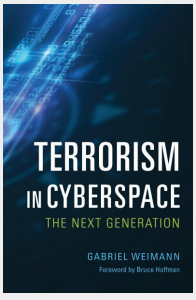
Terrorism in Cyberspace:
The Next Generation

By Gabriel Weimann

Washington, D.C.: Woodrow Wilson Centre Press & Columbia University Press, 2015, viii + 296 pages, $30,
ISBN: 9780231704496.

Reviewed by Hacı Mehmet BOYRAZ



Recently, there has been a growing body of literature on the multifaceted relationship between terrorism and cyberspace in different contexts. *Terrorism in Cyberspace*, which emerged out of about 15-years observation of about 10,000 terrorist websites, in addition to innumerable social media platforms, focuses on the past, present and future of terrorism in cyberspace. The author, in all parts of the book, tries to present readers with an understanding of what terrorist groups have been doing in cyberspace. The book fills a research gap by answering the following three research questions: what are the new faces of online terrorism; what can be expected in the near future; how can we counter new trends of terrorism in cyberspace? To address these questions, the book is divided into three main parts.

In the first part of the book, entitled *Terrorism Enters Cyberspace,* which consists of only one chapter, Weimann specifically examines how terrorist groups and organizations have enhanced their communication strategies. According to him, the growing presence of modern terrorism in cyberspace is at the nexus of two key trends: the democratization of communications driven by user-generated content on the internet, and modern terrorists' growing awareness of the potential for using the internet as a tool for their purposes. Those factors make cyberspace a favorite tool for terrorists. Weimann also argues that terrorists use cyberspace mostly for propaganda and communication purposes rather than attacking purposes, but, as he will later discuss, cyberterrorism is certainly on the terrorists' agenda and is likely to become their new mode of operation.

In the second part of the book, entitled *Emerging Trends* which consists of six chapters, Weimann focuses on six emerging trends of terrorism: narrowcasting, lone wolves, e-marketing terror, online debates, online fatwas, and terror on social media. Among those, he gives special importance to the first two. Narrowcasting is broadly defined as the dissemination of information to a narrow audience, not to the broader public at large. The terrorist groups use narrowcasting to appeal, seduce and recruit targeted subpopulations, including members of so-called diaspora communities or potential supporters living overseas in Western societies. At that point, Weimann presents Hezbollah's online gaming "Special Force", which targets and allows children to become warriors in a terrorist campaign against Israel. He discusses that the success of ISIS and other similar groups in recruiting hundreds of Europeans and North Americans to come and fight in Iraq and Syria is an ample evidence of the success of this narrowcasting tactic. On the other hand, lone-wolf terrorism is the fastest grow-

ing form of terrorism. It is the attack by individual terrorists who are not members of any terrorist organization. As they are extremely difficult to detect and to defend against, the lone-wolves are challenging the police and intelligence community.

In the third part of the book, entitled *Future Threats and Challenges,* and which consists of four chapters, Weimann analyzes the future threats and challenges related to terrorists' use of cyberspace. According to him, among the many future threats, cyberterrorism is the most threatening, because terrorists would be able to use computer network devices to sabotage critical national infrastructures such as energy, transportation and government operations. Weimann warns the public and state institutions that terrorists are keen to develop a cyberwarfare capacity with the possibility of money, ideology, religion and blackmail being used to recruit cyber-savvy specialists in the future. In this chapter, Weimann points out that countering terrorist usage of the internet to further ideological agendas requires a strategic, government-wide approach to designing and implementing policies to win the war of ideas.

In the last chapter of the third part, "Challenging Civil Liberties," Weimann addresses the challenges presented by the need to preserve civil liberties when countering online terrorist activities. He argues that there are two concerns regarding the new digital war on terrorism. The first concern is that the new surveillance measures may improve security but harm civil liberties. The second concern relates to the very essence of what we mean today by privacy, and reflects a more general worry about the "retreat of privacy" resulting from the use of many high-tech surveillance tools. In such a situation, he advises that individuals have to make some important decisions about how to protect themselves while upholding their civil liberties and the privacy protections that western ideals and constitutions require.

The most fundamental critique of the book is based on the examples that Weimann dealed with. He focuses on radical Islamic groups such as al-Qaeda to the extent that the other radical groups are never discussed in the analysis. In my opinion, this proves that the book is based on a group of selective readings by the author. The second critique is based on the methodology of the book. The author states that his main data are the terrorist websites and online platforms that his research team has been monitoring for more than 15-years. However, he does not give a package of necessary information about the methodology of collecting and interpreting of those data. The final critique is that a detailed chapter of definitions based on cyber issues in the book would have been of enormous help to non-specialists.

Overall, *Terrorism in Cyberspace* is an exceptional book that covers a broad spectrum of issues and challenges pertaining to terrorism in cyberspace. I would like to recommend this book as a useful tool for scholars and readers who are interested in the issues of terrorism in cyberspace.