

The Economics of Peace and Security Journal

© www.epsjournal.org.uk, ISSN 1749-852X

Book Review

Weimann, Gabriel. 2006. *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press. xv + 309 pp. ISBN 1-929223-71-4 (hb). Price: \$24.95.

by Bjørn Møller (31 March 2008)

Starting with the observation that many designated terrorist organizations maintain web sites, this book surveys the importance of the internet for (mainly international) terrorism today and in the near future. Web sites can be used to propagate the ideology of the group in question. They also facilitate recruitment and fund raising, and the web can be used to disseminate messages intended to cause panic, i.e., the very same kind of terror which has given terrorism its name. The web can thus serve as a weapons in psychological warfare, used not merely by terrorists, but also by their adversaries. To prevent such use has proved almost impossible.

The author mentions the rather surprising fact that 76 percent of all Islamist and Jihadist web sites are actually hosted by American companies (p. 67), including one belonging to Hamas (p. 86). Based on an inventory of terrorist web sites and an analysis of their contents, the author analyzes their implicit messages with the help of Bandura's theory of "selective moral disengagement," demonstrating how they use methods such as displacement and diffusion of responsibility and dehumanization of the targets.

The web is also an important means of communication between the members of terrorist groups, used, for example, for issuing of orders from leaders to the rank-and-file. Web sites can be used for terrorist training, for instance by posting manuals on the web (p. 114). Unfortunately, he seems unaware of the many flaws and mistakes which have been pointed out (e.g., by RAND staff) in some of the training manuals available on the web. The only people likely to get killed if somebody were to follow these instructions are the bomb makers themselves. Of course, in principle this is a temporary limitation as it is just as easy to post reliable do-it-yourself bomb making manuals as it is to post unreliable ones.

More ominously, the web may become a target of terrorists attacks, and due to the rapidly growing reliance of just about everything on the web, the consequences might be severe, say if electricity and transportation grids were to be affected or if legitimate electronic money transactions were prevented. To his credit, the author cautions against panic, pointing out that nothing like this has ever actually happened, and that the "Y2K scare" proved completely unfounded. The threat of cyberterrorism is exaggerated — public webs (at least in the West) are well-protected, and although privately owned networks may be more vulnerable, their sheer number provides the entirety of the web with considerable resilience.

Proceeding to a survey of the counter-measures, the author does not confine himself to listing government initiatives but also mentions the interesting phenomenon of an informal international counter-terrorist alliance of hackers who in the wake of 9/11 launched coordinated attacks on terrorist web sites. He also devotes a chapter to the tradeoffs between security and civil liberties, underlining the risks of severely damaging the latter in unnecessary and/or futile attempts to

prevent terrorist use of the internet: "... intensifying repression of civil liberties and exploitation of privacy are far more sinister in the long run than the threat of terrorism, international or domestic ... Modern societies, it appears, will have to learn to live with some terrorism."

The book offers a useful and, on the whole, balanced survey and analysis of a problem which may or may not materialize in the future.

Bjørn Møller, Danish Institute for Security Studies.