Cyberterrorism – The use of the Internet for terrorist purposes

Synopsis

Cyberterrorism and the misuse of Internet for terrorist purposes represents a serious threat, since many essential aspects of today’s society are completely dependent upon the functioning of computer systems and the Internet.

Further to the adoption by the Council of Europe of the Cybercrime Convention (2001) and the Convention on the Prevention of Terrorism (2005), its Committee of Experts on Terrorism (CODEXTER) has been studying this matter and surveying the situation in member states to evaluate whether existing legal instruments are sufficient to combat this emerging form of crime.

This publication contains an expert report prepared by the Max Planck Institute, which evaluates the main problems that arise in the context of cyberterrorism and provides recommendations, together with reports on the situation in the member and observer states of the Council of Europe and the relevant Council of Europe conventions.

Contents

Foreword
Analytical report
Executive Summary
Introduction14

I. Threat Analysis: Use of the Internet for Terrorist Purposes and Cyberterrorism
A. Attacks via the Internet
  1. Attacks on Infrastructure
  2. Attacks on Human Life
B. Dissemination of Content
  1. Presentation of Terrorist Views
  2. Propaganda and Threats
  3. Recruitment and Training
  4. Fundraising and Financing
C. Use of the Internet for other Purposes
  1. Individual Communication
  2. The Internet as a Planning and Support Instrument
D. Conclusions
II. Legal and Policy Evaluation: International Co-operation Against Terrorist Use of the Internet
A. Overview
1. The Need for International Co-operation
2. Aim, Method, and Structure of the Following Analysis

B. Developing and Harmonising National Substantive Criminal Law
1. Destructive Attacks Carried Out by Means of the Internet
2. Dissemination of Illegal Content
3. Use of the Internet for Other Purposes

C. Developing and Harmonising National Criminal Procedure and Preventive Measures
1. Computer-Specific Investigations
2. Financial Investigations
3. Terrorist-Specific Investigations
4. Evaluation and Consequences for Legal Policy

D. Improving International Co-operation
1. Co-operation in Computer-Specific Cases
2. Co-operation in Cases of Money Laundering and the Financing of Terrorism
3. Co-operation in Terrorist Cases
4. Co-operation in General Cases
5. Evaluation and Consequences for Legal Policy

III. Conclusions
A. Use of the Internet for Terrorist Purposes
B. Applicability of Existing Conventions
C. General Problems of Existing Conventions
D. New Efforts With Respect to Illegal Content

References
National reports:
Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Hungary, Latvia, Lithuania, Luxembourg, Moldova, Norway, Portugal, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, “The former Yugoslav Republic of Macedonia”, Turkey, United Kingdom, Mexico, United States of America

Selected Council of Europe reference texts
Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) Explanatory Report
European Convention on Cybercrime (ETS No. 185) Explanatory Report
Parliamentary Assembly Recommendation 1706 (2005) on media and terrorism
Parliamentary Assembly Recommendation 1565 (2007)
How to prevent cybercrime against state institutions in member and observer states