

2015

'Questions about Dawlah. DM me, plz.' The Sock Puppet Problem in Online Terrorism Research

Laura Huey

University of Western Ontario, lhuey@uwo.ca

Hina Kalyal

University of Western Ontario, hina.kalyal@fulbrightmail.org

Follow this and additional works at: <https://ir.lib.uwo.ca/sociologypub>



Part of the [Sociology Commons](#)

Citation of this paper:

Huey, Laura and Kalyal, Hina, "'Questions about Dawlah. DM me, plz.' The Sock Puppet Problem in Online Terrorism Research" (2015). *Sociology Publications*. 33.

<https://ir.lib.uwo.ca/sociologypub/33>

**‘Questions about Dawlah. DM me, plz.’
The Sock Puppet Problem in Online Terrorism Research**

Laura Huey, University of Western Ontario
Hina Kalyal, University of Western Ontario

This paper explores the problem of deception in online terrorism research. While conducting research into the growing phenomenon of female migration to Islamic State-held territory by Western females, we began following a Twitter account exhibiting suspicious activity. The account owner – believed to be a Canadian teenage female – indicated interest in learning more about joining the IS. We tracked this account for three weeks in order to discover more information about its activities and thus to develop a set of key indicators that might help predict future migration risk. We subsequently learned it was a fake account (‘sock puppet’) established to fool IS recruiters. The operation of such ruses and the problems they create is discussed here.

Throughout the latter part of 2014, media outlets across the globe began reporting on a new and disturbing trend: women, often young and unmarried, were leaving their homes and families to sneak into Syria and Iraq in order to join the terrorist group known as the Islamic State (IS)¹. In the majority of instances, friends and family were stunned, stating they had no previous clues as to the possibility their sister or daughter had been radicalized. One illustrative example is that of Zehra Duman of Melbourne, Australia. In November of 2014, the twenty-one year old college student left for Syria without revealing to anyone that she was leaving (Hamblin 2014). She then reappeared on December 11th, via social media, as the bride of Mahmoud Abdullatif, a former Australian party boy turned foreign fighter for the Islamic State (Dean 2014). Distraught, her father told reporters, “she’s been brainwashed, she wasn’t like this three or four months ago” (cited in Dean 2014).

¹ Explain acronyms here and am using Islamic State.

While it is highly unlikely that young women like Duman are being ‘brainwashed’ through social media, it is the case that pro-IS propaganda easily distributed through online platforms is helping to fuel this disturbing trend. On sites such as Facebook, ask.fm, and principally Twitter, vulnerable individuals join networks of individuals who promote radical Islamic views through a variety of standard propaganda techniques, ranging from emotional appeals through the presentation of scenes of real or misrepresented atrocity (Hoyle, Bradford and Frennett 2015) to the subversion of memes and use of other rhetorical and pictorial devices intended to depict jihad as ‘cool’ (Stern 2012). Once primed to accept IS ideological doctrine – in particular the belief that it is their duty as faithful Muslims to support the IS – they are amenable to suggestions to migrate (‘hijrah’) to IS held territory in order to support their embattled IS brothers and sisters. Once they successfully complete their hijrah, they then assume a new powerful identity within IS group culture, as a Muhajirah² or migrant.

Although the overall numbers of women making hijrah to IS held territory is unknown, and is likely to be at best a fraction of male foreign fighters making similar journeys, the presence of women within the overall numbers has drawn significant media attention. This attention has fuelled panic in the West, and in other parts of the globe, concerning the pull of IS recruitment strategies and the vulnerability of young women. As a result, researchers, security professionals, family members and others, have been keen to understand the trend and, perhaps more importantly, to garner knowledge of what online indicators might point to someone representing a potential migration risk.

² Although there is a standardized form of Arabic, there are variations in language and spelling across most countries in which Arabic is spoken. We are using the terms most frequently employed by pro-IS Twitter users, Muhijrah (singular) or Muhijrat (plural)

Research in online terrorism is, however, frequently hampered by an ubiquitous problem on the Internet: the use of false identities known in Internet parlance as ‘sock puppets.’ Sock puppets are accounts that are specifically set up with the intention of deceiving others in online forums and they are found within and across Internet communities, from self-help bulletin boards and online chat groups for pet lovers to Facebook and other social media platforms (Bu, Xhina and Wang 2012). In relation to online activities linked to terrorism, we find sock puppets used to disseminate terrorist group propaganda, to conduct surveillance on suspect individuals and groups, to collect material for news articles and research reports, and for a variety of mischievous and other purposes. For terrorism researchers, our efforts to collect valid data from online account activity can be seriously hampered by the use of sock puppets, especially for those of us who rely exclusively on online posts as our data source.

Within this paper we draw on a case study based on our own research experience. While collecting qualitative data on approximately 79 pro-Islamic State accounts identified as belonging to female account holders, we tracked the online activities of a sock puppet for a period of three weeks. What was particularly interesting about this account and its activities is that its posts and online behaviours, individually and in concert, indicated that the individual – purportedly a young, Canadian female – might represent a significant migrant risk. While watching the account, and looking for continuing indications that its owner was seriously interested in decamping for Syria, we used its online activities to begin developing a list of indicators that parents, researchers and security professionals should watch for if they suspect someone to be a hijrah risk. Although we had some initial suspicions we were following a sock puppet account, without confirmation we proceeded as though it were a legitimate account belonging to a young woman sincerely seeking information about migration to IS-held territory.

After the account disappeared, we discovered that it had been, indeed, a fake account. In the pages below, we reveal the extent of the ruse to show how convincing sock puppet accounts can be and thus the pitfalls researchers face when working in online milieus.

The Islamic State, Twitter and Sock Puppetry

A central misconception about pro-jihadist terrorism found within public discourse is that women play little to no role in group activities. This erroneous belief can be attributed to women's relative inferior status within Salafist movements. Although it is manifestly the case that women within many pro-jihadist groups do play a lesser role – for example, being barred from the battle field (Lahoud 2014) – they do effectively participate in a number of other meaningful ways (Al-Tabaa 2013). For example, they raise funds (Cunningham 2007), recruit new members (Bloom 2011), disseminate propaganda (Cragin and Daly), run charity groups on behalf of their organizations (Cunningham 2007) and, within some groups, play a more active role by participating in hostage takings and suicide bombings (Cunningham 2007; Bloom 2011).

Among jihadist groups, the Islamic State is unusual in that it has found another use for female recruits: as settlers to occupy territory currently held in Syria and Iraq. Within this role, women are expected to function as wives of mujahedeen (fighters) and as mothers to a new generation of believers under what IS leaders claim as a new caliphate. To encourage women to migrate to Syria or Iraq, female migrants and pro-IS sympathizers elsewhere disseminate pro-hijrah propaganda through social media (Klausen 2015) and provide information or connections on the ground to help facilitate their journey (Hoyle et al. 2015).

As female migration to jihadist-held territory is a rather recent phenomenon, it is not surprising that, to date, very little research in this area exists. One exception is a recent study by Carolyn Hoyle and colleagues at the Institute for Strategic Dialogue of female migrants to IS-

held territories. Drawing on an analysis of social media posts across multiple media sites by twelve female account holders, Hoyle et al. (2014) identified a number of reasons cited by Muhajirah for going to Syria and/or Iraq. Given the constant barrage of atrocity-related imagery propagated by IS across social media sites – much of it centred around real or perceived attacks against Muslims in Syria, Mali and Chechnya, among other places – it is not surprising that one of the reasons cited by migrant women in the Hoyle study was a sense of being under attack in the West and elsewhere and a desire to battle anti-Muslim/anti-Sunni oppression. A second related reason cited was the desire to participate in the construction of a new, utopic society in the form of an Islamic Caliphate – that is, a Sunni state governed under a strict version of shari’ah law (ibid.). Third, Hoyle et al. state that Muhajirah believe that it is their duty as faithful Muslimah (female Muslims) to participate in hijrah that supports jihad and the building of an Islamic state, and that many see in that duty a heroic identity to which they can ascribe (ibid.). All of these reasons tie together in the form of a common bond – sisterhood – that reinforces women’s sense of Muslim community (umma) and thus obligation (ibid).

If little is known about the hijrah phenomenon among women, even less is known about the potential for individuals to become female recruits. As a result, researchers have begun to look at women’s online activities, searching for clues that can lead to further insights into this phenomenon. In doing so, they are however confronted by the existence of individuals and groups who create accounts specifically for the purpose of misrepresenting themselves to others – that is, by sock puppets.

A sock puppet is an online account established in order to misrepresent the identity of the owner and his or her intentions. Bu et al. (2012: 367) explain:

The term—a reference to the manipulation of a simple hand puppet made from a sock—originally referred to a false identity assumed by a member of an internet community who spoke to, or about himself while pretending to be another person. The term now includes other uses of misleading online identities, such as those created to praise, defend or support a third party or organization.

As these authors note, sock puppets are used for a multitude of purposes. For example, researchers and journalists may use them to collect information on various groups and activities for news articles and reports (Elovici, Fire, Herzberg and Shulman 2014). Companies use sock puppets to plant positive messages about their products in online forums (Bu et al. 2012), whereas criminals employ false identities in pursuit of opportunities to victimize others (Zheng, Lai, Chow, Hui and Yui (2011). Cybervigilantes create fake online identities to collect information about targeted individuals and, in some cases, to engage in vigilante acts against those targets (Huey, Nhan and Broll 2014). Sock puppet accounts can also be linked to botnets that harvest user data or plant a stream of messaging in user groups and forums (Bilge et al. 2009; Boshmaf et al. 2011). While still others employ sock puppets for a range of personal reasons, from the desire to be mischievous ('troll') to wanting to spy on a loved one.

A significant problem for terrorism researchers, law enforcement and others is the question of how to identify posts made by legitimate accounts from those created by sock puppets. One technique is to use geolocation software in order to find account holders (TRAC 2015). However, many individuals are aware of the tracking facilities on their mobile phones and turn them off. As we have seen within pro-IS networks, those who are not aware are warned about such facilities by more tech-savvy individuals. Acquiring an user's IP address might also prove useful to distinguishing legitimate accounts from false accounts, but such efforts are also fraught with problems, including the need for researchers to interact directly with a targeted account, an activity many research ethics boards would frown upon. Some researchers have

attempted to construct sock puppet detection algorithms based on authorship-identification (Zheng et al. 2011; Bu et al. 2012), but thus far none of these techniques are widely available to researchers. Thus, the problem of discerning legitimate accounts from false ones – and thus valuable from useless data – remains a concern for researchers.

Method of inquiry

Data collection and analysis

The present paper is based on a case study that arose as the result of a larger mixed methodological study of gender and online radicalization. The larger study, which began in January 2015 and remains ongoing, specifically examines women’s participation in online radical milieus (Twitter, Facebook, YouTube and other forms of social media hosting pro-jihadist content). It is composed of three smaller inter-linked projects: a quantitative analysis of posting/tweeting patterns by males and females (from multiple pro-jihadist groups on Twitter³), a network analysis of selected online Twitter-based groups (pro-IS, pro-AQ) and a qualitative study tracking and analyzing posting activities of approximately 79 Twitter accounts disseminating pro-IS content, approximately 50⁴ of which are presently active.

The data for this paper is drawn exclusively from the third project. Beginning with an analysis of the followers of a popular pro-jihadist Twitter account (605 followers), one of the researchers used snowball sampling to identify and follow approximately 79 accounts posting pro-IS content. Initial criteria for selection included: the account owner self-identified as female,

³ Twitter was selected as the primary data collection site because of our interest in the IS. As other researchers have noted (Klausen 2015), Twitter appears to be the online milieu of choice for IS followers.

⁴ The number of accounts tracked is variable due to Twitter’s account suspension activities – Twitter administrators periodically suspend accounts due to graphic or other objectionable content (through their own searches or user complaints). In many instances, the account owner simply resumed under another account and tracking continued. In other cases, the account owner either left the site or we were unable to relocate them.

posted principally in English and was a member of one or more networks associated with IS. Determinations as to gender were aided by the use of female titles for names/twitter handles, pictures of female figures as avatars and/or references to one's role as a mother or wife. Over time, as accounts were suspended or deleted, new accounts were added to the list of those being 'followed'. As each woman was added, her Twitter account was captured in PDF using Adobe Acrobat and her tweets were collected on a daily basis in Excel format (for use with NVIVO) through the analytic software, Twitonomy. Further information about the account holder's online activities was also sought through keying her twitter name and handle into online search engines. These searches yielded links to Tumblr, Instagram, YouTube channels and postings on ask.fm (all open sources). Account holders also posted links to other open source online content, much of it produced by the IS, and this material was also collected with the result that we have 31 documents (e-books, magazines and blogs) specifically referencing hijrah and/or life in IS held-territory. These materials, combined with our ongoing analysis of twitter postings (using NVivo), helped to inform our understanding of the hijrah phenomenon and IS propaganda and recruitment techniques directed at women.

Our analysis of one of the accounts we located through snowball sampling serves as the basis for the present case study.

Pic 1. Blog-based propaganda



Signs of a potential Muhajirah?

On January 21, 2015 an account appeared on Twitter and began following 56 other Twitter accounts. One of these is an account dedicated to tweeting quotes from former Al Qaeda operative, Anwar al-Awlaki. Other accounts belonged to two well-known female IS recruiters. As these particular recruiters and other members of their networks were being tracked by the research team, we became aware of the account on January 28th and began to follow the account and collect its posts. A key factor in the decision to target this particular account for data collection were the names used: each of which denoted a female identity. For instance, *uhkt(i/e)* is Arabic for sister, *Umm* means mother, and a female variant for one of Canadian nationality. The combination suggested a Canadian female, which, given, our interest in radicalization among Western females, appeared as an appropriate research subject. We note that no other gender clues were immediately apparent; the avatar was simply a green bird (a standard Islamic symbol) and the account background was blank. However, subsequent friendly exchanges

between this account with other female-identified accounts – males and females intermingling freely on social media being generally frowned upon within IS – suggest that the account holder was female or at least believed to be female by other network members.

From tweets posted from January 21st to February 13th, 2015 (when the account was removed from twitter), we were unable to glean few other demographic or other details. One small exception was a potential clue provided as a result of a friendly exchange with another woman linked into pro-IS twitter networks in which she joked of her age, “let me hit two decades first.” Thus, we surmised that the account holder was possibly a teenaged girl.

Pic 2. Account info (name removed)



The account was only known to be active for the period January 21 to February 13, 2015 (it disappeared sometime between the evening of February 11th and the morning of the 13th). During that time we were able to collect only 37 tweets and retweets. Those we collected suggested a serious interest in migrating from Canada to Syria to join the Islamic State.

Sign 1: no vapor trail

Once the decision was made to track this account, we took a screen shot of it to capture its posting history, began following the user to collect her tweets, and engaged in a search for variants of the account name and handle on Twitter to see if this was a backup version of an existing account (a common practice among IS Twitter users, who run multiple accounts so they remain active online even when one account is suspended). Searches on Twitter turned up

nothing. Nor could we find evidence of an earlier version of this account that may have been suspended (often remnants of such accounts remain in the form of posts picked up by Twitter analytics).

Further compounding the mystery surrounding this user was the fact that the poster herself provided no links to accounts on other social media sites, a common practice among IS Twitter users who frequently also use other social media platforms such as ask.fm, tumblr, Instagram and chat sites such as kik (Hoyle et al. 2014). Indeed, for other accounts tracked online we were often able to acquire detailed personal history about an individual from their posting histories, a finding not unique to recruiters and propagandists in IS, who often use their stories as recruitment tools. Indeed, through their presence across multiple social media sites, we were sometimes able to piece together information on several of the pro-IS women living in the West, including full name, occupation, age, marital status and present location. Even in cases where woman took some pains to avoid revealing personal information, the nature of exchanges on social media often entails that some information will be divulged. However, in line with IS recruiters' advice to potential recruits, the owner of the suspect account clearly took pains to avoid posting any information that might reveal her identity or specific location.

Sign 2: new account immediately joins pro-IS networks

What made the lack of what we term here an online 'vapor trail' particularly intriguing is the fact that within one day of appearing on Twitter, this 'new' user had identified and begun following several accounts belonging to high profile IS members. Further, within a matter of days she was retweeting their comments. For example, she retweeted the following message from a British foreign fighter in Syria: "O you who have believed, TAKE YOUR PRECAUTION and either go forth in companies or go forth all together." – Surah Nisa 4:71."

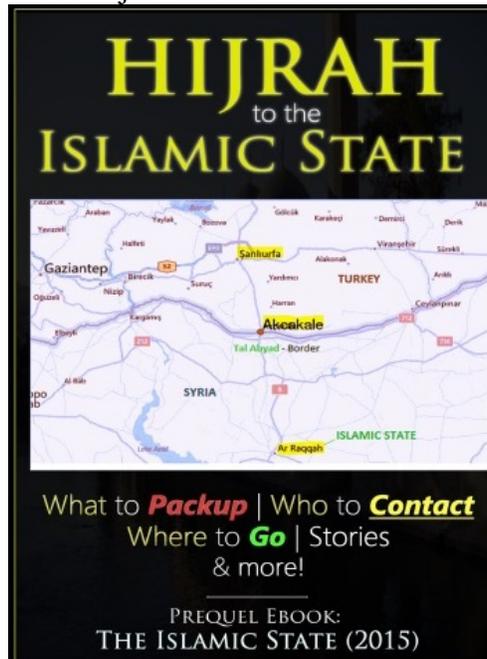
She was also quickly engaged in friendly banter with some of the women within pro-IS networks, including joking with one user about their respective mothers: “MINE TOOO. Like chill mama.” The account holder’s degree of familiarity with Twitter IS networks and their members suggested she may have had an earlier account connected to one of these networks. If so, this earlier account was either removed or deliberately not linked to the new Twitter account (as noted earlier, it is a common practice for suspended IS Twitter users to announce their return to network members when launching new accounts and/or to make themselves more readily identifiable as former members by using variants of their previous user name). If this was, however, a brand new account, then the owner would likely have made conscious efforts to cultivate ‘friends’ in the IS network. Given the paucity of tweets from this account, such ‘courting’ would have had to be done through direct messaging.

Sign 3: suspicious tweet contents

Of the 37 tweets collected, the content of four posts raised significant concerns about the potential for this user to represent a hijrah risk. We will explore two here and the other two in subsequent sub-sections. The first post appeared on January 23rd: “Questions about dawlah and travelling without muhram. DM me plz. May Allah swt reward you.” Three elements of this post stand out. First, dawlah is the Arabic word for country or state and is often used in IS communications to refer to the Islamic State, and particularly to the territory it presently holds. Second, traveling without mahram (muhram) refers to the Islamic practice of having women travel only with guardians. One of the central debates surrounding the practice of hijrah is whether it is acceptable for women, who often cannot let their families know they are leaving for fear of being turned into authorities, to travel alone to the Syrian border. Most IS facilitators and/or propagandists will recommend a woman travel with a mahram or simply avoid

commenting on the matter altogether. For example, the author of the IS produced e-book, *Hijrah to the Islamic State*, states categorically that he will “not get into arguments with anyone about whether it is allowed for sisters to make hijra without mahram (you can advise me privately, no problem, but don’t expect an answer” (unknown 2015). Third, the account holder requests that anyone willing to answer her questions should privately message her. The use of direct messaging and/or secure chat applications (apps) for relaying information regarding making hijrah is an established practice within IS circles, designed to limit the chances of individual migrants being caught.

Pic 3. Hijrah advice from the IS

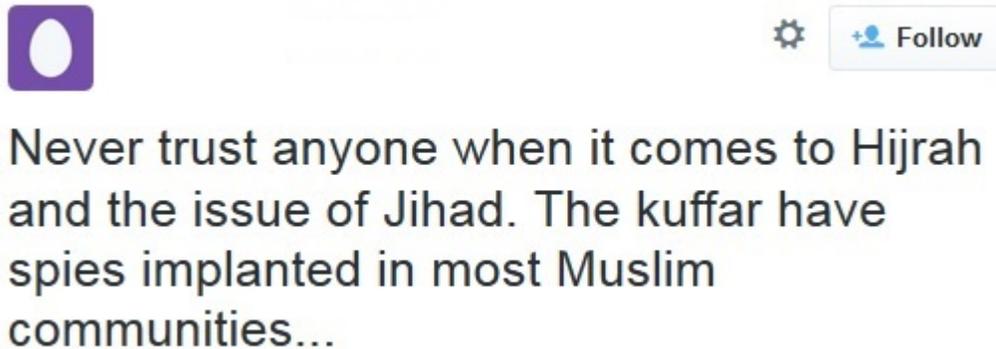


A subsequent post contributed to an overall impression that this person was showing an inordinate interest in the subject of hijrah. On January 27, 2015, she posts, “questions on sham”. Bilad al-Sham is Arabic for the ‘the country of Syria.’ Within IS circles, the only Muslim nation recognized is the universal community of believers, whose territory is the Islamic State. Thus Syria is referred to simply as Sham. In essence, then, the account holder signaled to those

following her posts – including a number of Western foreign fighters and migrant females – her interest in Syria, but did so in a cleverly vague, ambiguous way that is not directly incriminating.

Sign 4: disappearing content/accounts

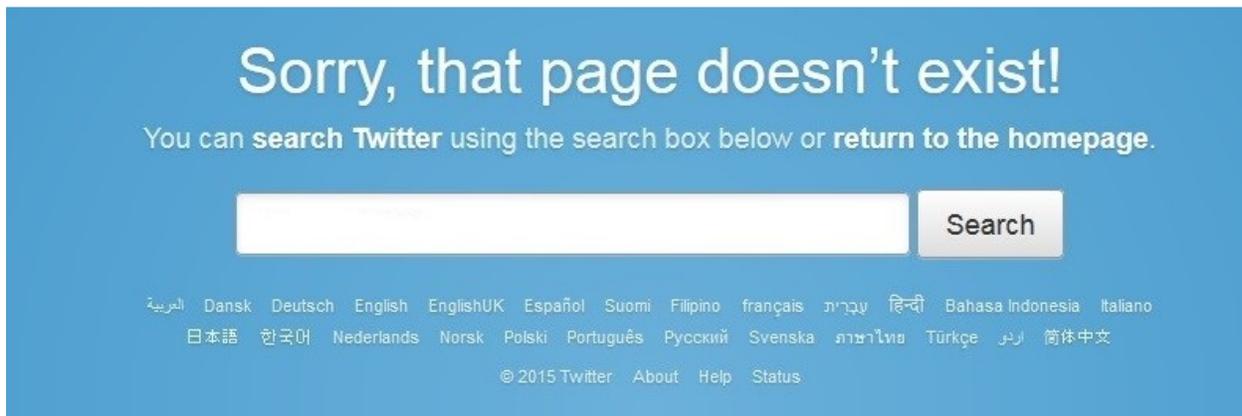
Pic 4. Tweeted hijrah advice (name removed)



In following this user’s activities it was noted that at least one post containing suspicious content was deleted. While watching this account one of the researchers noted the following post in notes collected about its activity: “Aslamualaikum wa rahmatullahi wa barakatu, ya akhwa, I have questions bout hijrah. Can sum1 DM me??” However, when tweets were collected the next morning for all accounts being followed the tweet was not found. The decision to take a note concerning this tweet proved to be fortunate, because it appears that sometime before the tweets were collected on January 31st, the account had been temporarily deactivated. When it reappeared in early February – the account was seen to have been reactivated on February 4th by one of the researchers – the post concerning hijrah was gone, having been deleted by the account owner. Considering that advice on IS sites is full of warnings concerning the dangers of revealing one’s intentions to embark on hijrah, there were two possible interpretations for this post. The first is that a naive individual tweeted it, then either thought better of the post or was advised by someone on her followers’ list to remove it. The second explanation is that the

individual was fishing for someone or some others to come forward with information and, not being sincere about migration, was unconcerned about potential risk of exposure until cautioned by someone else to be careful about posting her presumed intentions. Both explanations occurred to the research team; however, without concrete proof that the account belonged to a sock puppet, we proceeded on the assumption that it was a legitimate account.

Pic 5: Account gone (name removed)



Sign 5: asks known IS recruiter to DM her

On January 27, 2015, the account holder tweeted the following to one of the accounts, ““Uhkti please DM me.” The recipient of this tweet was a British migrant and notorious IS recruiter married to a British foreign fighter in Syria. The recruiter has attracted significant media attention for playing an active role in recruiting young women to Syria (Awford 2014). Hers is one of the three accounts identified in the IS book on hijrah as an appropriate contact for women with questions about migrating. On the 28th, the account holder posted this cryptic tweet: “Blessings in the shape of sisters who strengthen your imaan”.

Ruse revealed

Each of the signs above, particularly in combination, suggested the account holder was an individual with a degree of knowledge about IS networks, their members and their recruitment

strategies. What we did not know was the source of that knowledge and whether we were tracking a legitimate network member who had been exposed to IS propaganda and recruitment materials or someone seeking to penetrate that network in order to gather information on its workings. As a result, we also had to grapple with both methodological and ethical concerns: Should we continue following this account or delete it from our dataset? And, more importantly, if this account holder *was* legitimately a teenager seeking to migrate to Syria, did we have a responsibility to report the account to authorities? And, should we do so even if we did not have conclusive proof as to identity and the possibility remained that we were dealing with a sock puppet?

The answer as to the account holder's identity and intentions was subsequently revealed in March 2015. One of the researchers was comparing notes with a colleague doing similar work with males who migrate overseas when topic arose of the mysterious account. The colleague identified the account as belonging to a reporter for a major national newspaper, who had been conducting an 'undercover investigation' on the recruitment of young women to Syria. The colleague had flagged the account, and, suspecting it belonged to a particular journalist with whom he had friendly relations, warned this individual they should probably shut down the account before it attracted attention from national security professionals. One of the authors of this paper subsequently approached a reporter on the national news desk of this same media outlet. The journalist denied the account belonged to him, but did not deny that journalists from his organization use such ruses to gather information online.

Concluding thoughts

The influence of social media on the recruitment of females for the Islamic State (IS) has recently become been a staple feature of media reporting across the globe, but there mains a

paucity of research regarding this phenomenon. Identifying the potential for females to become IS recruits is difficult for a number of reasons, not least of which is the possibility of casting suspicion upon devout followers. Positively identifying such individuals is also a challenge due to measures taken to conceal their identities, their intentions and their travel plans as per IS instructions. Further, potential migrants are aided and supported by individuals who provide them with all the details and means for travel. Their accounts are often deleted or suspended due to suspicious activity, making tracking difficult if the account owner does not resume activity under a new account. The difficulties associated with conducting research into such individuals online are further compounded by another factor: the possibility of deliberate deceit.

Throughout the preceding pages we drew on the medium of a case study to show how individuals with access to IS propaganda materials – blogs, e-books and other sources – can use information gleaned from those sources to successfully pose as fictional individuals interested in exploring migration to Syria. Such ruses may not only fool individuals within terrorist networks into revealing confidential information about a group and its activities, but may also trick researchers without the means to verify online identities. Without adequate means of verifying the identities of the individuals within our samples, researchers who focus on participation in online radical milieus necessarily run the risk of collecting and analyzing data that should otherwise be excluded in order to avoid drawing conclusions based on false information.

This paper has attempted to provide insight into the sock puppet problem that can confound terrorism research. It also raises an important consideration: to the extent that online social platforms are used by the IS and other groups for propaganda and recruitment purposes (Klausen 2015; Hoyle et al. 2015), further research – particularly into forms of sock detection and avoidance – is necessary for the continuing development and growth of research in this field.

References

- Al-Tabaa, E. 2013. 'Targeting a Female Audience: American Muslim Women's Perceptions of al-Qaida Propaganda.' *Journal of Strategic Security* 6(3): 10-21.
- Awford, J. 2014. 'British rock musician turned ISIS extremist is luring teenage girls to Syria through Twitter with the promise of an 'awesome life' as a jihadi bride.' Daily Mail (UK), online. December 14, 2014. Available at:
<http://www.dailymail.co.uk/news/article-2881667/British-rock-musician-turned-ISIS-extremist-luring-teenage-girls-Syria-Twitter-promise-awesome-life-jihadi-bride.html>
- Bilge L., Strufe T., Balzarotti D., and Kirda E. 2009. 'All Your Contacts Are Belong to Us: Automated Identity Theft Attacks On Social Networks.' *Proceedings of the 18th International Conference on World Wide Web*. ACM: New York. Pp. 551-560.
- Bloom, M. 2011. *Bombshell: Women and Terrorism*. Philadelphia, PA: University of Pennsylvania Press.
- Boshmaf Y., Muslukhov I., Beznosov K., and Ripeanu, M. 2011. 'The Socialbot Network: When Bots Socialize for Fame and Money.' *Proceedings of the 27th Annual Computer Security Applications Conference*. ASAC: New York. Pp. 93-102.
- Bu, Z., Xia, Z and Wang, J. 2013. 'A sock puppet detection algorithm on virtual spaces.' *Knowledge-Based Systems*, 37: 366-377.
- Cragin, R. and Daly, S. 2009. *Women as Terrorists: Mothers, Recruiters, Martyrs*. Oxford, Eng.: Praeger Intl.
- Cunningham, K. 2007. 'Countering Female Terrorism.' *Studies in Conflict & Terrorism*, 30:113-129.
- Dean, S. 2014. 'Parents of a young woman, 21, who sneaked off to Syria to marry a jihadi playboy claim she has been 'brainwashed.' *Daily Mail*, online. December 28, 2014. Available at:
<http://www.dailymail.co.uk/news/article-2889286/Parents-young-woman-21-sneaked-Syria-marry-jihadi-Islamic-State-playboy-claim-brainwashed.html>
- Elovici, Y., Fire, M., Herzberg, A and Shulman, H. 2014. 'Ethical Considerations when Employing Fake Identities in Online Social Networks for Research.' *Science and Engineering Ethics*, 20: 1027-1043.

- Hamblin, A. 2014. 'Jihad bride spouts hate on social Media.' *Melbourne Herald-Sun* online. December 28, 2014. Available at:
<http://www.heraldsun.com.au/news/victoria/jihad-bride-spouts-hate-on-social-media/story-fni0fit3-1227168724143>
- Huey, L., Nhan, J., and Broll, R. 2013. "'Uppity Civilians' and 'Cyber Vigilantes': The Role of the General Public in Policing Cyber Crime." *Criminology and Criminal Justice*, 13(1): 81-97.
- Hoyle, C., Bradford, A., and Frenett, R. 2015. Becoming Mulan? Female Western Migrants to ISIS. Report of the Institute for Strategic Dialogue. Available online at:
http://www.strategicdialogue.org/ISDJ2969_Becoming_Mulan_01.15_WEB.PDF
- Klausen, J. 2015. 'Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq.' *Studies in Conflict & Terrorism*, 38:1–22.
- Lahoud, N. 2014. 'The Neglected Sex: The Jihadis' Exclusion of Women from Jihad.' *Terrorism and Political Violence*, 26:780–802.
- Stern, J. 2012. 'A Radical Idea.' Hoover Digest, 2012(1). Available online at:
<http://www.hoover.org/research/radical-idea>
- TRAC (Terrorism Research and Analysis Consortium). 2014. 'From Canada to the Islamic State: A Canadian Woman on the Frontlines With ISIS.' Available at:
<http://www.trackingterrorism.org/article/canada-islamic-state-canadian-woman-frontlines-isis/new-trend-canadian-female-recruitment-is>
- Zheng, X., Lai, Y., Chow, K., Hui, L. and Yiu, S. 2011. 'Detection of Sockpuppets in Online Discussion Forums.' Hong Kong University CS Tech Report. TR-2011-03. Available at:
www.cs.hku.hk/research/techreps/document/TR-2011-03.pdf