BOOK REVIEW

Terror on the Internet: The New Arena, the New Challenges, by Gabriel Weimann

WASHINGTON, DC: UNITED STATES INSTITUTE OF PEACE PRESS, 2006,
325 PAGES

Eva Moya

What are the opportunities for terrorist groups on the Internet? What are the possible consequences of an attack on the net? Which are the most common types of attack? Could a virtual attack combined with a physical attack be possible? Which are the ethical and legal limits when taking action on the Internet in order to protect the safety of the citizens? Gabriel Weimann, an eminent communication and terrorism analyst and professor of Communications at Haifa University in Israel, tackles the basic aspects of the issue of civil rights (such as privacy or freedom of expression) and public safety against possible cyberthreats.

Terror on the Internet offers an excellent overview of the origin and evolution of the scenario of cyberterrorism from the various approaches that shape it. It also highlights the interests of direct and indirect actors involved in it.

This book is relevant for professionals in the fields of counterterrorism and security on the Internet, since it expands the knowledge of these areas and goes deeper into the actual use of this technology in this area. Finally, it may be very useful as a source of suggestions for prospective analysis or for establishing possible tendencies in the evolution of this threat and how to counter it.

To respond these questions, Weimann comes across with valuable examples, gathered from the dark side of the net during his eight-year research, as well as reflections by several media, such as the *Washington Post* or the *New York Times*, and the work of prestigious professionals such as Paul Eedle or Dorothy Denning. He also compiles the arguments of organizations linked to the defense of civil rights, such as the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC).

He also completes his research with an analysis of some of the government actions carried out against this threat, mainly from the

United States, after the 9/11 attacks. These actions, which governments claim were necessary, have received great criticism due to the possibility of violating fundamental civil rights, notably those related to freedom in using the Internet.

In his analysis, the author reflects upon the difference between *cyberterrorism*, *cybercrime*, and *hacktivism*, terms that can be easily misleading nowadays, since the Internet is merely a medium, a tool or a channel that can be used in different ways. Therefore, to agree on a definition, should we focus on the reasons that induce the act, or should we reflect on the consequences from that? This is a necessary distinction to make in order to properly evaluate the severity of the terrorist cyberthreat and to determine whether certain actions already implemented to counter it are justified. Anyway, whether or not we accept the definitions proposed, at the end of the book, Weimann includes a listing of foreign terrorist organizations considered as such by the U.S. Department of State from 1997 until 2004 (an updated list is available at www.state.gove/j/ct/rls/other/des/123085.htm).

Terror on the Internet explains how the Internet scenario has reached a bigger relevance in our society in recent years, while different terrorist organizations take advantage of the Internet resources available (email or website) for their own goals: obtaining information, distributing propaganda, recruiting sympathizers, communicating with other members or other terrorist groups, raising funds, and performing Denial of Service (DoS) attacks. In some of the case studies, the author explains how these organizations develop a systematic campaign of communicating threats in order to spread a message of terror throughout the society, such as, for example, the threats spread by the global Islamic media published on Yahoo!—"Groups or the constant cyber-propaganda of Al Qaeda." These issues remind us of investigations carried out in Spain around concepts such as "Jihad 2.0," which has been thoroughly studied by Professor Manuel Torres Soriano (Spain, Universidad Pablo Olavide).

Meanwhile, from the point of view of counterterrorism, the author expresses the possibility that some of the actions implemented by the U.S. government to protect cyberspace could be very costly in terms of limiting civil rights; for instance, the USA PATRIOT Act, including its 2003 revision (called PATRIOT II), was criticized by various organizations, including the ACLU and public authorities such as Audrey B. Collins, judge of the Federal District Court, who went on to state that "a provision in the law banning certain types of support for terrorist groups was so vague that it risked running afoul of the First Amendment." One example provided is when documents were removed from several websites for being considered information that could pose a risk to security.

One of the activities against terrorism on the net is based on the use of advanced monitoring or tracking technology, which could violate fundamental rights such as privacy. To illustrate the situation, Weimann comments on the reactions to the FBI's use of some tools such as Carnivore, which can access all email messages and traffic from an IP address, as well as finding out who connects to a webpage or FTP server. Another example is Magic Lantern, a tool that, installed in the target computer, can record all keystrokes and obtain codes and passwords. Organizations such as EPIC are speaking about how important it is to introduce certain safeguards in the use of these kinds of tools, such as obtaining a wiretap order from a U.S. judge.

In the war against terrorism, not only government agents are involved but there are also private initiatives by some so-called virtual warriors, such as Abraham Kandel, executive director of the National Institute for Systems Test and Productivity in the United States, who devote part of their time to monitoring traffic online in order to detect sensitive emails that can lead them to terrorists.

Finally, Weimann pays attention to the effects and impact of media on public opinion, and he asks himself to what extent this could be amplifying the severity of the threat, or warning about a reality that demands our full attention.

The opinions expressed in this review do not imply endorsement by any government institution.

Eva Moya works at Intelligence Services and Democratic Systems (URJC) and at the Juan Velázquez de Velasco Institute for Research on Intelligence for the Security and Defense (Carlos III) in Spain. She was awarded a Master Intelligence Analysis degree from Rey Juan Carlos University (Spain).