Cyberterrorism in the 21st century is now one of the greatest threats to global security and information. It transcends national borders (and by extension national legal systems), making it difficult for individual countries to formulate a cohesive defence plan against it. The world is yet to see any serious acts of cyberterrorism targeting multiple countries at once, but there’s a need for countries to develop legal precedents to deal with this should it happen. This book investigates cyberterrorism in terms of the conventions and legislation developed in response to the growing need to protect the digital infrastructure and information of citizens, companies and governments. It looks at the challenges faced by international organisations in first defining then responding and curbing cyberterrorism. Following this is analysis of legal provisions, with case studies of enforcement and of jurisdiction of these provisions.

Unique in the way that all aspects of cyberterrorism are considered, from initial infringement to eventual prosecution, this book provides recommendations and guidance to law-based post-graduates and professionals working on digital crime, and to those interested in national and international legal legislation against it.