The Use of Social Engineering Techniques in Online Radicalisation

Sumaia Sabouni, Andrea Cullen, Lorna Armitage
University of Bradford

ABSTRACT
The use of online forums and social media sites by extremists for recruiting and radicalising individuals has been covered extensively by researchers. Meanwhile, the social engineering techniques utilised by these extremists to lure marginalised individuals into radicalisation has been neglected. In this article, the social engineering aspects of online radicalisation will be explored.

Specifically, the five Principles of Persuasion in Social Engineering (PPSE) will be mapped onto the online radicalisation methods employed by extremists online. Analysing these tactics will aid in gaining a deeper understanding of the process of indoctrination and of the psychology of both the attacker and the target of such attacks. This understanding has enabled the development of a preliminary radicalisation framework based on the social traits of a target that may be exploited during an attack.

INTRODUCTION
Due to the increased use of the internet, the process of radicalisation has witnessed a noticeable shift from spreading propaganda and ideologies through physical institutions, to using internet forums and social media sites [1]. This strategic shift has granted extremists a perceived sense of anonymity [2], allowed them access to an increase audience size, and facilitated the act of like-minded individuals exchanging radical thoughts by utilizing the interactive features available in online platforms [3]. The use of numerous online platforms by extremists for recruitment and radicalisation and the creation of online detection and prevention methods have been covered in many studies [4], [5], [6]. What the research horizon is currently lacking is the in-depth analysis of the social engineering techniques harnessed by online extremists to radicalise individuals and how certain online medium features have facilitated this. This work includes a review of current literature and the development of a preliminary model. It starts with a brief overview of social engineering, followed by the listing of the Principles of Persuasion in Social Engineering (PPSE). A more detailed account of these principles will then be presented, along with the mapping of these persuasion tactics to the techniques used online by extremists.

SOCIAL ENGINEERING OVERVIEW
This report does not narrow the science of social engineering down to the context of information security; the cultural and psychological stratagems used by hackers to influence individuals to assist them in the unlawful access of computer systems and networks [7]. But rather, the science of social engineering referred to in this

report is the general term of manoeuvring individuals to performs acts that may or may not be in their best interest [8]. It is used in all human interactions, from children persuading their parents to yield to their demands, to politicians convincing their audience to vote for them. Social engineering attacks rely on human error and social psychology by exploiting behavioural and psychological weaknesses [9]. Such attacks are typically comprised of four major steps; "information gathering, relationship development, exploitation, and execution" [10].

There are many social engineering principles used to influence and manipulate individuals. Over the years, researchers identified several techniques of influence and persuasion, the problem with these principles was that they were discipline-bound and did not have clear common factors. In a recent paper, five independent principles were derived that effectively integrate these numerous principles, named the Principles of Persuasion in Social Engineering (PPSE) [11]. These principles are: 1. authority, 2. social proof, 3. liking, 4. commitment, reciprocation and consistency, 5. distraction.

MAPPING SOCIAL ENGINEERING TACTICS TO ONLINE RADICALISATION TECHNIQUES

When the aim of an extremist is to radicalise individuals and recruit members, a strong element of influence and persuasion is required to convince the target to make this drastic move. When applied, these tactics increase the likelihood of a target's susceptibility to the attacker's request. In the following sections, these principles of persuasion will be mapped to the corresponding documented behaviours performed by radicals online.

Authority

Authority plays a vital role in the acceptance of information. Information gained from an accredited figure of authority holds greater value than that from one of no authority. The reason for this is that humans are conditioned to respond to authoritative personalities without questioning their authority [9]. Figures of authority in certain disciplines gain this authority through a high level of knowledge and acumen in their field [12].

Many studies have been conducted on the impact of the internet on authority, the role of religious authority and whether it affirms or threatens traditional, offline authority. Early research argued that the internet would pose a threat to religion and would result in "proliferation of misinformation and disinformation'' and would lead to the ''loss of control over religious materials'' [13]. However, a more recent study on Christian blogs suggested that online religious authority may more often endorse traditional authority [14]. Regarding Islamic radicalisation, it has been reported that during the process of indoctrination of an individual, a religious authority that poses as a "spiritual sanctioner" is present, to smooth the process and increase the power of influence on the individual [15]. This view was confirmed in a recent report on the approaches used in Islamic State recruitment, where author Charlie Winter suggests that the recruitment of an individual into a terrorist organisation is not complete without the existence of an enlister that acts as the "provider of logistical information and humaniser of risk" [16]. Consequently,

it seems that the existence of such an authoritative figure may strongly increase the possibility of the target accepting the transition to extremism.
Whether online extremist authority figures affirm or threaten traditional authority is a debatable issue. These online religious authorities that facilitate indoctrination believe themselves to be teaching the conservative and authentic interpretation of Islam, whereas they view more moderate authorities as teaching a diluted version of Islam [17]. Therefore, it may be concluded that online religious authority used in Islamic radicalisation affirms extremist interpretations of Islam, and threatens more moderate interpretations of it.

Conformity or Social Proof

Conformity is the psychological phenomenon of viewing a behaviour as acceptable if people in the group perform this behaviour. There are several implications of this principle. The first obvious implication is that once an individual begins interacting with extremists through online platforms, a gradual normalisation of the extremists' radical ideologies and beliefs will occur [18].

Secondly, in addition to the normalisation of extremist beliefs, opinions are amplified due to the concepts of homophily and group polarisation; which are the acts of like-minded individuals seeking each other out and exchanging similar opinions, resulting in the mutual reinforcement of views and attitudes [18].

Thirdly, a problem with this principle lies in the situations where an individual is faced with unfamiliar situations, here their first instinct is to mirror the behaviour of those they believe are more enlightened than them. In the context of religious extremism, Choudhury [19] suggests that those that are drawn to extremism have poor religious knowledge and often do so as a result of an identity crisis [20]. The MI5 intelligence agency confirmed this theory in their findings of religious naivety as being a key vulnerability that would make a subject more likely to be affected by extremist ideologies [21]. Hence, if a subject is relatively naïve to religion, this may result in the subject copying surrounding extremists while justifying all violent acts due to his belief that these extremists lead the religious pathway. Examples of individuals that did not originate from strong religious backgrounds but found religion shortly before the time of indoctrination are the wave of Somali-Americans that left America in 2008 to join Al-Shabaab extremist organisation in Somalia [4]. Other examples include the Bastille Day truck attacker Mohamed Lahouaiej-Bouhlel [22] and Omar Mateen, the Orlando nightclub shooter [23], both of which were described by acquaintances as not being particularly religious.

Finally, the criminology phenomenon known as "responsibility diffusion" dictates that an individual may feel less responsible for their actions if they are acting in a group [9]. This means that targets of online radicalisation attempts are led to believe that they are not solely accountable for any actions that may choose to perform within the group. This may help mitigate the risk the target feels towards joining and aiding a group in spreading its propaganda.

Liking

The phenomenon of liking and being liked by another human being increases the likelihood of approving their requests and following their orders. Liking is also the first step towards building trust and confidence between two individuals. Moreover, this desire to create and maintain positive social bonds with other human beings is extremely critical as was demonstrated in a study that concluded that the threat of rejection causes neural reactions similar to those caused by physical pain [24].

Online extremists utilise this phenomenon by allowing socially deprived individuals to become part of their strongly tied community [3]. Marginalisation and the desperate need to belong have been identified by many researchers as being a primary trigger for online radicalisation [18], [25], [3]. This acceptance of a marginalised individual into a community may satisfy their fundamental need for belonging and contribute greatly to the target liking the attackers. Unlike charm, liking is a practiced skill that cannot be faked [8]. The attacker must have genuine feelings of admiration towards the target. This may strongly be the case in online extremism, where an individual must be approved and trusted to join the organisation and gain access to sensitive information.

In another use of this phenomenon, the Federal Bureau of Investigation (FBI) claims that most extremists are recruited through their friends that have confirmed ties leading to the extremist group [26]. In this theory, the targets are not necessarily socially-deprived due to them having social relationships with individuals prior to their indoctrination, but the liking of these individuals that have ties to extremist groups facilitates their radicalisation. Nevertheless, the main weakness with this theory lies in the fact that many cases of targeted attacks and the grooming of individuals has also been reported by researchers [27], [28], [29]. Therefore, it may be concluded that the authoritative figure that facilitates the indoctrination of an individual as mentioned above, may be socially linked to the individual prior to the recruitment process, or may target the individual in an attempt to 'groom' them for radicalisation [16].

Commitment, Reciprocation and Consistency

Commitment, reciprocation and consistency are important principles in influencing human action. Commitment is used by social engineers to pressure targets at hand to agree to a situation that they may or may not have agreed to with the absence of this influence [12]. Once a commitment is made by an individual, it is a natural process for that individual to attempt to remain consistent with the decision made. Accordingly, it is probable that an individual that agrees to become a part of an organisation will attempt to make his actions uniform with this decision.

Reciprocation on the other hand is the mutual exchange of an act with an act of like-value. Moreover, if this act were an act of kindness, the recipient of the act may feel the duty to repay it with a similar behaviour. By performing warm acts, as insignificant as they may seem, the receiver is immediately put at a disadvantage [30]. On the question of online radicalisation, allowing a disaffected, socially-deprived individual to join an extremist community contributes to filling the urgent need to belong that the individual had failed to achieve with their physical

surroundings. Thus, this action may carry strong sentimental value for the target and may be interpreted as an act of kindness that must be reciprocated.
This reciprocation may then take varying forms, ranging from spreading the extremist groups' ideology and seeking out new recruits, to the most severe form being the planning and execution of an act of violence. The individual's conscience decision to join the extremist community and adapt their ideology is a substantial commitment, various forms of reciprocation that follow afterwards may be the individuals attempts to demonstrate consistency.
The consistency referred to in previous literature is the consistency of the target of the social engineering attack after making a commitment to the attacker, as is explained above. However, seeing as this paper is focussed on extremists' online presence, the consistency of the attacker is also an important asset that may increase the chances of the attack succeeding. The consistency of the attacker may be achieved through regular online posts and updates that contribute greatly to maintaining the message being delivered and establishing the reputation of the attacker. With the current size of data being posted online daily, this consistency is essential for any online profile to stay relevant. This frequency of updates is a visible feature seen in online platforms used by prominent Islamic extremist groups and helps the groups form their reputations and maintain recognition [3].

Distraction

Distraction is accomplished by creating strong emotional responses that intensify the emotional state of the individual. This can be achieved by focussing the target's attention on one thing to cause them to overlook another; this focus may be upon something the target is in desperate need of, or something that is scarce, or has been censored or restricted [11]. If the distraction is strong enough, it may cause the distortion of logical facts the target once acknowledged and may even cause the target to alter their entire belief system and moral standards [8], [16].

One of the methods in which radicals may achieve this distraction is through their frequent posts on online platforms. The social media platform, YouTube, is the most common platform for spreading radical ideas [31]. This is most likely due to the graphical content exhibited in many radical videos, and the impact of the visualisation of such content on the emotional state of an individual. Examples of online posts by Islamic extremists that accomplish this distraction are news about conflict-driven areas, reports about discriminatory attacks against Muslims and stories of the groups' victories [3]. Such content may evoke a wide range of emotions, such as the feeling of moral duty and obligation to defending one's religion; obligation was identified as a key influence tactic [8]. Distraction could also be exhibited by consuming the target with the concept of the Muslim community being a "disenfranchised youth" that belongs to an out-group [25], and emphasising the concept of not belonging to the host society [31], causing an identity crisis within the individual. Consequently, these distractions may possess the power to manipulate the individual into joining a radical group while overlooking their unfounded ideology.
From the above, it was concluded that each of the Principles of Persuasion in Social Engineering (PPSE) may be mapped to a prominent social trait in the target exploited by the principle. Figure 1. depicts a preliminary model of the process of radicalisation based on this mapping. The authority tactic was found to link with the social trait of compliance, seeing as the more compliant an individual is, the more receptive the individual may be to self-proclaimed figures of authority. From

the reviewed literature [19], [20], social proof/conformity was found to be associated mainly with the naivety of a target in unfamiliar situations. Additionally,

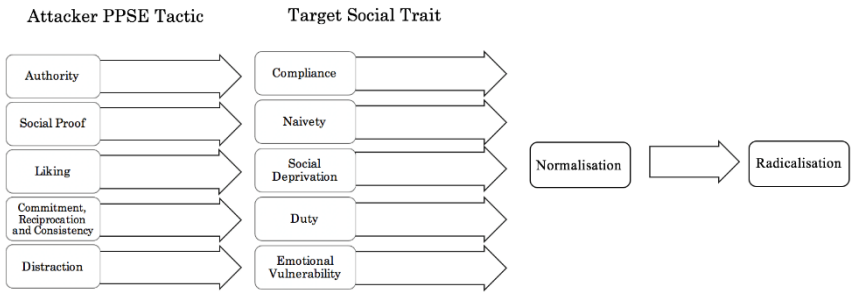

Figure 1. Preliminary radicalisation framework based on the PPSE

targets were found to be more susceptible to the phenomenon of liking when they suffered social deprivation and marginalisation within their surrounding communities [18], [25], [3].
Also, commitment, reciprocation and consistency may be strongly connected to the varying types of duty an individual experiences (moral, religious, civic, etc.). Finally, distraction is created by forming an intense emotional response within the target, and therefore, relies heavily on the target's emotional vulnerability.
When the principles listed are implemented by an attacker, a gradual normalisation of extremist views may occur that could eventually lead to the radicalisation of the individual. The aim of this model is to help identify more specific and targeted intervention strategies by exploring the psychology of the targets of radicalisation and further understanding the motivation of the attackers. This proposed model will require thorough testing across varied radicalisation environments to inspect its accuracy and help develop a generalised radicalisation process.

CONCLUSIONS AND FUTURE WORK

The reviewed literature found that most researchers had widely assessed aspects of online radicalisation in isolation of the principles of social engineering that underpin any human interaction. On investigating the association between the Principles of Persuasion in Social Engineering (PPSE) and online radicalisation, strong elements of influence are exhibited in the behaviours of extremists online.

This research has found that extremists exploit targets' personality traits and emotions by utilising persuasion methods to increase the targets receptiveness to the attack. One of the most prominent features in the targets of online radicalisation attempts, is the sense of alienation from the surrounding society [3]. Extremists' tactics of satisfying these individuals' fundamental need for belonging through offering them positions within their group can be mapped directly onto the persuasion principle of liking. Other phenomena that aid extremists in indoctrinating individuals include group polarisation [18] and responsibility diffusion [9], both of which overlap with the persuasion principle of conformity or social proof.

Whether the targets of these attempts to recruit extremists are mainly blameless victims in the attack, or if they are dangerous individuals that consciously decide to acquire ill-founded ideologies is a debatable topic. However, analysing the social engineering principles adopted by radicals online, may result in greater insight into the psychology of both the attackers and the targets as well as a deeper understanding of the online process itself. This understanding is crucial to pave the way for a more rounded prevention solution, that focuses on treating the target's weaknesses and vulnerabilities to empower them to resist such attacks whilst raising awareness of the price of social deprivation within communities. Ultimately it looks at creating a framework to indicate where limited resources should be focused for developing much earlier interventions in the radicalisation process and deriving countermeasures against it. The framework introduced may also aid in the simplification of the complex phenomenon of radicalisation to gradually help the development of a generalised radicalisation process that may be applicable across several radicalisation environments.

Furthermore, as the literature presented here focuses largely on the indoctrination of individuals into radical Islam, further research would be especially useful in at least two areas: the first being the application of the preliminary model presented in Figure 1 regarding other forms of extremisms, e.g. far right extremism; the second is the need to highlight which social engineering principles apply specifically to lone wolf terrorism, seeing as such terrorists act in support of a group without the direct reinforcement or instructions/grooming from such groups [27].

REFERENCES

[1] Scanlon, J. R. and Gerber, M. S. (2014) 'Automatic detection of cyber-recruitment by violent extremists', Security Informatics, 3(5), pp. 1–10. doi: 10.1186/s13388-014-0005-5.

[2] Torok, R. (2013) 'Developing an explanatory model for the process of online radicalisation and terrorism', Security Informatics, 2(6), pp. 1–10. doi: 10.1186/2190-8532-2-6.

[3] Neo, L. S., Dillon, L., Shi, P., Tan, J., Wang, Y. and Gomes, D. (2016) 'Understanding the Psychology of Persuasive Violent Extremist Online Platforms', in Combating Violent Extremism and Radicalization in the Digital Era, pp. 1–15.

[4] Weine, S., Horgan, J., Robertson, C., Loue, S., Mohamed, A. and Noor, S. (2009) 'Community and family approaches to combating the radicalization and recruitment of Somali-American youth and young adults: A psychosocial perspective', Dynamics of Asymmetric Conflict, 2(3), pp. 181–200. doi: 10.1080/17467581003586897.

[5] Argomaniz, J. (2014) 'European Union responses to terrorist use of the Internet', Cooperation and Conflict. SAGE Publications, 50(2), pp. 250 –268. doi: 10.1177/0010836714545690.

[6] Kukhianidze, L. (2016) 'Criminological Analysis of Terrorism', European Scientific Journal, ESJ, 12(29).

[7] Abraham, S. and Chengalur-Smith, I. (2010) 'An overview of social engineering malware: Trends, tactics, and implications', Technology in Society, 32(3), pp. 183–196. doi: 10.1016/j.techsoc.2010.07.001.

[8] Hadnagy, C. (2010) Social Engineering: The Art of Human Hacking, The Art of Human Hacking. John Wiley & Sons.

[9] Luo, X. (Robert), Brody, R., Seazzu, A. and Burd, S. (2011) 'Social Engineering: The Neglected Human Factor for Information Security Management', Information Resources Management Journal, 24(3), pp. 1–8. doi: 10.4018/irmj.2011070101.

[10] Adewole, A. O. and Durosinmi, A. E. (2015) 'Social Engineering Threats and Applicable Countermeasures', African Journal of Computing & ICT, 8(2). Available at: www.ajocict.net (Accessed: 24 November 2016).

[11] Ferreira, A. and Lenzini, G. (2015) 'An analysis of social engineering principles in effective phishing', in 2015 Workshop on Socio-Technical Aspects in Security and Trust. IEEE, pp. 9–16. doi: 10.1109/STAST.2015.10.

[12] Cialdini, R. (1984) Influence: The Psychology of Persuasion. HarperCollins.
[13] Dawson, L. (2000) 'Researching religion in cyberspace: Issues and strategies', in Hadden, J. and Cowan, D. (eds) Religion on the internet: Research prospects and promises. New York: JAI Press, pp. 25–54.

[14] Campbell, H. A. (2010) 'Religious Authority and the Blogosphere', Journal of Computer-Mediated Communication, 15(2), pp. 251–276. doi: 10.1111/j.1083-6101.2010.01519.x.

[15] Aly, A. and Striegher, J. (2012) 'Examining the Role of Religion in Radicalization to Violent Islamist Extremism', Studies in Conflict & Terrorism, 35(12), pp. 849–862. doi: 10.1080/1057610X.2012.720243.

[16] Winter, C (2016) An integrated approach to Islamic State recruitment. The Australian Strategic Policy Institute.

[17] Gartenstein-Ross, D. and Grossman, L. (2009) Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process. Washington, D.C.

[18] Torok, R. (2011) 'The online institution: Psychiatric power as an explanatory model for the normalisation of radicalisation and terrorism', Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011, pp. 78–85. doi: 10.1109/EISIC.2011.43.

[19] Choudhury, T. (2007). The role of Muslim identity politics in radicalisation: A study in pro- gress. London, UK: Department for Communities and Local Government.

[20] Bhui, K. and Ibrahim, Y. (2013) 'Marketing the "radical": symbolic communication and persuasive technologies in jihadist websites.', Transcultural psychiatry, 50(2), pp. 216–34. doi: 10.1177/1363461513479329.

[21] Christmann, K. (2012) Preventing religious radicalisation and violent extremism: A systematic review of the research evidence., Youth Justice Board. doi: 10.13140/2.1.4641.6169.

[22] Beaumont, P. and Fischer, S. (2016) 'Mohamed Lahouaiej-Bouhlel: who was the Bastille Day truck attacker?', The Guardian. Available at: https://www.theguardian.com/world/2016/jul/15/bastille-day-truck-driver-was-known-to-police-reports-say.

[23] Sullivan, K. and Wan, W. (2016) 'Shooter., Troubled. Quiet. Macho. Angry. The volatile life of the Orlando shooter.',

[24] Lavigne, G. L., Vallerand, R. J. and Crevier-Braud, L. (2011) 'The fundamental need to belong: On the distinction between growth and deficit-reduction orientations.', Personality and Social Psychology Bulletin, 37(9), pp. 1185–1201. doi: 10.1177/0146167211405995.

[25] Lynch, O. (2013) 'British Muslim youth: radicalisation, terrorism and the construction of the "other"', Critical Studies on Terrorism, 6(2), pp. 241–261. doi: 10.1080/17539153.2013.788863.

[26] FBI (2006) The Radicalization Process: From Conversion to Jihad.

[27] IEP (2015) Global Terrorism Index: Measuring and Understanding the Impact of Terrorism, IEP Report 36. doi: 10.1162/ISEC_a_00023.

[28] CSCB (2016) Safeguarding children and young people from radicalisation and extremism: guidance for the children's workforce Safeguarding from radicalisation and extremism.

[29] Deen, A. (2016) I used to be an Islamic extremist. This is the truth about how you can prevent further terror attacks | The Independent. Available at: http://www.independent.co.uk/voices/i-used-to-be-an-islamic-extremist-this-is-the-truth-about-how-you-can-prevent-further-terror-attacks-a7145816.html#commentsDiv (Accessed: 24 November 2016).

[30] Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M. and Hartel, P. H. (2015) 'The persuasion and security awareness experiment: reducing the success of social engineering attacks', Journal of Experimental Criminology, 11(1), pp. 97–115. doi: 10.1007/s11292-014-9222-7.

[31] Haider, H. (2015) Radicalisation of diaspora communities (GSDRC Helpdesk Research Report 1187). Birmingham.