Chapter 56

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.

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

Related Content

Times of Change, Times of Turbulence: Seeking an Ethical Framework for Curriculum Development during Critical Transition in Higher Education
William Boydand Diane Newton (2011). *International Journal of Cyber Ethics in Education (pp. 1-11).*
www.irma-international.org/article/times-change-times-turbulence/56104

Tracing the Non-Debatable Topic in Online Discussion
Gabriele Bechtel (2010). *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction (pp. 852-865).*
www.irma-international.org/chapter/tracing-non-debatable-topic-online/42822

A Digital Forensic Analysis of Advance Fee Fraud (419 Scams)
Christine I. Ofulue (2010). *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction (pp. 296-317).*
www.irma-international.org/chapter/digital-forensic-analysis-advance-fee/42787

The Web 2.0 Mandate for a Transition from Webmaster to Wiki Master
Roger W. McHaney (2014). *Cyber Behavior: Concepts, Methodologies, Tools, and Applications (pp. 1441-1461).*
www.irma-international.org/chapter/the-web-20-mandate-for-a-transition-from-webmaster-to-wiki-master/107796

Cyberloafing in the Workplace
Christine A. Henleand Uma Kedharnath (2012). *Encyclopedia of Cyber Behavior (pp. 560-573).*
www.irma-international.org/chapter/cyberloafing-workplace/64785