

"Strategies for Securing the Cyber Safety Net for Terrorists: A Multi-Disciplinary Approach"

Cyberspace provides a potent safety net for terrorists as its under regulated spaces allow for a variety of illegal acts in support of terrorist activities. As traditional sources for terrorist funding have come under increased scrutiny and control, terrorists have increasingly turned to other illegal avenues for their fund raising activities. While high level crimes, such as drug running and human trafficking, have received increased attention, the threat to global security of such "low level" digital crimes as digital piracy, phishing and identity theft remain largely ignored. This paper explores the growing evidence that such "personal" crimes as digital piracy, counterfeiting, phishing and digital fraud are being used to fund terrorists' activities. It examines the digital safety net in which these crimes exist, created by a mix of cultural and economic factors that have undervalued the global security threat of these crimes. After comparing current international enforcement efforts, in the United States, European Union and India, with a focus on cyberfraud and digital piracy laws, the paper suggests a multidisciplinary, transborder approach for reducing this safety net and enhancing global security within the context of broader counter-terrorist efforts.