2015 'Islamic State web accounts to be blocked by new police team' 22nd June 2015 retrieved from http://www.bbc.co.uk/news/world-europe-33220037 [accessed 22nd June 2015]

[2] Pantucci R (2015) 'From Al-Shabaab to Daesh' RUSI Analysis 23rd June 2015 retrieved from https://www.rusi.org/analysis/commentary/ref:C55893A6C7A17A/ [accessed 23rd June 2015]

[3] BBC News (2015) 'Terror threat posed by thousands of EU nationals' 13th January 2015 retrieved from http://www.bbc.co.uk/news/uk-30799637 [accessed 22nd January]

monitor terrorist suspects, adding that Tech firms should consider the impact sophisticated encryption software has on law enforcement.

Just using the example of Twitter, Wainwright revealed that Islamic State is believed to have up to 50,000 different Twitter accounts, tweeting up to 100,000 messages a day[4] with Berger and Morgan claiming the number of IS Twitter accounts could be as high as 90,000[5] thereby nearly doubling the number of daily tweets from IS. Katz highlights the difficulty intelligence and policing agencies face in monitoring social media and encrypted electronic communications, where again just using the example of Twitter, she reports how IS is circumventing the blocking of their social media accounts.[6] One method being IS account holders having multiple back-up accounts and tweet followers to follow and retweet up to six accounts at a time. For Katz the threat of IS on Twitter is real. She says Twitter alone is a launch pad for IS recruitment or calls for lone wolf attacks or to send dangerous messages into every corner of the world. This helps to explain why it is important that policing agencies co-ordinate their efforts in monitoring terrorist groups use of electronic communications.

This issue was recognised by the Council of the European Union (EU) in March 2015 where it stated in the fight against terrorism, the internet is a major facilitator for radicalisation to terrorism and agreed that Europol will develop an EU Internet Referral Unit where, amongst its tasks, was to co-ordinate and share the identification of terrorist and

---

[4] BBC News 2015 'Europol chief warns on computer encryption' 29th March 2015 retrieved from http://www.bbc.co.uk/news/technology-32087919 [accessed 30th March 2015]

[5] Berger JM and Morgan J (2015) 'The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter' Center for Middle East Policy at Brooking, 20th March 2015 retrieved from http://webcache.googleusercontent.com/search?q=cache:nUpiATbv50wJ:www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf+&cd=1&hl=en&ct=clnk&gl=uk [accessed 19th June 2015]

[6] Katz R (2015) 'How Islamic State is still Thriving on Twitter' InSite Blog on Terrorism & Extremism 11th April 2015 retrieved from http://news.siteintelgroup.com/blog/index.php/entry/377-how-the-islamic-state-is-still-thriving-on-twitter [accessed 18th June 2015]

extremist online content with relevant partners.[7] This builds on the 'Check the Web' initiative organised by Europol and launched by the Council of the EU in May 2007. While this initiative has had success in child abuse and human trafficking investigations, the programme has had limited success in relation terrorism investigations.[8] This may be due to the difficulty states have had in securing co-operation from communications providers in passing on information relating to suspected terrorist activity to intelligence and counter-terrorism policing agencies. Underlying this difficulty are the concerns communications providers have over the surveillance society and the data protection of their customers.

Concerns of the surveillance society regarding abuses to individuals' rights of privacy and data protection received global awareness following the former employee of the US intelligence agency, National Security Agency (NSA), Edward Snowden's revelations on the activities of the NSA and its co-operation with the UK's counterpart, GCHQ.[9] Snowden claimed that some NSA surveillance was carried out without lawful authority or the NSA used legal loopholes by requesting assistance from GCHQ to monitor the activities of US citizens, especially in relation to the bulk collection of electronic communications data. An advantage of Europol taking the lead in running the monitoring of IS internet use is that privacy rights and data protection is deeply embedded in EU law. This will apply to Europol as it became a legal EU body under articles 87 and 88 of the 2009 Treaty of Lisbon and the EU Council Decision of the 6th April 2009.[10] This is important in relation to accountability as

---

[7] Council of the European Union (2015) Fight against terrorism: follow-up to the statement of 12 February by the Members of the European Council and to the Riga Joint Statement of 29 January by the Ministers of Justice and Home Affairs of the EU – Implementation Measures 2nd March 2015 6606/15 retrieved from http://webcache.googleusercontent.com/search?q=cache:ZA8lI-RxecQJ:www.statewatch.org/news/2015/mar/eu-council-cosi-terrorism-riga-statement-followUp-6606-15.pdf+&cd=1&hl=en&ct=clnk&gl=uk [accessed 14th April 2015]

[8] Argomaniz J (2012) 'The EU and Counter-Terrorism: Politics, polity and policies after 9/11' London Routledge, p.45

[9] Greenwald G (2014) 'No Place to Hide: Edward Snowden, the NSA and the US Surveillance State' New York: Metropolitan Books

[10] Kaunert, C and Leonard, S (2011) 'EU Counterterrorism and the European Neighbourhood Policy: An Appraisal of the Southern Dimension' *Terrorism and Political Violence* 23(2) 286-309, p.294

by having vertical legal legitimacy Europol's actions can be scrutinised by the EU's court, the European Court of Justice (ECJ). Only recently the ECJ showed how ruthless it can be in protecting privacy rights and data protection when in the *Digital Rights* case[11] it held the 2006 EU Directive on data protection was invalid. The ECJ held that legislation must lay down clear and precise rules governing the scope and application of surveillance measures as well as imposing minimum safeguards. This is so persons whose data has been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against unlawful access and use of that data.[12] This would apply to the current Europol headed police unit monitoring the internet as it is specifically to deal with IS and it is looking for communication linked to radicalisation and potential activity linked to terrorist attacks.

This proposal is a sensible way forward as with the EU having data protection so deeply embedded in its law and activities, Europol is more likely to be successful in receiving co-operation of internet and communications service providers. As a result it can be an effective unit in assisting those agencies involved in counter-terrorism investigations. Of course as stated, this is still a difficult task in monitoring the wide range of social media and internet sources available to groups like IS as well as monitoring the large number of communications made in those sources, but it is a step in the right direction.

[11] C-293/12 available on http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dee19ddd9932bb48eb9b68bf016f816643.e34KaxiLc3eQc40LaxqMbN4ObxyMe0?text=&docid=153045&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=265427

[12] *Digital Rights* Case C-293/12, paragraph 54