III. Book Reviews

Gabriel Weimann, *"Terrorism in Cyberspace: The Next Generation"*

(New York, NY: Columbia University Press/Washington, DC: Woodrow Wilson Center Press, 2015), 313 pp., US $ 90.00 [Hardcover], US $ 30.00 [Paperback], ISBN: 978-0-231704496.

Reviewed by Joshua Sinai

In the United States, Canada and Western Europe, dozens of al Qaida, al Shabaab- and ISIS-related terrorist-related plots have been thwarted by government counterterrorism agencies through electronic surveillance of terrorist operatives' suspicious activities on the Internet. While their activities were likely also monitored "on the ground," the fact that terrorists of all extremist ideological and religious types are so reliant on using their computers and smartphones to access the Internet for their communications, cyberspace has become a necessary focus of operations for counterterrorism agencies.

Tracking the suspicious activities of potential terrorists in cyberspace is so crucial, in fact, that in certain cases where terrorists succeeded in carrying out their attacks, such as Major Nidal Hassan's murderous rampage at Fort Hood and the Tsarnaev brothers' bombing of the Boston Marathon, electronic data had existed about their suspicious online activities, but counterterrorism agencies had failed to 'connect the dots' to appreciate the significance of such evidence in their possession prior to these incidents.

Because it is obvious to counterterrorism professionals from intelligence and law enforcement that it is crucial to electronically monitor such suspicious activities (with full legal compliance), it has been somewhat surprising to see the recent controversy in the United States Congress over reauthorization of electronic surveillance operations under the Patriot Act [which was passed in a modified form in early June]. For this reason, among others, we are fortunate to have Gabriel Weimann's "Terrorism in Cyberspace: The Next Generation," as an authoritative account of the ways in which terrorists operate in cyberspace. Dr. Weimann (whom I know and, for full disclosure, also wrote the blurb on the book's back cover), is Professor of Communications at the University of Haifa, Israel, where he leads a research program that tracks terrorist activities on the Internet. He also is the author of the landmark book *Terror on the Internet: The New Arena, The New Challenges* (Washington, DC: USIP Press, 2006).

In his new book, Gabriel Weimann addresses the following questions: how are terrorists exploiting the Internet, what new trends in cyberspace can be expected in the future, how can terrorist operations on the Internet be effectively countered, and how can we balance the need for security while protecting civil liberties.

Prof. Weimann explains that terrorist groups–and lone wolves–view the Internet as an ideal arena to exploit for their communications, propaganda, training, fundraising, and for mobilizing support for their violent activities because of its ease of access from anywhere around the world, "lack of regulation, vast potential audiences, fast flow of information," and, most importantly, the anonymity to post "their extremist beliefs and values" and then "disappear into the dark." (p. 21). Terrorists and their supporters exploit the Internet's websites, email, chatrooms, virtual message boards, mobile phones, Google Earth, YouTube and other online video sharing sites, as well as social networking sites such as Facebook and Twitter. Such exploitation, however, is not being conducted openly, as their tech-savvy operatives often use encryption tools and anonymizing software to make it difficult for counterterrorism agencies to identify "the originator, recipient, or content of terrorist online communications." (p. 23)

Dr. Weimann identifies three new trends in Internet exploitation: narrowcasting (targeting propaganda and recruitment messaging to narrow audiences that are deemed to be especially susceptible, such as children, women, lone wolves, and diaspora communities), encouraging the proliferation of lone wolf adherents, such as Major Nidal Hassan, and advancing cyberterrorism.

The proliferation of lone wolves is especially worrisome, according to the author, because "they are extremely difficult to detect and to defend against." (p. 66) Nevertheless, they are not undetectable to counterterrorism agencies because they must still "connect, communicate, and share information, know-how, and guidance — all online — on the 'dark web.'" (p. 66)

Cyberterrorism is the most threatening of the trends, according to Gabriel Weimann, because they would be able to use their "computer network devices to sabotage critical national infrastructures such as energy, transportation, or government operations." (p. 150) Dr. Weimann warns that terrorists are keen to develop a cyber-warfare capability, with the possibility of "money, ideology, religion, and blackmail" being used to recruit such "cybersavvy specialists" in the future.

How can terrorist exploitation of cyberspace be countered and defeated? While the Internet and its online platforms, as Dr. Weimann points out, provide terrorists with "anonymity, low barriers to publication, and low costs of publishing and managing content," (p. 150) at the same time they also provide counterterrorism agencies with the capability to damage and block them. Under what Dr. Weimann terms the "MUD" model (monitoring, using, and disrupting), he recommends covertly tracking their activities in order to gain information about their strategies, motivations, internal debates and associations, while disrupting them with 'hard' power cyber-weapons to spread viruses and worms against their websites. These would be accompanied by 'soft' power elements that conduct psychological operations to discredit their extremist propaganda and offer constructive alternatives to resorting to terrorism..

In light of the still continuing controversies over the electronic surveillance provisions of the Patriot Act, the book's final chapter, "Challenging Civil Liberties," is particularly valuable in discussing the challenges presented by the need to preserve civil liberties when countering online terrorist activities. Dr. Weimann cites the impact of Edward Snowden's illicit revelations of the U.S. government's counter-online surveillance measures and proposes a set of guidelines to regulate governmental online surveillance.

"Terrorism in Cyberspace" is a timely and indispensable resource for all those concerned about effectively countering terrorists' exploitation of the Internet's and the dark elements that can reside there.

N.B.:*This is an expanded version of a review that originally appeared in The Washington Times on June 2, 2015. Reprinted with permission.*

About the Reviewer: **Dr. Joshua Sinai** *is the Book Reviews Editor of 'Perspectives on Terrorism'. He can be reached at: Joshua.sinai@comcast.net.*