H-Net Reviews
in the Humanities & Social Sciences

Gabriel Weimann. *Terrorism in Cyberspace: The Next Generation.* Washington, DC: Woodrow Wilson Center Press. New York: Columbia University Press, 2015. 344 pp. $30.00, paper, ISBN 978-0-231-70449-6.

Reviewed by David R. Mair

Published on H-Diplo (April, 2016)

Commissioned by Seth Offenbach (Bronx Community College, The City University of New York)

Gabriel Weimann has been at the forefront of online-terrorism research since the early 2000s when he first investigated the main functions through which terrorists utilize the Internet for their core operational and logistical goals.[1] As such, his new book has been eagerly anticipated by those within the online-terrorism research community.

In his latest work, ***Terrorism in Cyberspace: The Next Generation***, Weimann attempts to explain how terrorism has evolved in cyberspace over the course of the past decade through analysis of a database of terrorist websites that he has curated since the late 1990s. With data collection spanning from this date until October 2013, Weimann has collected, stored, and categorized over 9,600 terrorist websites of groups that appear on the United States Department of State *List of Designated Foreign Terrorist Organizations.*[2]

Weimann's goal is to answer three research questions. First, what are the new faces of online terrorism; second, what can be expected in the near future; and third, how can we counter these threats? His book is therefore separated into three sections: "Terrorism Enters Cyberspace," "Emerging Trends," and "Future Threats and Challenges." Underpinning these research questions is a desire to provide empirical evidence for his arguments. In his introduction, Weimann quotes William McCants in testimony before the House Homeland Security Subcommittee on Counterterrorism and Intelligence: "There is little research to go on, which is striking given how data-rich the Internet is.... This sort of baseline quantitative research barely exists at the moment" (pp. 3-4). This review will seek to evaluate ***Terrorism in Cyberspace*** by assessing how well Weimann answers each research question in the corresponding section of his book. It will conclude with an assessment of the strengths and weaknesses of the book and its contribution to the literature.

Weimann begins, as would be expected, with an overview of how terrorist groups use the Internet. This is not new ground for Weimann, having written one of the seminal pieces of literature on the topic: “www.terror.net: How Modern Terrorism Uses the Internet.” Weimann’s assessment of the core functions achieved by terrorist use of cyberspace has not changed a great deal in the past decade. Weimann cites the contemporary uses as psychological warfare, propaganda, online indoctrination, recruitment and mobilization, data mining, virtual training, cyberplanning and coordination, and fund-raising. The categories are broadly similar to those identified in his earlier work, which included psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, sharing information, and planning and coordination.[3]Weimann appears to argue, then, that while the sophistication of terrorists’ use of the Internet may have increased and evolved, the overarching functions have not. This concept is supported by online terrorism researchers such as Stuart Macdonald and David Mair, and Dorothy Denning.[4]

When discussing the new threats emerging from terrorists’ use of the internet, Weimann makes some bold claims. In chapter 8, “Cyberterrorism,” Weimann claims that cyberattacks are a promising tool for terrorists, citing the low entry costs, the anonymous and remote nature of cyberattacks, and the vulnerability of and increased damage to targets (pp. 152-154). Interestingly, Weimann is able to produce evidence of terrorist actors utilizing cyberattacks against US financial targets and other “Zionist-Crusaders” (p. 160). This is in stark contrast to other researchers, such as Thomas Rid and Maura Conway, who have argued that al-Qaeda and its ilk were not in a position to use cyber weapons as they lacked the technical sophistication and motivation to invest in offensive cyber capabilities.[5] Weimann challenges this claim, noting that al-Qaeda has included cyberterrorist attacks in aspirational manuals and communiques, and pointing out the technical sophistication of the various websites hosted by jihadist groups. Here Weimann makes a strong and convincing case for the threat posed by cyberterrorism.

The final research question and section of *Terrorism in Cyberspace* deals with issues of response. Here Weimann sets himself the task of assessing the best ways of dealing with terrorism online. This is a fairly large challenge, as Weimann notes that there is currently no set strategy in place to counter terrorist narratives online. Utilizing the M.U.D. model (monitoring, using, disrupting), however, Weimann argues that online terrorist content can be utilized by counterterrorism agencies to identify intelligence sources, discover key distribution nodes and inject misinformation, launch offensive cyber capabilities against identified targets, or assist in the production of credible counternarratives that turn people away from violent engagement. The creation of effective counternarratives necessitates a strong understanding of the original terrorist narrative, which Weimann demonstrates effectively. He also uses empirical research to suggest that counterterrorism efforts focus on four topics: undermining terrorist leadership, highlighting civilian suffering, highlighting crimes committed by terrorist actors, and focusing on the hardships of life as an active terrorist. Contemporary researchers and counterextremism practitioners, such as Anne Aly, agree with this approach, stating that moral engagement with those engaged in violent extremism is a key part of creating effective counternarratives.[6] Importantly, Weimann also states that the vehicle of communication is key when delivering counternarratives, as governments are not seen as credible. Weimann insists that former terrorists or family members engage in counternarrative projects instead.

Ultimately, the main criticism to be leveled at this text is that despite its stated intention to contribute to the literature empirically, there is no real attempt to do so. Examples and case studies are often presented to illustrate Weimann’s point, but there is no sense of the quantitative background to Weimann's work. The evidence base for this book is a dataset of over 9,600 websites of designated terrorist organizations. However, at no point does Weimann break down this figure into subcategories and variables. It is here that the reviewer believes that Weimann has missed a valuable opportunity to contribute to the literature through an empirical understanding of terrorists' online content.

For example, despite indications that the dataset holds information on terrorist entities from across the globe and from a wide variety of ideological backgrounds (pp. 22-23), the type of terrorist actor depicted in the examples given throughout the text is almost always jihadist in nature. This is explained somewhat when Weimann indicates that most contemporary terrorist websites belong to jihadist terrorist organizations (p. 36). However, this does not mean that other terrorist actors do not use the iInternet or that their Internet usage is of lesser interest. In fact, throughout the book, the author cites only two examples of how non-jihadi terrorists (in both cases extreme right-wing terrorists) use the Internet (pp. 65-66). A breakdown of the types of terrorist actor featured in Weimann's database along with more examples of different terrorist actors would have provided Weimann with a stronger argument for how all terrorist entities use the Internet and would have allowed him to respond to calls to fill a gap in the literature from writers such as Conway (p. 13) who have argued that combining analysis of different terrorist actors will provide a better landscape of terrorists' use of cyberspace.[7]

Similarly, Weimann does not provide information on the function of each website. While the ways in which terrorists use the Internet are explained in great detail, Weimann does not use his database to show empircally how terrorists use websites and the latter's function as an online platform. For example, how many of the websites in Weimann's dataset contain a forum or a discussion board? How many acted as distributors for terrorist publications or speeches? How many engaged in the narrowcasting approach wherein specific information is presented to specific populations to engender a specific response? A database of this size would have provided for a very strong analysis of terrorists' online platforms.

Finally, while Weimann mentions responding to terrorist use of the Internet through Internet referral units (p. 242), he does not discuss the ultimate impact of shutting down terrorist websites. Speaking in December 2015, Earl Howe revealed that since its creation in 2010, the UK Counter Terrorism Internet Referral Unit (CTIRU) has removed over 120,000 pieces of terrorist content from the Internet.[8] As he is an expert on tracking terrorist websites, it would have been worthwhile hearing Weimann's thoughts on the effectiveness of these techniques.

Where Weimann should be congratulated is for his mastery of the online *jihadisphere*. Weimann's historical and contemporary understanding of al-Qaeda, Hamas, and Hezbollah is excellent and he is able to produce key summaries and examples of each group, their operatives, and the ways in which they have utilized the Internet to engage in violent extremism. Of special note is the chapter on online debates where Weimann discusses the various diplomatic incidents that have occurred online within and between competing terrorist entities. Weimann is a confident communicator and his concise and logical arguments build a strong case for the continued monitoring and combatting of terrorists' use of the Internet. While Weimann's text does not discuss the Islamic State--who rose to power following the conclusion of his data collection--his book remains an excellent analysis of jihadists' online content and is a very good contribution to the literature on terrorism in cyberspace.

Notes

[1]. Gabriel Weimann, “www.terror.net: How Modern Terrorists Use the Internet,” United States Institute for Peace, ***Special Report*** 116 (March 2004), http://www.usip.org/sites/default/files/sr116.pdf.

[2]. United States Department of State, Designated Foreign Terrorist Organizations, http://www.state.gov/j/ct/rls/other/des/123085.htm.

[3]. Weimann, ibid, 5-11.

[4]. Stuart Macdonald and David Mair, “Terrorism Online: A New Strategic Environment” in ***Terrorism Online: Politics, Law and Technology,*** ed. Lee Jarvis, Stuart Macdonald, and Thomas Chen (Oxon: Routledge, 2015), 10-34; and Dorothy Denning, “Terror’s Wed: How the Internet is Transforming Terrorism,” in ***Handbook on Internet Crime***, ed. Madjid Yar and Yvonne Jewkes (Devon: Willan Publishing, 2010), 194-213.

[5]. Thomas Rid, “Al-Qaeda lacks expertise for cyberwar, expert tells MPs,” March 14, 2013, BBC News website, http://www.bbc.co.uk/news/uk-politics-21769078; Maura Conway, “Reality Check: Assessing the (Un)likelihood of Cyberterrorism,” in ***Cyberterrorism: Understanding, Assessment and Response***, ed. Thomas Chen, Lee Jarvis, and Stuart Macdonald (New York: Springer, 2012), 103-122.

[6]. Anne Aly, Elisabeth Taylor, and Saul Karnovsky, “Moral Disengagement and Building Resilience to Violent Extremism: An Education Intervention,” ***Studies in Conflict and Terrorism***, 37 (2014): 369-385.

[7]. Maura Conway, “From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Milieu” (2012), http://www.isodarco.it/courses/andalo12/doc/Zarqawi%20to%20Awlaki_V2.pdf, 13.

[8]. HL Deb, 2 December 2015 c1189.