
Mark J. Roberts

Follow this and additional works at: https://digitalcommons.usf.edu/jss
pp. 103-105

Recommended Citation
DOI: http://dx.doi.org/10.5038/1944-0472.9.3.1553
Available at: https://digitalcommons.usf.edu/jss/vol9/iss3/8

This Book Review is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact scholarcommons@usf.edu.

Violent Extremism Online examines how terrorists use the Internet to disseminate propaganda and radicalize new recruits. In this anthology encompassing various topics, the authors sport a mix of academia and practical experience, all seeking to examine, understand, and offer solutions for society to cope with an ever-changing phenomenon.

The Internet is ubiquitous. In times past, letters, newspapers, television, and cassette tapes propagated ideas, which took time to produce and disseminate. In an age of instant gratification, terrorists use the Internet to influence and radicalize potential recruits susceptible to their message. They also use it to communicate with colleagues and intended audiences to influence their thinking and perceptions in real time. As Canadian savant Marshall McLuhan observed over half a century ago, “the medium is the message.”

All of this is unplowed ground as terrorists use the Internet to transmit and reshape thousands of messages, creating a relationship between the sender, the message, and the recipient. In some cases, terrorists have live tweeted attacks in progress via video streaming.

Examining “Electronic Jihad” (E-Jihad), one author examines how terrorists use the Internet medium to spread their message. He specifically mentioned how al-Qa’ida (AQ) in the Arabian Peninsula’s (AQAP) late leader Anwar Awlaki used the Internet to spread AQAP’s message in order to shape values, attitudes, and beliefs. Awlaki issued propaganda videos and the online magazine Inspire to recruit, influence, and train new members. As an Internet mujahedin, Awlaki saved a fortune on printing costs as he developed a virtual community of interest with global reach.

Electronic Jihad has three elements: Online libraries, jihadist websites with tracts and sermons from extremist preachers, and myriad discussion fora for radical discourse. Using these platforms, Awlaki raised from afar a crop of Homegrown Violent Extremists (HVEs) in the United States more cheaply, more efficiently, and more rapidly than an in-person preacher might have.
AQ, AQAP, and the Islamic State (IS) have used Electronic Jihad to promote radical agendas, spread anti-Western propaganda, raise funds, attract new members, conduct psychological operations, mobilize jihadis, instigate anti-Western sentiment, wage cyber war, and train fighters. Examining charismatic preachers’ use of the Internet, another author outlines how these radicals under the guise of holy men have drawn people to fight for IS in Syria and Iraq. Charismatic preachers “awaken” people by pushing a victimization narrative to non-Arabic speakers, exploiting their ignorance. These preachers justify violence by appealing to a “tradition” of which the converts have no knowledge. Anwar Awlaki propagated numerous English language jihadi videos on the Internet. He was able to recruit vulnerable, impressionable people looking for a sense of purpose and belonging. Sending a focused the message to the intended audience, the preachers advocate jihad as an individual duty to defend an Islam that is under attack.

A different author investigates why terrorists migrate to social media. As a recently new phenomenon, social media is undiscovered country. It is also inexpensive, easy to access, and instantaneous. In this new medium, lone wolves can be radicalized, recruited, and trained on-line. This includes resources such as virtual libraries, videos, and bomb making instruction manuals. AQAP’s Inspire magazine advocates and utilizes Open Source Jihad, making theoretical and practical materials available worldwide to would be terrorists in order to carry out attacks on the West. In the face of aggressive on-line violent extremist efforts, U.S. counterterrorism initiatives have lagged far behind.

Another author describes how during an attack on a shopping mall in Kenya, terrorists tweeted the attack live. In so doing, they engaged in strategic communications purveying a message of violence aimed at the millions of people worldwide watching on the Internet, not just the victims undergoing the live event itself. In this sense, terrorism became theater intended for the Kenyan people, the Kenyan government, the West, the media, terrorist sympathizers, and emergency responders. The terrorists chose a high-profile target to generate maximum mass media exposure.

Yet another author dissects how violent extremist postings online have included videos of beheadings, footage of close range shootings, bomb-making guides, combat literature, and speeches or sermons by terrorist leaders. These and other postings have been used by governments as legal evidence to prosecute terrorist cases. In some instances, this training and
motivation material is used by prosecutors to prove intent to commit acts of terror.

One of the authors breaks down how violent jihadist preachers seek to manipulate their audiences via targeted messaging intended to raise money, recruit, indoctrinate, and give them a cause to rally around. By focusing on managing the message, the violent jihadist preachers make their audience active participants in the process and co-conspirators for their cause. The preachers use a multi-staged approach to bring in their new recruits: Searching, seduction, captivation, persuasion, and operative. Each stage has a precise choreography to gradually, methodically bring the recruit into the fold. The potential recruits can be categorized as seekers, lurkers, inquirers, advocates, or activators. A different strategy is used for each category to bring the recruit into and through the multi-staged approach.

One of the authors compares and contrast how AQAP and IS appeal to their intended audiences. The author describes AQAP’s content as “remote, undirected and boring,” while contrasting IS’ approach as “familiar, interactive and ‘cool’” that relates more profoundly with modern youth online culture (p. 134).

Another author discusses U.S. online counter narrative initiatives through the State Department. This initiative monitors and evaluates terrorist narratives, counterterrorism initiatives and communications strategies, and identifying terrorist trends to attempt to get ahead of them in order to rebut their messaging to worldwide audiences.

The book’s essays are well written, thoughtful, and practical. The book has a wide range of utility for both undergraduate and graduate students, policy and strategy practitioners, and the layperson interested in learning how violent Islamic extremists use the Internet to manipulate and influence others. Overall, the book makes a valuable contribution to the body of knowledge on the topic.

*Mark J. Roberts is a terrorism subject matter expert.*