Radicalization, the Internet and Cybersecurity: Opportunities and Challenges for HCI

Joanne Hinds(✉) and Adam Joinson

Information, Decisions and Operations, School of Management,
University of Bath, Bath, UK
{J.Hinds,A.Joinson}@bath.ac.uk

Abstract. The idea that the internet may enable an individual to become radicalized has been of increasing concern over the last two decades. Indeed, the internet provides individuals with an opportunity to access vast amounts of information and to connect to new people and new groups. Together, these prospects may create a compelling argument that radicalization via the internet is plausible. So, is this really the case? Can viewing 'radicalizing' material and interacting with others online actually cause someone to subsequently commit violent and/or extremist acts? In this article, we discuss the potential role of the internet in radicalization and relate to how cybersecurity and certain HCI 'affordances' may support it. We focus on how the design of systems provides opportunities for extremist messages to spread and gain credence, and how an application of HCI and user-centered understanding of online behavior and cybersecurity might be used to counter extremist messages. By drawing upon existing research that may be used to further understand and address internet radicalization, we discuss some future research directions and associated challenges.

Keywords: Radicalization · Cyber security · Online behavior

1 Introduction

The role of the Internet in radicalization has been the topic of considerable debate since the widespread adoption of the web in the mid to late 1990s. As far back as 1999, David Copeland, a right-wing extremist, detonated nail bombs in London using expertise gained from books downloaded from the internet [1]. Although early discussions e.g. [2] primarily focused on the use of the internet to conduct, co-ordinate or prepare for terrorist acts, more recently much of the discussion has been around propaganda and the use of the internet to mobilize support [3–5]. Not surprisingly, much of the discussion of Internet radicalization has been conducted in the security and terrorism studies field. For instance, in the years 2001–2016, the term 'radicalization' (or 'radicalisation') was used 21 times in the titles of articles in the journal "Security and Conflict Studies", and mentioned in the text of 232 papers. During the same period,

The original version of this chapter was revised: A Funding Disclosure Statement has been inserted. The correction to this chapter is available at https://doi.org/10.1007/978-3-319-58460-7_51

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 481–493, 2017.
DOI: 10.1007/978-3-319-58460-7_33

the term was used zero times in papers in ACM CHI, CSCW, or indeed HCII. However, it is our contention that researchers in human-computer interaction (HCI), and cyber security more generally, have investigated a number of phenomena and topics that we believe are directly relevant to understanding (and addressing) internet radicalization.

The goal of the present paper is to highlight ongoing challenges faced by security researchers in understanding 'internet radicalization', and to suggest where HCI and cybersecurity researchers might fruitfully contribute. We begin by outlining what is meant by the term 'radicalization', before considering the nature of 'online radicalization', and then the potential links between cybersecurity, HCI and radicalization.

1.1 Definition of Radicalization

In general, the term 'radicalization' is a poorly understood concept, with considerable disagreement over not only its definition, but also whether or not it serves a meaningful purpose in understanding politically motivated violence [6]. Whilst there is no universal, agreed-upon definition, radicalization is broadly acknowledged to be a process in which an individual willingly moves towards more extremist views e.g. [7]. Importantly, radicalization is not necessarily negative or a precursor to terrorism, as many people who accept radical ideas do not participate in violent behavior as a result of their beliefs [8]. Further, radical ideas are not necessarily anti-social as radicalism can give rise to positive change (e.g. universal suffrage), and the categorization of an individual or group as 'radical' or 'radicalized' is not a politically neutral activity. More recently, discussions of radicalization have also become entwined with concerns about safeguarding vulnerable young people (e.g. to stop teenage girls traveling to war zones).

Violent radicalization (or violent extremism) is usually argued to be when an individual adopts 'extreme political, social and/or religious ideas and aspirations, and where the attainment of particular goals justifies the use of indiscriminate violence. It is both a mental and emotional process that prepares and motivates an individual to pursue violent behavior.' [8] (p. 38). Many individuals holding radical beliefs and opinions will not commit extremist or violent acts and, conversely, many terrorists are often not deep believers and have limited knowledge of their motivating ideology [9].

There are myriad potential causes for radicalization toward violent extremism (e.g. social inequality, poverty, violation of basic rights; [6]), a detailed description of which is outside the remit of the present paper. Rather, in the following section we briefly summarize the main approaches, before moving to consider how these might relate to work within HCI and cybersecurity.

1.2 Radicalization: Theories and Models

Most theories of radicalization propose a combination of individual and social factors that, in combination, can both push and pull individuals towards violent action [10]. Typically, not one factor is assumed to be sufficient on its own to trigger radicalization, but rather is assumed to operate in conjunction with other factors and vulnerabilities to lead an individual towards violent radical action. Research suggests that there is not a

specific psychological profile or vulnerability that might pre-dispose individuals to violent radicalization [10]. For instance, *relative deprivation*, the notion that a person comes to feel deprived as a result of comparing their situation with others, has been consistently linked with radicalization, e.g. [11–14]. A sense of relative deprivation can drive people to join movements e.g. [15], the intention being that joining a movement will bring about social change and put an end to their grievances [10]. Other 'triggers' for radicalization may be the tendency of (some) people to adopt religious beliefs or join religious groups after experiencing some form of crisis e.g. [16–18].

Whilst a definite, agreed-upon process of radicalization has not been established, a number of models have outlined some proposed stages of radicalization, a summary of which are outlined as follows:

1. **Social/economic deprivation or a personal crisis** – An individual experiences relative deprivation or some form of crisis, which can be personal or group-based [19–22]. The individual views their situation as unfair/unjust.
2. **Resentment and information seeking** – The perception of relative deprivation causes an individual to feel increasing resentment towards others who they perceive as being more fortunate. An individual may seek answers to their situation and in doing so becomes receptive to new ideas and possibly new religious beliefs [22, 23].
3. **Attributing blame and justification of violence** – Individuals blame others for their perceived injustice [19] and socialize with likeminded others, which strengthens these new beliefs [20]. Violence is viewed as a legitimate means to rectify perceived injustices [19, 23].
4. **The violent act** - An individual embraces and fully commits to the group's beliefs and mission [23, 24].

While none of these models directly incorporates the role of the internet in radicalization, it seems plausible that it could be utilized at any stage as a source of information or communications mechanism that could help to develop/reinforce feelings of hardship and justified violence. In the following section, we discuss some of the more specific aspects of the internet (referred to as 'affordances') that may contribute towards an individual's radicalization.

2 Online Radicalization

At a fundamental level, the internet allows rapid access to vast amounts of information as well as the opportunity to connect to others through social networks, fora, messaging systems etc. Each of these mechanisms has an associated set of 'affordances', a term commonly used in HCI to describe how technology functions and thus how it should be used. This idea of objects *affording* certain types of behavior was adopted by human-computer interaction researchers, most notably Norman [25], following the introduction of the term by cognitive psychologist Gibson [26]. Norman argues that affordances are the "perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used" [25]

(p. 9). We would argue that the notion of affordances – while valuable in highlighting the links between design, the user, and action – does not fully represent the ways in which design and behavior interact. Taylor et al. [27] argue that:

> *'Research on the 'social shaping' of technology … suggests that we shape technology as much as we are in turn influenced by the decisions made by designers, or the content it provides … this means that use of the Internet needs to be considered from neither a simple 'technologically deterministic' standpoint (e.g. the Internet causes radicalisation), nor simply as a socially neutral 'tool' (p. 4).*

Gibson [28] describes how affordances can be both perceivable and straightforward (e.g. Facebook allows people to keep in touch with friends) or more hidden/camouflaged (e.g. a person can use Facebook to portray themselves in a more positive light by only posting attractive photographs). It is therefore possible to speculate how similar affordances may apply to online radicalization. For instance, ideologues have become proficient at using social media, online communities etc. to disseminate their radical ideologies, gain support [29, 30] and to provide instruction in terrorist activity. Online magazines such as Dabiq and Inspire along with other internet resources can equip an individual with everything they need to know to commit a terrorist attack, from assembling a bomb to breaching security in an airport [31].

It is indisputable that such resources available online (including via the dark web) provide ample support for violent extremists in terms of attack planning, as well as (potentially) the opportunity to gather information in relative anonymity. However, in this respect the internet is nothing more than a conduit for the provision of information and communications, with little or no influence on the process itself. A RAND report [32] surveyed 15 cases of mostly Islamic terrorist activities, where the internet was implicated in radicalization and actual attacks in the UK. They concluded that while the internet provided more opportunities for radicalization, it did not necessarily increase the speed at which individuals became radicalized, or replace face-to-face contact or kin and peer influence. A more recent study by Gill et al. [33] studied the use of the Internet by 223 convicted terrorists in the UK. They conclude that patterns of use differ according to the requirements of the terrorist (e.g. to gain expertise in explosives, recruit co-conspirators or gain ideological justification), also stating that, "The Internet is largely a facilitative tool that affords greater opportunities for violent radicalization and attack planning". In other words, these findings suggest that certain affordances of the internet can potentially fuel different aspects of radicalization (although it is not possible to decipher exactly how this is achieved). This suggests that technology in itself is not enough to radicalize individuals to take action, but rather that the internet acts as an enabler *once* an individual is radicalized, or when specific hurdles need to be addressed (e.g. how to choose a target, build an improvised explosive device etc.).

Another aspect to consider is that radicalization encompasses a broad spectrum of people with different needs, motives and goals, ranging from lone actors to individuals seeking belonging from group membership. Thus, this is likely to be reflected in different uses and approaches toward using information disseminated online. In the following section, we move to explore some ways in which certain affordances may enable certain types of behavior/transformations in the context of group behavior, echo chambers, offline action and self-presentation online.

2.1 Group Behavior

The internet allows people to communicate rapidly to masses of people online, as well as seek out and develop new relationships with different people and different groups. In doing so the internet may help individuals to develop and maintain an identity through joining an online community, forum, social media group etc. Being part of a group can provide an individual with a sense of belonging [34, 35] and the internet can provide an opportunity for individuals to seek out and connect with likeminded others with whom they may not have the opportunity to meet offline. Classic studies of group behavior have demonstrated that groups have the potential to change behavior – individuals exert less effort as they feel less accountable for their actions e.g. [36], individual attitudes and opinions can become more extreme through group polarization [37], individuals can favor consensus through groupthink [38] and groups can increase a person's inclination to conform, e.g. [39]. Therefore, by extension, can similar effects underpin or play a role in radicalization?

Research on computer-mediated communication demonstrates how some group effects can be exaggerated online. The SIDE model (social identity model of deindividuation effects) for instance, explains how anonymity can enhance people's identification with a group [40, 41], leading to group polarization e.g. [42]. Taken together, the ability to change and strengthen an individual's opinions and behavior, combined with an individual's search for belonging may increase the potential for radicalization online.

2.2 Echo Chambers and Identity Demarginalization

Related to the notion that the internet can foster group polarization is the idea that the internet can fuel echo chambers, where particular opinions can easily start to be recirculated and reinforced, which could have the gradual effect of causing someone to experience a change in mindset. There are numerous design aspects that can serve to fuel this, for instance much of the content an individual is exposed to is a result of content that has been filtered by certain algorithms. For example, social media is a primary news source for over 60% of US internet users [43], which means that most news consumed is filtered by both algorithms and 'friends' [44], and is consumed in the context of others' reactions. As seen in the 2016 US Election, this 'filter bubble' and 'echo chamber' can lead to the rapid spread of false news stories and creation of ghettos of information with little transfer across ideological boundaries [45]. Since radicalization often relies on a sense of injustice and unfairness, an unintentional outcome of the design of online systems may well be that individuals are exposed to increased amounts of material that fuels such grievances. Furthermore, most social media services not only create echo chambers, but also provide validation to content through the positive reactions of others and supportive comments and sharing. Thus, even 'fake' news can gain additional credence by being shared and supported by large numbers of other people. According to principles of social comparison and herding (e.g. [46]) people look to others for guidance on how to act and respond, particularly when

uncertain. If a large number of people are also sharing and supporting radical content, it is likely that for any one individual, such views will be more likely to be adopted.

Simultaneously, a relatively large number of people sharing the same content and opinions serves to demarginalize a previously socially anti-normative set of beliefs or actions. Early work by McKenna and Bargh [47] found that participation in online newsgroups by people with stigmatized identities led to increased self-acceptance, likelihood of 'coming out' to family and friends, and less social isolation. Similar findings emerge from qualitative work on the Stormfront extreme right wing forum [48], with respondents stating that participation helped express an identity that was stigmatized and hidden in face-to-face dealings. There is further evidence that identities expressed online – particularly those publicly affirmed and responded to – later transfer to offline action [49]. It is not that much of a stretch then to predict that the combination of in-group homogeneity, echo chambers, public expression of usually hidden identities or beliefs and supportive comments from others would be enough to encourage increased radicalization.

2.3 Online Action and Offline Acts

Computer-mediated communication has also been found to influence how a group behaves offline. For instance, social media applications (in particular microblogging applications such as Twitter) can be extremely useful for sharing information and reaching large numbers of people when events unfold rapidly and other forms of communication may fail, e.g. [50, 51]. Further, the freedom to publish information publicly enables people to bypass official media censorship and inform a global audience. Subsequently, this surge of online collective information exchange can cause 'mobilizing' effects where groups assemble and combine their efforts offline e.g. [52, 53]. These mobilizing effects typically occur at the onset of major news events, disasters and crises. For instance, during the Arab Spring, a series of political protests and demonstrations that occurred across the Middle East in 2011, many people on the ground in Cairo used Twitter to communicate meeting times, coordinate actions and gather support [54, 55]. We also see similar mobilizing activities in the 'shaming' of individuals via social media [56], where large numbers of people mobilize online to express outrage and condemn an individual judged to have transgressed.

Whilst there is clear evidence for the power of social media to fuel and support social unrest (and hence similar situations that may lead to violent extremist activity), none of these examples provide ample evidence that the people participating were radicalized (e.g. the people participating in the London riots in 2011 were not hailed as 'radicalized'). There has also been heavy criticism over the extent of the effectiveness of social media to actually promote and fuel offline action. For instance, whilst Twitter was used heavily during the London riots, there was little evidence to suggest that Twitter was used to promote illegal activities at the time, rather it served as a tool for spreading information (and misinformation) about subsequent events and showing support for beliefs in others' commentaries [57]. The ability for users to provide cheap and easy support via social media has been referred to as 'slacktivism' [58, 59], where low-risk, low investment actions such as signing a petition or 'liking' a Facebook page

can lead them to feel their contribution is enough [60, 61]. These online activities therefore provide little insight for online radicalization, as those that may appear to hold strong beliefs and even encourage or threaten violent extremism online may have no intention of taking offline action.

2.4 Deception and Self-presentation

In addition to changing how individuals behave when immersed in a group, computer-mediated communication can affect how individuals present themselves and interact with others online. Social contextual cues such as body language, facial expressions, intonation etc. that are visible in face-to-communication are absent, e.g. [62]. This can mean that information can more easily be misinterpreted or individuals may 'fill in the blanks', that is, they make assumptions about information that is unclear or is not communicated explicitly.

The absence of cues can make it easier to lie and deceive others online, especially when communicating with others whom an individual has never met before, e.g. [63, 64]. For instance, extensive research of online dating demonstrates that deception is frequently observed when people exaggerate details of their physical attributes (height, weight, age) in attempt to enhance their attractiveness online, e.g. [65, 66]. The style of deception that is demonstrated in online dating highlights numerous techniques that ideologues could use in radicalization. For instance, ideologues can pose as someone else by using an identity more appealing to the victim in terms of how they appear or what they represent. Private conversations can be used to develop intimacy, which can be extremely persuasive as messages can be personalized and cannot be viewed by others, who may attempt to intervene. These tactics mirror grooming attempts, which have in some cases appeared to have lured young people into joining radical groups, for example the three teenage girls who left the UK for Syria in 2015 after interacting with extremists online [67].

Unlike dating, many of the interactions that occur through these media will continuously occur publicly with (potentially) many others. A number of studies have suggested that the awareness of an audience causes individuals to present themselves more favorably to avoid embarrassment, shame or unfavorable impressions, e.g. [68–70]. Because individuals now have many opportunities to present themselves online (and spend significant amounts of time doing so), some research has suggested that they may alter their identity offline as a result, an effect commonly referred to as 'identity shift' [49]. In a study where participants were instructed to present themselves in an extraverted manner online, Gonzales and Hancock [49] found that participants subsequently began to demonstrate extraverted behavior offline. By extension, these findings may imply that similar shifts in identity may occur for individuals who start to present themselves as dedicated followers of radical groups in any of their online profiles.

The potential for identity shift is not only a factor in terms of how one presents themselves online, but also how their audience responds to and reinforces that identity. Walther's hyperpersonal model [71], for instance explains how the combination of reciprocal interactions and selective self-presentations over time lead to exaggerated

levels of affect and intimacy which in turn can make an individual feel more committed to the identity they have created or developed online. The internet provides many opportunities for others to provide feedback (likes, retweets, comments, etc.) which may prove to be conducive to an individual exploring new aspects of their identity online. Further, feedback from others can serve as cues (referred to as 'warrants' [72]) that can help to verify or increase someone's inclination to believe that an individual is being truthful.

3 HCI Opportunities and Challenges

Throughout this article we have outlined the complex nature of radicalization and how such affordances provided by the design of social media applications, fora etc. may help to foster mechanisms that may, over time cause someone to change their opinion, identity or even conduct violent action offline. However, the lack of real understanding about radicalization, (which is in turn reflected in our lack of ability to truly measure or detect whether it is happening) means that is incredibly difficult to make any specific recommendations for how to address these issues with persuasive design in an online arena. At best, we can speculate how certain affordances may bring about certain types of behavior (e.g. rapid real-time communication on Twitter can provoke offline activity). In this respect, approaches to tackle this could lead toward attempting to counter or diffuse such behavior should it be anticipated or when it occurs.

One particular challenge in addressing these issues is that behavior often evolves from people's use of technology in a way that was unintended or unanticipated from the original design. For example, the design of social media was not expected to increase the spread of misinformation – rather it was hailed as a unique opportunity for a business to 'lose its chains' e.g. [73]. Many of the same processes that enable radicalization online also have socially beneficial outcomes - ranging from the ability of people to seek help and guidance for health problems in a pseudonymous environment to providing important methods for alternative news to spread outside of oppressive regimes. Therefore, this raises the question of what equivalent unintended types of behavior would result from attempts to address radicalization online.

Another consideration is that different groups will likely use the internet in different ways, in order to meet varied motives. It is therefore unlikely that a one-size-fits-all solution could address all the nuances between these different groups. Further, given that not all radical groups are problematic (indeed in many instances radical groups are harmless or even beneficial), there would be a danger in trying to counter certain opinions or behaviors online. Flexible approaches towards design are therefore needed, that consider radicalization as a multivariate problem. In spite of this, we discuss a number of light suggestions that may act as potential steps towards addressing radicalization online. However, because most of these approaches could be applied in both good and bad contexts, we acknowledge the potential pitfalls associated with each one.

First, an obvious, simplistic solution would be to block, or re-direct users from viewing (potentially) radicalizing content. This poses the immediate benefit of preventing them from possibly being influenced by propaganda or other radicalizing material. However, such content may have already been viewed/shared and it is likely

that it could merely be re-posted elsewhere. Likewise, this approach is far too unrealistic and restrictive to apply so broadly across the web as it runs the risk of constraining opportunities for positive influence and interaction.

Second, although individual's generally have control over the content they consume, much of the information they are exposed to is determined by algorithms and the content shared by their contacts [44]. This can create the potential for internet echo chambers to emerge, which (in certain contexts) may create the impression that specific ideological views are shared by a larger proportion of people than is the case, as well as demarginalizing more extreme views. Changes to algorithmic design that aim to steer individuals away from or block suspicious content could attempt to diffuse or hinder the formation of echo chambers. However, this approach also runs the risk of wrongly disrupting beneficial content.

Third, in a similar vein, counter-messaging strategies could be employed in attempt to directly neutralize or diffuse extreme opinions or attempts to influence online. Counter-messaging is an emerging area of research, which has examined how targeted responses to hateful or opinionated online speech can effectively inhibit or end it. For instance, presenting counter-messages *may* be effective, particularly if combined with evidence of social proof (i.e. the number of people sharing/supporting a particular viewpoint). Some strategies for tackling this have already been suggested, for instance, the US based Anti-Defamation League [74] recommend that certain techniques such as responding to the original speaker, using comedy/satire and correcting falsehoods can be useful. At present, there is little evidence that indicates how successful these strategies are, so further research would benefit from attempts to establish effective messaging strategies online.

Fourth, the speculation that individuals can experience an identity shift as a result of their online interactions suggests that particular cues or warrants in social media applications (such as likes, comments, retweets etc.) could be used in attempt to reinforce or influence behavior. In other words, if an individual is suspected to be vulnerable to a potential identity shift, targeted efforts could seek to dissuade potentially radicalizing elements (e.g. not liking or commenting on a post which displays a support of violence) and instead reinforcing more positive behaviors (e.g. retweeting a post about sport). Such approaches would need to be cautious in order to ensure that the right kind of behaviors were reinforced.

Fifth, similar approaches could be used to set behavioral norms in forums. Some existing HCI/cybersecurity research has described how moderators can shape how people behave online by removing, re-directing or rating posts. This can encourage lurkers to contribute [75], set the standard for new users who may not know how to behave when they enter a community [76], discourage bad behavior and manage conflicts (e.g. trolls or flame wars). Certain design aspects such as reputation systems/rewards can also reinforce good/bad behavior, for instance, moderators on Slashdot (a social news website) assign labels and ratings to posts which causes the highest rated comments to appear at the top [77].

It seems likely that online communities could be a place where people experiencing relative deprivation may seek out like minded others for support. Preece [78] describes how designing communities to foster empathy are crucial for empowering people to discuss their problems and provide support to others. It therefore seems that

encouraging and rewarding behavior through skillful moderation, rewards etc. may be an effective way to allow people to obtain the support they need, whilst motivating compliance within online communities. Of course, the potential for this to effectively disrupt radicalization would be dependent on the type of community and the moderators' motives.

Overall, these suggestions provide numerous approaches that may contribute towards tackling radicalization online. Whilst no method is without limitation, further research would benefit from exploring if and how behavior can be shaped in the context of radicalization online.

4 Conclusion

In summary, whilst is seems possible that an individual may become radicalized online, there is little evidence to suggest it actually occurs. Unfortunately, the lack of understanding about what radicalization actually is makes the task of recognizing it with any real accuracy impossible. By extension, it is therefore unrealistic to assume that this problem can be solved entirely by a technological solution. However, by drawing upon prior research from HCI and cybersecurity we have highlighted numerous avenues that may contribute towards designing systems and shaping behavior in ways that attempt to (at least) steer individuals in a more positive direction. Taken together, we hope these ideas may encourage HCI and cybersecurity researchers to think about new approaches towards tackling radicalization online.

Funding Disclosure Statement. This research was funded by the Centre for Research and Evidence on Security Threats (ESRC Award: ES/N009614/1), which is funded in part by the UK security and intelligence agencies. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

References

1. Conway, M.: Terrorism and the internet: new media—new threat? Parliam. Aff. **59**(2), 283–298 (2006)
2. Conway, M.: Terrorist use of the internet and the challenges of governing cyberspace. In: Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, pp. 95–127 (2007)
3. Aly, A., Macdonald, S., Jarvis, L., Chen, T.M.: Introduction to the special issue: terrorist online propaganda and radicalization. Stud. Terror. Confl. 40, 1–9 (2016)
4. Conway, M.: Determining the role of the internet in violent extremism and terrorism: six suggestions for progressing research. Stud. Confl. Terror. **25** (2016)
5. Gendron, A.: The call to jihad: charismatic preachers and the internet. Stud. Confl. Terror. **40** (1), 44–61 (2017)
6. Schmid, A.P.: Radicalisation, de-radicalisation, counter-radicalisation: a conceptual discussion and literature review. ICCT Res. Pap. **97**, 22 (2013)
7. Fraihi, T.: Escalating radicaliastion: the debate within muslim and immigrant communities. In: Jihadi Terrorism and the Radicalization Challenge in Europe. Ashgate, Hampshire (2008)

8. Wilner, A.S., Dubouloz, C.J.: Homegrown terrorism and transformative learning: an interdisciplinary approach to understanding radicalization. Glob. Chang. Peace Secur. **22**(1), 33–51 (2010)
9. Borum, R.: Radicalization into violent extremism I: a review of social science theories. J. Strateg. Secur. **4**(4), 7–36 (2011)
10. Horgan, J.: From profiles to pathways and roots to routes: perspectives from psychology on radicalization into terrorism. Ann. Am. Acad. Polit. Soc. Sci. **618**(1), 80–94 (2008)
11. Runciman, W.G.: Relative deprivation and social justice: study attitudes social inequality in 20th century England (1966)
12. Gurr, T.R.: Why Men Rebel. Routledge, Abingdon (2015)
13. Korpi, W.: Conflict, power and relative deprivation. Am. Polit. Sci. Rev. **68**(04), 1569–1578 (1974)
14. Walker, I., Pettigrew, T.F.: Relative deprivation theory: an overview and conceptual critique. Br. J. Soc. Psychol. **23**(4), 301–310 (1984)
15. Gunning, J.: Social movement theory and the study of terrorism. In: Critical Terrorism Studies: A New Research Agenda, pp. 156–177 (2009)
16. Lofland, J., Skonovd, N.: Conversion motifs. J. Sci. Stud. Relig. **20**, 373–385 (1981)
17. Moscovici, S.: Toward a theory of conversion behavior. Adv. Exp. Soc. Psychol. **13**, 209–239 (1980)
18. Rambo, L.R.: Theories of conversion: understanding and interpreting religious change. Soc. Compass **46**(3), 259–271 (1999)
19. Borum, R.: Understanding the terrorist mindset. FBI Law Enforc. Bull. **72**(7), 7–10 (2003)
20. Moghaddam, F.M.: The staircase to terrorism: a psychological exploration. Am. Psychol. **60**(2), 161 (2005)
21. Sageman, M.: A strategy for fighting international Islamist terrorists. Ann. Am. Acad. Polit. Soc. Sci. **618**(1), 223–231 (2008)
22. Wiktorowicz, Q.: Joining the cause: Al-Muhajiroun and radical Islam. In: Devji, F. (ed.) The Roots of Islamic Radicalism conference, Yale. Landscapes of the Jihad: Militancy, Morality and Modernity. C Hurst & Co Publishers Ltd., London (2004)
23. Silber, M.D., Bhatt, A., Analysts, S.I.: Radicalization in the West: The Homegrown Threat, pp. 1–90. Police Department, New York (2007)
24. Precht, T.: Home grown terrorism and Islamist radicalisation in Europe. From conversion to terrorism (2007)
25. Norman, D.A.: The Psychology of Everyday Things. Basic Books, New York (1988)
26. Gibson, J.J.: The theory of affordances. In: Shaw, R., Bransford, J. (eds.) Perceiving, Acting, and Knowing (1977)
27. Taylor, P.J., Holbrook, D., Joinson, A.: Same kind of different. Criminol. Public Policy **16**(1), 127–133 (2017)
28. Gibson, J.J.: The theory of affordances. In: The Ecological Approach to Visual Perception, pp. 127–143 (1979)
29. Ashour, O.: Online de-radicalization? Countering violent extremist narratives: message, messenger and media strategy. Perspect. Terror. **4**(6) (2011)
30. Chen, T., Jarvis, L., Macdonald, S.: Cyberterrorism. Springer, Heidelberg (2014)
31. Torok, R.: "Make A Bomb In Your Mums Kitchen": Cyber Recruiting and Socialisation of 'White Moors' and Home Grown Jihadists (2010)
32. Von Behr, I.: Radicalisation in the digital era: the use of the Internet in 15 cases of terrorism and extremism (2013)
33. Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., Horgan, J.: Terrorist use of the internet by the numbers. Criminol. Public Policy **16**(1), 99–117 (2017)
34. Tajfel, H.: Social psychology of intergroup relations. Ann. Rev. Psychol. **33**(1), 1–39 (1982)
35. Taylor, D.M., Moghaddam, F.M.: Theories of Intergroup Relations: International Social Psychological Perspectives. Greenwood Publishing Group, Westport (1994)

36. Latane, B., Williams, K., Harkins, S.: Many hands make light the work: the causes and consequences of social loafing. J. Pers. Soc. Psychol. **37**(6), 822 (1979)
37. Myers, D.G., Lamm, H.: The polarizing effect of group discussion: the discovery that discussion tends to enhance the average prediscussion tendency has stimulated new insights about the nature of group influence. Am. Sci. **63**(3), 297–303 (1975)
38. Janis, I.L.: Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes. Houghton Mifflin, Boston (1972)
39. Asch, S.E.: Studies of independence and conformity: I. A minority of one against a unanimous majority. Psychol. Monogr.: Gen. Appl. **70**(9), 1 (1956)
40. Lea, M., Spears, R.: Computer-mediated communication, de-individuation and group decision-making. Int. J. Man Mach. Stud. **34**, 283–301 (1991)
41. Postmes, T., Spears, R., Lea, M.: Breaching or building social boundaries? SIDE-effects of computer-mediated communication. Commun. Res. **25**, 689–715 (1998)
42. Sia, C.L., Tan, B.C., Wei, K.K.: Group polarization and computer-mediated communication: effects of communication cues, social presence, and anonymity. Inf. Syst. Res. **13**(1), 70–90 (2002)
43. Gottfried, J., Shearer, E.: News Use Across Social Media Platforms 2016. Pew Research Centre (2016). http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/. Accessed 10 Feb 2017
44. Bakshy, E., Messing, S., Adamic, L.A.: Exposure to ideologically diverse news and opinion on Facebook. Science **348**(6239), 1130–1132 (2015)
45. Baer, D.: The 'Filter Bubble' Explains Why Trump Won and You Didn't See It Coming (2016). http://nymag.com/scienceofus/2016/11/how-facebook-and-the-filter-bubble-pushed-trump-to-victory.html. Accessed 10 Feb 2017
46. Cialdini, R.B.: Influence, vol. 3. A. Michel (1987)
47. McKenna, K.Y., Bargh, J.A.: Coming out in the age of the internet: identity "demarginalization" through virtual group participation. J. Pers. Soc. Psychol. **75**(3), 681 (1998)
48. De Koster, W., Houtman, D.: Stormfront is like a second home to me: on virtual community formation by right-wing extremists. Inf. Commun. Soc. **11**(8), 1153–1175 (2008)
49. Gonzales, A.L., Hancock, J.T.: Identity shift in computer-mediated environments. Media Psychol. **11**(2), 167–185 (2008)
50. Qu, Y., Huang, C., Zhang, P., Zhang, J.: Microblogging after a major disaster in China: a case study of the 2010 Yushu Earthquake. In: Proceedings of CSCW 2011, pp. 25–34 (2011)
51. Starbird, K., Palen, L., Hughes, A., Vieweg, S.: Chatter on the red: what hazards threat reveals about the social life of microblogged information. Proceedings of CSCW **2010**, 241–250 (2010)
52. Conway, M.: From al-Zarqawi to al-Awlaki: the emergence and development of an online radical milieu. CTX: Combat. Terror. Exch. **2**(4), 12–22 (2012)
53. Gleason, B.: # occupy wall street: exploring informal learning about a social movement on Twitter. Am. Behav. Sci. **57**(7), 966–982 (2013)
54. Starbird, K., Palen, L.: (How) will the revolution be retweeted? Information diffusion and the 2011 Egyptian uprising. In: Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work, pp. 7–16. ACM, February 2012
55. Wulf, V., Misaki, K., Atam, M., Randall, D., Rohde, M.: 'On the ground' in Sidi Bouzid: investigating social media use during the tunisian revolution. In Proceedings of the 2013 Conference on Computer Supported Cooperative Work, pp. 1409–1418. ACM, February 2013
56. Cheung, A.S.: China internet going wild: cyber-hunting versus privacy protection. Comput. Law Secur. Rev. **25**(3), 275–279 (2009)
57. Tonkin, E., Pfeiffer, H.D., Tourte, G.: Twitter, information sharing and the London riots? Bull. Am. Soc. Inf. Sci. Technol. **38**(2), 49–57 (2012)

58. Christensen, H.: Political activities on the Internet: slacktivism or political participation by other means? First Monday **2** (2011). http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3336
59. Schumann, S., Klein, O.: Substitute or stepping stone? Assessing the impact of low-threshold online collective actions on offline participation. Eur. J. Soc. Psychol. **45**(3), 308–322 (2015)
60. Morozov, E.: The brave new world of slacktivism [Weblog post] (2009). http://neteffect.foreignpolicy.com/posts/2009/05/19/the_brave_new_world_of_slacktivism
61. Gladwell, M.: Small change: why the revolution will not be tweeted [Weblog post] (2010). http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell
62. Sproull, L., Kiesler, S.: Reducing social context cues: electronic mail in organizational communication. Manag. Sci. **32**(11), 1492–1512 (1986)
63. Ellison, N., Heino, R., Gibbs, J.: Managing impressions online: self-presentation processes in the online dating environment. J. Comput.-Mediat. Commun. **11**(2), 415–441 (2006)
64. Toma, C.L., Hancock, J.T., Ellison, N.B.: Separating fact from fiction: an examination of deceptive self-presentation in online dating profiles. Pers. Soc. Psychol. Bull. **34**(8), 1023–1036 (2008)
65. Guadagno, R.E., Okdie, B.M., Kruse, S.A.: Dating deception: gender, online dating, and exaggerated self-presentation. Comput. Hum. Behav. **28**(2), 642–647 (2012)
66. Hancock, J.T., Toma, C., Ellison, N.: The truth about lying in online dating profiles. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 449–452. ACM, April 2007
67. McVeigh, T., Reidy, T.: Families who fear Isis is targeting their children urged to lock up their passports. Guard. (2015). https://www.theguardian.com/society/2015/feb/21/syria-isis-uk-families-warned-lock-up-passports-daughters
68. Kelly, A.E., Rodriguez, R.R.: Publicly committing oneself to an identity. Basic Appl. Soc. Psychol. **28**, 185–191 (2006)
69. Tice, D.: Self-concept shift and self-presentation: the looking glass self is also a magnifying glass. J. Pers. Soc. Psychol. **63**, 435–451 (1992)
70. Schlenker, B.R., Dlugolecki, D.W., Doherty, K.: The impact of self- presentations on self-appraisals and behavior: The power of public commitment. Pers. Soc. Psychol. Bull. **20**, 20–33 (1994)
71. Walther, J.B.: Computer-mediated communication impersonal, interpersonal, and hyperpersonal interaction. Commun. Res. **23**(1), 3–43 (1996)
72. Walther, J.B., Parks, M.R.: Cues filtered out, cues filtered. In: Handbook of Interpersonal Communication, pp. 529–563 (2002)
73. Kaplan, A.M., Haenlein, M.: Users of the world, unite! The challenges and opportunities of social media. Bus. Horiz. **53**(1), 59–68 (2010)
74. Anti-Defamation League: Best practices for responding to cyberhate (2014)
75. Harper, F.M., Frankowski, D., Drenner, S., Ren, Y., Kiesler, S., Terveen, L., Riedl, J.: Talk amongst yourselves: inviting users to participate in online conversations. In: Proceedings of the 12th International Conference on Intelligent User Interfaces, pp. 62–71. ACM, January 2007
76. Kiesler, S., Kraut, R., Resnick, P., Kittur, A.: Regulating behavior in online communities. In: Building Successful Online Communities: Evidence-Based Social Design. MIT Press, Cambridge (2012)
77. Lampe, C., Resnick, P.: Slash (dot) and burn: distributed moderation in a large online conversation space. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 543–550. ACM, April 2004
78. Preece, J.: Empathic communities: balancing emotional and factual communication. Interact. Comput. **12**(1), 63–77 (1999)