JOURNAL OF COMMUNICATION

Journal of Communication ISSN 0021-9916

Book Reviews

Terrorism in Cyberspace: The Next Generation

Gabriel Weimann

Columbia University Press, Kindle Edition, 2015

Gabriel Weimann's *Terrorism in Cyberspace: The Next Generation* is a thorough update to his 2006 book *Terror on the Internet*. It summarizes Weimann's work since 2006, and the work of some other major voices in the field. In a review of the contents of over 10,000 terrorist websites, Weimann and his team analyze the use of networked communications technology. The text draws comparisons between current terrorist practices and marketing, political organizing, and hacktivist practice. While the book presents a comprehensive review of an area of current security and terror studies, it is unfortunately hamstrung by apparent prejudices as to who counts as a terrorist and a marked lack of fluency in the technological concepts at work.

Terrorism in Cyberspace is unequivocally focused on Islamic terrorist groups. There is no substantial coverage of other ideologically motivated terror groups. A particularly notable lacunae is White supremacist groups in North America, whose use of message boards, forums, and other networked communications technologies has been thoroughly researched. Besides a handful of offhand citations, right-wing extremist terror actors in North America and Europe are wholly uncovered in this text. Weimann notes in his introduction that he uses the U.S. Department of State's list of foreign terror organizations to establish his research scope. He does not further justify, either theoretically or practically, his exclusion of non-Islamic terror actors from his analysis, nor does he acknowledge this limitation in his project's scope. We are left with a text that declares itself to be a general analysis, but that in actuality is quite limited.

Perhaps unsurprisingly, Weimann cites uncritically a number of reports produced by either U.S. governmental agencies or DC-based think tanks such as MEMRI or the Middle East Policy Council. This in part explains this text's marked pro-United States, progovernment perspective. This comes out most clearly in Weimann's chapter describing the tradeoffs necessary between civil liberties and security in the fight against terror. Here Weimann interprets a number of *Washington Post*, ABC, and *USA Today* polls to claim that "in the public's view, the optimal level of civil liberties, in practice, is not necessarily always the fullest extent of those liberties: Americans are willing to trade a degree of civil liberty for other valued benefits, such as the prevention of terrorism" (pp. 4347–4349). He goes further in arguing that "We know that the American public supports the monitoring of the Internet, including private e-mail traffic, but as in the case of TSA measures this

acceptance relies on known procedures, known agents, and agreed-upon limits" (pp. 4379–4381). These statements reflect a generous interpretation of both the studies cited and of the current opinion regarding the massive surveillance regime uncovered by Edward Snowden and post-9/11 transportation security and communication privacy.

Weimann takes a curious approach to the internet and networked communication devices, describing them more as a collection of discrete tools than as environments and theaters of action. This leads to him devoting substantial time to, say, the description of "cyber-fatwas," Islamic religious rulings notable, apparently, for being distributed online. Noting mostly that online distribution makes such teachings more accessible than previously possible, Weimann does not deliver a cogent argument for why accessibility, in and of itself, alters the form of the fatwa or otherwise justifies the special "cyber" designation. The "internet-as-tool" perspective lends the observations on the use of networked communications technologies by terrorist actors a freighted intentionality and a determinist slant that ignores the ubiquity of the technologies and practices in question. That these actors make use of these technologies for political and ideological purposes is presented as an exotic nightmare scenario, rather than an expected outcome that could have been predicted based on similar uses of the same technology by other ideologically motivated political actors, including non-Islamic terror populations. Overall, the text seems preoccupied with the fact that Islamic terrorist organizations are made up of people who, like most other people these days, use the internet as part of their daily lives. Weimann's book makes much of their use of e-mail, message boards, websites, social networks, mobile phones, and other common communications technologies, but despite Weimann's occasionally dramatic language, the findings presented here should not be surprising to anyone who has studied the social use of networked communication technologies and the modern web.

The text contains a number of technical glosses which, while not rising to the level of errors, indicate a tolerance for a certain amount of sloppiness with specifics. The book describes Tor as a "proxy service," which it technically is not. Weimann devotes an entire subsection to "data mining," which describes the use of tools like Google Earth and publicly accessible databases like the Wikileaks Cablegate trove by terrorist actors, without ever clearly distinguishing that type of basic online research from sophisticated tools like the NSA's Boundless Informant and XKeystore, both of which are also referred to as "data mining" tools. Terrorist organizations are said to "capture information about the users who browse their websites" (pp. 579–580) but absolutely no information is given about how this is done. Is it through the use of cookies? Ad-trackers? Newsletter subscriptions? Geocities-style guestbooks? The reader is left to guess for themselves, and probably assume the worst.

The book frequently uses terms like "cyberattacks" and "hacking" with little further explanation, despite the fact that these are notoriously underdefined terms and can be used to describe a

wide manner of sins. Weimann cites a 2013 *Daily Telegraph* article to support his claim that "In 2012 alone, NATO suffered around 2,500 cyberattacks on its networks, according to the alliance's secretary general" (Weimann 3051–3052) without noting what these "attacks" were and what percentage were legitimate, malevolent threats to the integrity of NATO networks, as opposed to any number of the automated spiders, bots, and port scanners which are common on today's open web. Weimann lumps the August 2013 URL-jacking episode, wherein the URLs of *The New York Times* and several other major media sites were temporarily redirected, under the label of "terrorist hacker" attacks.

In the chapter on "cyberterrorism," Weimann makes particularly free use of inflammatory hypotheticals, framed as though they are an immanent possibility: "Consider the following comparative scenario: A suicide bomber can enter a bus, and if successful can manage to kill all the passengers on the bus and possibly harm bystanders and others in the immediate area. With cyberattacks, a terrorist can take control of traffic lights in a certain area, the air traffic control systems of a busy airport, or the computers controlling the underground transport system in a major city—and could cause hundreds or even thousands of fatalities over a much wider area" (Weimann 2884–2887). Despite alarmist news reporting and the fevered dreams of Hollywood filmmakers, there has never been a documented incident of hackers, terroristic or otherwise, "taking over" air traffic control systems, subway control systems, or traffic lights outside of controlled experiments. No one has died from an act of "cyber terror."

With section titles like "What is Social Media?" it is apparent that the intended audience for this text is not anticipated to be particularly technologically sophisticated. As such, Weimann's glosses and overuses of intentionally alarming hypotheticals and terms like "cyberattack," "cyberterrorism," "hack," "cyber Pearl Harbor," and "cyber 9/11" are especially problematic. Weimann's handling of these concepts is unnuanced and alarmist. This, combined with his tunnel-vision focus on Islamic terror actors to the exclusion of all others and his apparent faith in the justified trammeling of a lot of civil liberties in exchange for a little safety, leaves *Terrorism in Cyberspace* an off-balance, but not entirely unexpected book. The text reflects current prejudices about who is called a terrorist, stokes preconceptions regarding the apocalyptic potential of networked communications technologies, and with a recommendation for a surveilled and censored internet that might be safe from the "abuses" of terrorist actors, but which would be effectively denuded of those creative aspects which inspired such defensive zeal in the first place.

Molly Sauter
McGill University