Chapter 2
A Cyber-Psychological and Behavioral Approach to Online Radicalization

Reyhan Topal
Bilkent University, Turkey

ABSTRACT

This chapter attempts to synthesize the mainstream theories of radicalization and the cyber-psychological and behavioral approaches with a view to identifying individuals' radicalization online. Based on the intersections of those two fields, this chapter first elaborates how radical groups use cyberspace with a specific concentration on the so-called cyber caliphate claimed by the Islamic State of Iraq and al-Sham (ISIS). Second, it revisits mainstream theories of radicalization and specifies the psychological and behavioral facets of the radicalization processes proposed by those theories. Following that, it integrates theories of radicalization with cyber-psychological and behavioral explanations of online radicalization to reveal how ISIS's use of cyberspace attracts individuals and facilitates online radicalization.

INTRODUCTION

Since 1990s, individuals and groups have been building new societies, spaces, and networks on the internet with their online identity bricks. Such experiences of digitalization have broadened the scope of social research, as scholars attempted to incorporate a new cyber dimension into their debates. Hence, recent research on terrorism and radicalization has moved beyond the classical theories of radicalization to empirical assessments of digital dynamics that may pave the way for online radicalization of individuals, which in turn culminate in acts of violence. In order to explain the contextual dynamics of online radicalization, scholars closely watch contemporary developments in cyberspace, and encompass the radical use of cyber tools in their research. Reiterating generally acknowledged facts about the internet, many of those studies dwell on the internet's facilitating role for individuals, who have radical ideas to some extent and who are already become radicalized, to socialize among other likeminded individuals, and for virtual radical groups to convey their messages to a larger audience by exceeding spatial and temporal limits.

DOI: 10.4018/978-1-5225-7119-3.ch002

Notwithstanding the increasing volume of publications that review online radicalization and terrorism, to date there have been very few scholarly efforts to expound on the cyber-psychological and behavioral dimensions of online radicalization. For the purpose of filling such a gap, this chapter aims to examine the intersections of radicalization theories and the cyber-psychological and behavioral approaches in order to identify how individuals become radicalized online. This chapter will first analyze how radicals use cyberspace with a specific concentration on the so-called cyber caliphate claimed by the Islamic State of Iraq and al-Sham (ISIS). Second, the chapter will elaborate on mainstream theories of radicalization in detail, and explore the psychological and behavioral facets of the radicalization processes referred by those theories. Finally, it will synthesize theories of radicalization with cyber-psychological and behavioral explanations of online radicalization in order to explain how ISIS' use of cyberspace attracts individuals and paves the way for online radicalization. Even though the utilization of online tools by radical groups might be traced back to the 1980s when members of those groups prepared propaganda movies on videotape and published sophisticated magazines to disseminate via mail (Stern and Berger, 2016), the use of cyberspace as an ideological battleground for radical groups occurred in the 2000s following the rise of social media as a phenomenon. Therefore, this chapter aims to reach a more comprehensive picture of contemporary developments in online radicalization by elaborating further on ISIS and the cyber-psychological and behavioral dimensions of the debate. Taking this into consideration, this chapter will specifically focus on the themes of *socialization, enculturation, cognitive opening, and anonymity* as psychological and behavioral dimensions to assess how cyberspace may play a facilitating role in radicalization.

ONLINE RADICALIZATION AND RADICALS' USE OF CYBERSPACE

Currently almost one-third of the world's population uses smart phones (Statista, 2017), Facebook has more than 2 billion active users (Statista, 2017), and Twitter has 328 million monthly users (Statista, 2017). Considering the transformative characteristic of internet technologies, and the facilitating role of social media platforms for communication and influence, it seems unsurprising that radical groups embraced those opportunities for the same reasons as other groups (Aly, et al., 2017). If one construes terrorism as a type of communication (Schmid and de Graaf, 1982) or as a form of "communicative violence" (Aly, et al., 2017), then disseminating propaganda messages to attract the masses and gain sympathizers/new recruits are central to it. Hence, this aspect of internet technologies which is prone to abuse became a golden opportunity for radical groups that hinge on communication due to the aforementioned reasons.

Research on online radicalization stemmed from concerns related to the dark side of the internet, which might facilitate the radicalization of individuals and furthermore their engagement with violent extremist activities. Before it was brought to light that al-Qaeda members shared the details of the planned terrorist attacks to be held on 9/11 through email drafts on a common email address, very few attempts had been made to address the possibility of online radicalization, although the inexorable progress and spread of internet technologies had already been a hot topic among social scientists. During 1990s, scholars expected diverse outcomes from the new digital age. On the one side, there were optimists who mostly cited the positive benefits of the internet, such as opening new channels for social relations by promoting pluralism and diversity (Rheingold, 1993), and providing a real medium for friendship (Katz & Aspden, 1997). On the other, there were pessimists who underscored the alarming side of the internet. According to those perspectives, the internet would create "a nation of strangers" (Turkle, 1995)

by destroying social integration, and engender an "internet paradox" by reducing social involvement, psychological well-being, and emotional investment (Kraut et al., 1998). The truly interesting side of the debate was that online radicalization mostly used the internet's positive benefits such as providing a diverse and easily reachable mass, but then these aspects were twisted by potential radicals to reach like-minded individuals and groups, and to engage in violent extremism and terrorist acts.

The historical progress of how radical groups used cyberspace says a lot about how quickly they integrated their virtual goals and activities into a new cyber environment, though it is difficult to place each and every activity of those groups into chronological order. Despite Al Qaeda's early attempts to make use of the internet, Lebanon's Hezbollah emerged later on as a leading agent of radicalization in cyberspace. Today, Hezbollah has more than 20 websites in 7 languages (Arabic, Azeri, English, French, Hebrew, Persian, and Spanish), many television and radio channels as well as a quite complex social media network (The Meir Amit Intelligence and Terrorism Information Center, 2013), all of which provide the group with vast opportunities to establish networks, communicate, and spread propaganda. Among some of the cyber capabilities of Hezbollah are leaking planes' camera systems, organizing attacks on DoS (Denial of Service) and DDoS (Distributed Denial of Service), and hacking fiber optic cables (Richards, 2014). The group used most of those aforementioned capabilities during the Israel-Lebanon War of 2006 (Saad, Bazan & Varin, 2015). Founding the "Cyber Hezbollah", a branch of the group responsible for the group's cyber initiatives, Hezbollah holds regular cyber conferences with the participation of "Islamist hackers" and "cyber jihadists" in order to find new strategies in cyberspace (Wahdat-Hagh, 2011). Improved cyber skills give Hezbollah the opportunity to spread propaganda, communicate, win over the hearts and minds of potential radicals, and facilitate online radicalization.

As cyber technologies and online media sources gradually sophisticated, radical groups advanced their online strategies accordingly. A recent and staggering example was how members of Al Shabaab used the group's Twitter account during the terrorist attack at the Westgate Mall in Kenya in 2013 (Mair, 2017). During the four-day siege - which resulted in 67 fatalities and 175 wounded - the world watched closely while the group live-tweeted the terrorist attack on its Twitter feed. Considering that Kenya is one of the most active countries in Africa on Twitter, and President Uhuru Kenyatta is among the most-followed African leaders (Simon et al., 2014), Shabaab's use of Twitter as a communication channel seemed well-planned in attracting both domestic and international attention. Lashkar-e-Taiba, a Pakistan based militant organization, also has sophisticated cyber capabilities, and claimed to use Google Earth in order to gather intelligence and determine routes during its attacks on Mumbai in November 2008 (Glanz, Rotella and Sanger, 2014). What is more, Jamaat-ud-Dawah, the so-called charity arm of Lashkar-e-Taiba, allegedly held a two-day conference on social media for their future cyber initiatives, in Lahore, on December 26 and 27, 2015 (Sharma, 2016). In the light of those examples, the ability of radical groups to adopt and engage with a dynamic digital world is worth discussing.

Among other contemporary examples, ISIS is distinguished with its more sophisticated use of online platforms and its developed understanding of cyberspace in general. In order to draw a detailed picture of ISIS, one should undoubtedly consider its cyber dimension, which makes the group a cyber threat of modern times. Only through the use of social media and online communication was ISIS able to make its dramatic debut onto the global arena,claiming that it had founded a sharia-based sovereignty not only in Syria and Iraq but also across the world. ISIS is not unique in declaring war against non-believers, or in calling each and every Muslim to a global jihad. As an example, al Qaeda's members were mostly comprised of Arabs who fought against Soviet Russia during the "Afghan jihad" (Johnson and Mason, 2007) and went onto commit the 9/11 attacks against the US, and Lebanon's Hezbollah promised to

continue fighting without recognizing any treaties, ceasefires, or peace agreements until the Muslims re-gained their rights and lands (Levitt, 2013). All these groups are of the same opinion about maintaining a global war against the Westand bringing the Muslims altogether under the same flag of Islam, like many other radical Islamist groups. What differentiates ISIS is that the group has been working to declare and promote those claims to the world online unlike the former examples, which remained relatively less salient and efficient in cyberspace. ISIS became the first radical group to claim a "cyber caliphate" when Cunaid Hussein, an ISIS militant from Britain, hacked the official Twitter and YouTube accounts of the U.S. Central Command, and published the following message online: "In the name of Allah, the Most Gracious, the Most Merciful, the Cyber Caliphate continues its Cyber Jihad" (CNN, 2015). By doing so, ISIS also became the first actor to conceptualize the "cyber jihad". So, why does ISIS persist on having supremacy in cyberspace?

Considering the spatial, financial, and legal obstacles in reaching a large audience and convincing others of ISIS' ongoing ideological battle, online radicalization appears to be the easiest and most efficient way to disseminate messages in order to gain new recruits. There are many facets to be discussed and understood about why the group claims a cyber caliphate, with persuasion and propaganda being the primary goals of ISIS in cyberspace. Their communication strategy attempts to persuade prospective recruits to do the following: Join the group, and fight in order to restore a caliphate for Islam (Farwell, 2014). If the target is non-believer, then persuade the target to accept Islam and move to Syria (*hijrah*). ISIS pursues complicated and well-planned communication strategies, particularly in social media, such as using the rhetoric of *takfir*, a very powerful doctrine of excommunication by pronouncing a Muslim an infidel (Zelin, 2014). Using the rhetoric of *takfir*, ISIS threatens Muslims with dismissal from Islam if they do not advocate what the group offers in the name of their peculiar interpretation of religion. Muslim youths, especially the ones who live in Western countries, facing discrimination, and isolation in small Muslim enclaves (Graham, 2015), pay great attention to ISIS' call, as the group's call for a global jihad and a universal caliphate under the flag of sharia on the borderless earth of Allah appears to promise limitless freedom, a utopia that those young people have long been yearning for. So, online propaganda and communication strategies of ISIS mostly address such a disgruntled group of youth easily prone to online radicalization.

The dissemination of knowledge plays a vital role for ISIS in online radicalization. Notwithstanding its extremist and irrational interpretation of the world and religion, the group's online media strategy stands as a modern and sophisticated one (Lesaca, 2015) that encompasses a wide spectrum of online magazines in different languages such as Dabiq in English and Konstantiniyye in Turkish, numerous social media platforms including Twitter, Facebook, and YouTube accounts, as well as blogs and forums to gather similar minds together. Through those platforms, the group has the opportunity of sharing high-quality photographs and videos, which reflect ISIS' growing violent political extremism (Conway, 2017). Hence, online media is an endless source for ISIS to simply reveal its tour de force. Apart from elaborating on the advanced skills of ISIS members, one should shed light on the reasons why and how ISIS uses cyberspace and online media so efficiently for online radicalization. Next chapter will problematize radicalization, and analyze mainstream theories of radicalization, and then be followed by another one that will integrate the cyber-psychological and behavioral approaches into radicalization theories to understand how cyberspace facilitates radical groups such as ISIS for online radicalization.

REVISITING THE THEORIES OF RADICALIZATION

Scholars of radicalization propose different types of models in order to explore the radicalization of individuals, as well as the decision to participate in radical groups, and engage in violent behavior. In each model, scholars underscore multifaceted social, economic, structural, psychological, circumstantial, and other types of determinants to dismantle the path towards radicalization. Therefore, there is not one strain of radicalization model that is agreed upon, giving the radicalization debate a lively characteristic. For example, the radicalization model proposed by some scholars concentrates on the theme of cognitive opening and attempts to analyze which material and non-material circumstances make individuals drift towards radicalization (Bjorgo & Horgan, 2009; Blee, 2002; Simi & Futrell, 2010). For others, the psychological wellbeing of individuals is of significance, so that emotions such as alienation, anger, disenfranchisement, and belief of being unjustly treated might pave the way for radicalization (Kimhi & Even, 2006). Peer dynamics (Bakker, 2006), motivation of group belonging (McCauley & Moskalenko, 2011), adventure-seeking (Gibson, 1994), seeking power and prestige (Stern, 2003), and demographic factors such as gender and age (Chermark & Gruenewald, 2015) are also usually considered significant factors among scholars.

Though there is a plethora of studies on why and how individuals become radicalized and join radical groups in the literature of radicalization and terrorism, there is almost no scholarly attempt to contextualize online radicalization within the radicalization theories. In order to examine the online radicalization process of individuals, one should carefully integrate those theories into the literature on radicals' use of cyberspace. Most of the radicalization theories regard the radicalization as a process, and attempt to analyze that process stage by stage. Among different types, there have been several established and widely-accepted models which try to examine the radicalization process. This chapter focuses on the mainstream models so as to contextualize online radicalization from a cyber-psychological and behavioral approach in those models.

Borum's model of radicalization in FBI Law Enforcement Bulletin is a prototypic psychological one (Borum, 2003). In his model, Borum proposes 4 stages: An initial stage where an individual notices that his/her conditions are not desirable, the second stage where the individual compares those undesirable conditions and comes to the conclusion that "it is not fair", the third stage where the individual blames a specific target for the unfair situation, and the last stage where the individual generates stereotypes and dehumanizes the enemy who seems responsible for the unfair situation (Borum, 2003). So, Borum's model of the process of radicalization focuses more on the ideological and psychological sides of the process.

Based on his ethnographic study among the members of Al-Muhajiroun, Wiktorowicz develops a 4-stage model of joining extremist groups, though he considers the term radicalization problematic: An initial stage where the "cognitive opening" of the individual occurs as a result of reverse life experiences such as discrimination or victimization, the second stage where those experiences lead the individual towards "religious seeking", the third stage where the individual regards the worldview of extremist Islamic groups as overlapping with his/her worldview and engages in a "frame alignment", and the last stage where the individual's "socialization and joining" the extremist Islamic groups occurs (Wiktorowicz, 2004). In spite of being a limited analysis of participation in extremist Islamic groups, Wiktorowicz's model offers significant insights about behavioral process of pre-participation.

Examining the radicalization process through a 5-floor staircase model, Moghaddam's model is also well-established (Moghaddam, 2005). On the ground floor, the individual experiences unfairness and relative deprivation, and if the individual believes that he/she cannot reach at greater justice through

mobility or cannot influence the decision makers, he/she is more likely to climb onto the second floor where the anger and frustration with the deprivation is channeled towards the "enemy" mostly through physical force. On the third, the individual finds other like-minded individuals, and begins justifying terrorism. On the fourth, individual joins a terrorist group, and embraces the "us vs. them", and "good vs. evil" categorizations of the group. Finally, individual is trained for injuring and killing others, and sent to realize terrorist acts (Moghaddam, 2005). So, Moghaddam takes the process from a psychological/perceptional step, feeling of relative deprivation, and ends with physical act of violence.

Criticizing the gaps in the micro and macro approaches to the study of terrorism and radicalization, Sageman attempts to bridge both through a middle-range approach (Sageman, 2008). So, in contrast to the previously mentioned three models which explain radicalization process through sequential stages, Sageman puts forward the interplay of three cognitive and one situational factors to propose a non-linear radicalization process (Sageman, 2008). Among the cognitive factors are the sense of moral outrage which refers to feeling of being morally violated, the frame of interpretation which is used to justify the situation such as "war against Islam", and resonance with personal experiences such as discrimination (Sageman, 2008). According to Sageman, those cognitive factors reinforce each other, and in total, these factors may result in radicalization of the individual. As a situational factor, Sageman mentions "mobilization through networks", which refers to the individual's confirmation of his/her ideas through communication with other radicalized individuals (Sageman, 2008).

In the light of those established models, how could one explain online radicalization? The following chapter will integrate theories of radicalization into cyber-psychological and behavioral explanations of online radicalization so as to reveal how the ISIS' use of cyberspace attracts individuals and paves the way for online radicalization.

A CYBER-PSYCHOLOGICAL AND BEHAVIORAL APPROACH TO ONLINE RADICALIZATION

Throughout the previous chapters which reviewed the online presence of ISIS and the theories of radicalization, many aspects pertaining to the psychological and behavioral facets of the debate were covered. Both chapters referred to the psychological and behavioral dimensions of radicalization while addressing the reasons of ISIS' claims for a cyber caliphate and the main determinants of radicalization. With the purpose of contributing to the literature on online radicalization, this chapter elaborates on how internet technologies may facilitate online radicalization by providing favorable conditions for socialization, enculturation, cognitive opening, and anonymity. In doing so, this chapter tries to expand the scope of theories of radicalization by applying the aforementioned themes to explain online radicalization through the example of the ISIS' use of cyberspace.

Scholars generally argue that anonymity on the internet enables individuals to connect and socialize with others who share similar ideologies and values with themselves (Quinn and Forsyth, 2013). Such anonymity helps particularly lonely, marginalized, non-assertive, and asocial individuals socialize very quickly, since it is easier to communicate online without the pressure of face-to-face interaction, and online socialization helps individuals eliminate their socio-phobia. According to previous research, individuals experience lower social anxiety, more social desirability and higher self-esteem in the cyberspace than the virtual world due to the veil of anonymity. (Joinson, 1999). Such "positive" impact has several outcomes, according to McKenna and Bargh (2000):

The assurance of anonymity gives one far greater play in identity construction than is conceivable in face-to-face encounters. One can, for instance, change one's gender, one's way of relating to others, and literally everything about oneself […] On the internet, where one can be anonymous, where one does not deal in face-to-face interactions, where one is simply responding to other anonymous people, the roles and characters one maintains for family, friends, and associates can be cast aside.

With regards to radicalization, it could be asserted that most people tend to behave in a harmonious way in the social environment, and the fear of legal ramifications and social rejection may prevent individuals from expressing their radical views and seeking other individuals with similar opinions (Holt, 2007; Quinn and Forsyth, 2013). Yet, anonymity allows individuals to socialize with others without those hesitations, and also diminish personal obstacles such as high social anxiety and low self esteem. This also explains why online platforms constitute the main basis of ISIS' attraction of sympathizers and new recruits. As previously mentioned, many Muslims living outside the Muslim-majority countries feel themselves excluded and unjustly treated in the societies they live in. The anonymity in the cyberspace gives them the opportunity of impersonation, and they easily meet and socialize with like-minded individuals who encourage them to engage in violent extremist activities and join ISIS. Therefore, the anonymity and socialization opportunities provided by the cyberspace address Wictorowicz's "socialization and joining," Moghaddam's "finding likely minds," and Sageman's "mobilization through networks" elements in the ISIS case.

Cognitive opening refers to the phenomenon in which personal crises or awakenings expose individuals to a new reality (Blee, 2002) such as radicalization or taking the decision to engage in violent acts. When individuals enter the process of cognitive opening, they seek ideas consistent with their own. In such a process, the internet, an endless source of ideological communication and messaging, might provide individuals easy access to networks and messages from the radical groups (Britz, 2010). What is more, cyberspace might be a source of cognitive opening following the previous steps of socialization with the help of anonymity. Therefore, internet accelerates the transition from cognitive opening to taking action, and individuals might easily end up participating in radical groups. To have a better understanding of cognitive opening and online radicalization, one should revise the ISIS case one more time. The ISIS' online media strategy is based on "convincing" others of anything the group claims, despite the irrationality of those claims, in order to accelerate the transition from cognitive opening to taking action. To exemplify, ISIS on its online platforms pretends to win its battle in Syria, and have already established a caliphate in the country where people are happily living. According to what ISIS claims online, new recruits will embrace real Islam by joining group, and they will be martyrs and go to the paradise if they die. Comparing their unjust situation with what ISIS promises, people decide to join the group more easily. Publishing online journals and photographs, and releasing videos which are professionally edited, ISIS disseminates those ideas with the help of cyberspace. Those aspects address Wictorowicz's "cognitive opening" and Moghaddam's "perception of fairness and feeling of relative deprivation" in the ISIS case.

Enculturation is one of the most significant aspects of online radicalization. When individuals experience cognitive opening, and find the ideology for which they have long been seeking, they enter into the process of enculturation where they learn the content of that ideology, its code of behavior, and the traditions that its followers embrace. The process of online enculturation is similar to how an individual embraces violent behavior on the streets in the real world. Forums, newsgroups, social media channels, and many other online platforms might facilitate the global transmission of knowledge (Rosenmann &

Safir, 2006), and radical groups get their share from such massive transmission. Once individuals who feel sympathy for radical groups socialize with other sympathizers and members online, they easily embrace the code of conduct and behavior patterns from members of these groups. So, they do not have to physically come together and spend time with one another for such enculturation to occur, as the internet melts the physical barriers of communication. ISIS' online media strategy appears to be a rich source of enculturation for anyone, as the group attempts to make a *jihadi* culture with its own jargon. To exemplify, the group uses the words *visit* (regular meetings of the group members), *invitation* (gaining new members), *migration* (participation to the ISIS), and *demonic* (anything in contrary with the ideology of the ISIS) in its online magazines. Once this jargon is embraced by people, even in the virtual absence of the ISIS in the life of radicals online, such *jihadi* culture will reproduce itself in different groups and in different times. Borum's "dehumanizing the enemy," Wictorowicz's "religious seeking," Moghaddam's "us versus them," and Sageman's "frame of interpretation" elements fit very well into such enculturation, and points to why scholars should integrate online radicalization into the literature on radicalization theories with respect to cyber-psychological and behavioral aspects of the debate.

CONCLUSION

Despite the increasing volume of publications that analyze online radicalization and terrorism, there have been almost no scholarly efforts that shed light on the cyber-psychological and behavioral dimensions of online radicalization. This chapter examines the intersections of radicalization theories and the cyber-psychological and behavioral approaches in order to identify how individuals get radicalized online through the ISIS case. Analyzing the online radicalization and radicals' use of cyberspace with a specific concentration on the ISIS' claim of a cyber caliphate, the chapter revisits the mainstream theories of radicalization, and specifies the psychological and behavioral facets of the radicalization processes proposed by those theories. Then, it integrates theories of radicalization with cyber-psychological and behavioral explanations of online radicalization so as to reveal how ISIS' use of cyberspace attracts individuals and paves the way for online radicalization. By doing so, it aims to reach a more comprehensive picture of contemporary developments in online radicalization by elaborating further on ISIS and the cyber-psychological and behavioral dimensions of its use of cyberspace by focusing on the themes of *socialization, enculturation, cognitive opening, and anonymity* as psychological and behavioral dimensions to assess how cyberspace may play a facilitating role for radicalization.

REFERENCES

Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2017). Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. *Studies in Conflict and Terrorism*, *40*(1), 1–9. doi:10.1080/1057610X.2016.1157402

Bakker, E. (2006). *Jihadi Terrorists in Europe, Their Characteristics and the Circumstances in Which They Joined the Jihad: An Exploratory Study*. The Hague: Clingendael Institute.

Bjorgo, T., & Horgan, J. (2009). *Leaving Terrorism Behind: Individual and Collective Disengagement*. New York: Routledge.

Bjørgum, M. H. (2016). Jihadi Brides: Why do Western Muslim Girls Join ISIS? *Global Politics Review*, *2*(2), 91–102.

Blee, K. M. (2002). *Inside Organized Racism: Women and Men in the Hate Movement*. University of California Press.

Borum, R. (2003). Understanding the Terrorist Mindset. *FBI Law Enforcement Bulletin*, 7-10.

Britz, M. T. (2010). Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts. In T. J. Holt (Ed.), *Crime On-Line: Correlates, Causes, and Context* (pp. 193–220). Raleigh, NC: Carolina Academic Press.

Center, T. M. (2013). Terrorism in Cyberspace: Hezbollah's Internet Network. *Terrorism Info.* Retrieved 06 01, 2017, from http://www.terrorism-info.org.il/Data/articles/Art_20488/E_276_12_739632364.pdf

Chermak, S. D., & Gruenewald, J. (2015). Laying the Foundation for the Criminological Examination of Right-wing, Left-wing, and Al Qaeda Inspired Extremism in the United States. *Terrorism and Political Violence*, *27*(1), 133–159. doi:10.1080/09546553.2014.975646

CNN Staff. (n.d.). CENTCOM Twitter account hacked, suspended. *CNN*. Retrieved 20 10 2017, from http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/index.html

Conway, M. (2017). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict and Terrorism*, *40*(1), 77–98. doi:10.1080/1057610X.2016.1157408

Farwell, J. P. (2014). The Media Strategy of ISIS. *Survival: Global Politics and Strategy*, *56*(6), 49–55. doi:10.1080/00396338.2014.985436

Gibson, J. W. (1994). *Warrior Dreams: Violence and Manhood in Post-Vietnam America*. Louisville, KY: Hill & Wang.

Glanz, J., Rotella, S., & Sanger, D. E. (2014). Mumbai Attacks Piles of Spy Data, but an Uncompleted Puzzle. *New York Times*. Retrieved 04 16, 2017, from https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?mcubz=2

Graham, J. (2015). Who Joins ISIS and Why? *Huffington Post*. Retrieved 06 10, 2017, from http://www.huffingtonpost.com/john-graham/who-joins-isis-and-why_b_8881810.html

Holt, T. J. (2007). Subcultural Evolution? Examining the Influence of on- and off-line Experiences on Deviant Subcultures. *Deviant Behavior*, *28*(1), 171–198. doi:10.1080/01639620601131065

Johnson, T. H., & Mason, M. C. (2007). Understanding the Taliban and Insurgency in Afghanistan. *Orbis*, *51*(1), 71–89. doi:10.1016/j.orbis.2006.10.006

Joinson, A. (1999). Social Desirability, Anonymity, and Internet-based Questionnaires. *Behavior Research Methods, Instruments, & Computers*, *31*(3), 433–438. doi:10.3758/BF03200723 PMID:10502866

Katz, J. E., & Aspden, P. (1997). A Nation of Strangers. *Communications of the ACM*, *40*(12), 81–86. doi:10.1145/265563.265575

Kimhi, S., & Even, S. (2006). The Palestinian Human Bombers. In J. Victoroff (Ed.), *Tangled Roots: Social and Psychological Factors in the Genesis of Terrorism* (pp. 308–322). Trenton, NJ: IOS Press.

Kraut, R., Mukhopadhyay, T., Szczypula, J., Kiesler, S., & Scherlis, W. (1998). Communication and Information: Alternative uses of the Internet in households. In *Proceedings of the CHI* 98 (pp. 368-383). New York: ACM. 10.1145/274644.274695

Kruglanski, A. W., & Fishman, S. (2009). Psychological Factors in Terrorism and Counterterrorism: Individual, Group, and Organizational Levels of Analysis. *Social Issues and Policy Review*, *3*(1), 1–44. doi:10.1111/j.1751-2409.2009.01009.x

Lesaca, J. (2015). *On Social Media, ISIS Uses Modern Cultural Images to Spread Anti-modern Values.* Brookings Institute. Retrieved 05 30, 2017, from: https://www.brookings.edu/blog/techtank/2015/09/24/on-social-media-isis-uses-modern-cultural-images-to-spread-anti-modern-values/

Levitt, M. (2013). *Hezbollah: The Global Footprint of Lebanon's Party of God*. Washington, DC: Georgetown University Press.

Mair, D. (2017). #Westgate: A Case Study: How al-Shabaab Used Twitter During an Ongoing Attack. *Studies in Conflict and Terrorism*, *40*(1), 24–43. doi:10.1080/1057610X.2016.1157404

McCauley, C., & Moskalenko, S. (2008). Mechanisms of Political Radicalization: Pathways Toward Terrorism. *Terrorism and Political Violence*, *20*(3), 415–433. doi:10.1080/09546550802073367

McKenna, K. Y., & Bargh, J. A. (2000). Plan 9 From Cyberspace: The Implications of the Internet for Personality and Social Psychology. *Personality and Social Psychology Review*, *4*(1), 57–75. doi:10.1207/S15327957PSPR0401_6

Moghaddam, F. M. (2005). The Staircase to Terrorism: A Psychological Exploration. *The American Psychologist*, *60*(2), 161–169. doi:10.1037/0003-066X.60.2.161 PMID:15740448

Quinn, J. F., & Forsyth, C. J. (2005). Describing Sexual Behavior in the Era of the Internet: A Typology for Empirical Research. *Deviant Behavior*, *26*(3), 191–207. doi:10.1080/01639620590888285

Rheingold, H. (1993). *The Virtual Community: Homesteading on the Electronic Frontier*. MIT Press.

Richards, J. (2014). *Cyber-War: The Anatomy of the Global Security*. New York: Palgrave Macmillan. doi:10.1057/9781137399625

Rosenmann, A., & Safir, M. P. (2006). Forced Online: Pushed Factors of Internet Sexuality: A Preliminary Study of Paraphilic Empowerment. *Journal of Homosexuality*, *51*(3), 71–92. doi:10.1300/J082v51n03_05 PMID:17135116

Saad, S., Bazan, S., & Varin, C. (2015). Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a New Strategic Battlefield. *Webscience*. Retrieved 06 01, 2017, from: http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. University of Pennsylvania Press. doi:10.9783/9780812206784

Schmid, A. P., & de Graaf, J. (1982). *Violence as Communication: Insurgent Terrorism and the Western News Media*. London: SAGE Publications.

Sharma, M. (2016). *Lashkar-e-Cyber of Hafiz Saeed.* Institute for Defense Studies and Analyses. Retrieved 06 01, 2017, from: http://www.idsa.in/idsacomments/lashkar-e-cyber-of-hafiz-saeed_msharma_310316#footnote1_amq1mz7

Simi, P., & Futrell, R. (2006). Cyberculture and the Endurance of Radical Racist Activism. *Journal of Political and Military Sociology*, *34*(1), 115–142.

Simon, T., Goldberg, A., Aharonson-Daniel, L., Leykin, D., & Adini, B. (2014). Twitter in the Cross Fire—The Use of Social Media in the Westgate Mall Terror Attack in Kenya. *PLoS One*, *9*(8), 1–11. doi:10.1371/journal.pone.0104136

Statista. (2017a). *Number of Smartphone Users Worldwide from 2014 to 2019 (in Millions).* Retrieved 06 01, 2017, from: http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Statista. (2017b). *Number of Monthly Active Facebook Users*. Retrieved 06 10, 2017, from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Statista. (2017c). *Number of Monthly Active Twitter Users.* Retrieved 06 10, 2017, from https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

Statista. (2017d). *Number of Smartphone Users Worldwide*. Retrieved 06 10, 2017, from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Stern, J. (2003). *Terror in the Name of God: Why Religious Militants Kill*. New York: Harper Collins.

Stern, J., & Berger, J. M. (2016). *ISIS: The State of Terror*. New York: Harper Collins Publishers.

Taylor, M., & Horgan, J. (2006). A Conceptual Framework for Addressing Psychological Process in the Development of the Terrorist. *Terrorism and Political Violence*, *18*(4), 585–601. doi:10.1080/09546550600897413

Turkle, S. (1996). Virtuality and Its Discontents: Searching for Community in Cyberspace. *The American Prospect*, *24*(1), 50–57.

Usborne, D. (2015). Centcom 'Hacked' by ISIS Supporters: US Military Twitter Feed Publishes Personal Information of Senior Officers. *Independent*. Retrieved 05 03, 2017, from http://www.independent.co.uk/news/world/americas/us-central-command-hacked-by-islamic-state-supporters-9973615.html

Wahdat-Hagh, W. (2011). Iran And Cyber-Hezbollah Strategies: Killing Enemies In Hyperspace – Analysis. *Eurasia Review.* Retrieved 06 01, 2017, from: http://www.eurasiareview.com/25112011-iran-and-cyber-hezbollah-strategies-killing-enemies-in-hyperspace-analysis/

Wiktorowicz, Q. (2004). *Joining the Cause: Al-Muhajiroun and Radical Islam.* Paper presented at the Roots of Islamic Radicalism Conference, New Haven, CT.

Zelin, A. Y. (2014). *Al-Qaeda Disaffiliates with the Islamic State of Iraq and al-Sham.* Retrieved 05 30, 2017, from Washington Institute: http://www.washingtoninstitute.org/policy-analysis/view/al-qaeda-disaffiliates-with-the-islamic-state-of-iraq-and-al-sham

KEY TERMS AND DEFINITIONS

Anonymity: The condition in which someone's identity is unknown. It is the adjective of anonymous, which derived from the Greek word *anonymia*, meaning nameless.

Cognitive Opening: The state of mind in which an individual is eager to receive the message that mostly has an ideological characteristic.

Cyberspace: The virtual space where computer networks and internet exist.

Enculturation: The process in which an individual learns, internalizes, and applies the codes of a specific culture.

Internet: A worldwide platform that interconnects computer networks.

Online Radicalization: An aspect of radicalization where an individual begins or advances his/her radicalization process through cyberspace.

This research was previously published in Psychological and Behavioral Examinations in Cyber Security edited by John McAlaney, Lara A. Frumkin, and Vladlena Benson, pages 210-221, copyright year 2018 by Information Science Reference (an imprint of IGI Global).