

Contents

Preface	v
The Cyberterrorism Project	xv
Terrorist Use of the Internet and Cyberspace: Issues and Responses <i>Camino Kavanagh, Madeline Carr, Francesca Bosco and Adam Hadley</i>	1
Cyberterrorism and Critical Infrastructure Protection	
Cyberterrorism: A Challenge for External and Internal Security <i>Wolfgang Röhrig and Salvador Llopis</i>	25
Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications <i>Mobolarinwa Balogun, Hayretin Bahşi and Bilge Karabacak</i>	49
Critical Infrastructure Cyber-Security Risk Management <i>Theodoros Spyridopoulos, Konstantinos Maraslis, Theo Tryfonas and George Oikonomou</i>	59
The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists <i>Leonie Maria Tanczer</i>	77
Cyber-Enabled Terrorist Financing	
Online Terrorist Financing <i>Bürke Uğur Başaranel</i>	95
Cybercrime-Funded Terrorism and the Threats Posed by Future Technologies: Appealing Economics and Targets <i>Giovanni Bottazzi and Gianluigi Me</i>	109
Jihadi Online Propaganda: Purposes and Effects	
Between the Arab Revolutions and the Islamic State's Caliphate: al-Qaeda Leaders' Online Propaganda 2012–2014 <i>Gunnar J. Weimann</i>	129
Radicalisers as Regulators: An Examination of <i>Dabiq</i> Magazine <i>Stuart Macdonald</i>	146
The Role of Discourse Analysis in Terrorism Studies: Comparing <i>Inspire</i> and <i>Dabiq</i> <i>Nuria Lorenzo-Dus, Luke Walker and Anina Kinzel</i>	158

Learning from ISIS's Virtual Propaganda War for Western Muslims: A Comparison of <i>Inspire</i> and <i>Dabiq</i> <i>Haroro J. Ingram</i>	170
Online Jihadi Instructional Content: The Role of Magazines <i>Maura Conway, Jodie Parker and Sean Looney</i>	182
Online Counterterrorism	
<i>Public Actors, Private Actors, and Cooperative Approaches</i>	
Hard and Soft Power Approaches to Countering Online Extremism <i>Keiran Hardy</i>	199
Anglosphere Approaches to Counter-Terrorism in Cyberspace <i>Tim Legrand</i>	214
Prosecuting Terrorist Activity in Canada <i>Angela Gendron</i>	229
An Efficient Response to ISIS in Cyberspace: Public-Private Partnership <i>Minhac Çelik</i>	249
Prevention, Anti-Radicalisation and the Role of Social Media: A View from Germany <i>Holger Nitsch and Dominik Irani</i>	257
<i>Online CVE Strategies</i>	
Counter-Terrorism Strategic Communications: Back to the Future – Lessons from Past and Present <i>Alastair Reed</i>	269
Interrupting Engagement with Online Extremist Content: Utilising “Noisy” Foreign Fighters <i>Jamal Barnes and Kosta Lucas</i>	279
Interpreting Public Reactions to Terrorist Events Using Open Source Network Analysis <i>Daniel Grinnell</i>	290
<i>Surveillance</i>	
Reframing ‘Mass Surveillance’ <i>Sergei Boeke</i>	307
Beyond Big Data: Surveillance, Metadata and Technology-Enabled Intelligence Opportunities in Counter-Terrorism <i>David Wells</i>	319
National Security, Terrorism and the Legality of Secret Surveillance: The Case of France <i>Theodore Christakis</i>	327

Innovative Approaches/Responses

Internet Forensics as a Tool for Responding to Cyber-Fronts <i>Murat Gunestas and Kamil Yilmaz</i>	341
(En)gendering Cyberterrorism in the UK News Media: A Discursive Analysis <i>Lee Jarvis</i>	356
Predicting the Emergence of Self-Radicalisation Through Social Media: A Complex Systems Approach <i>Roger Bradbury, Terry Bossomaier and David Kernot</i>	379
Subject Index	391
Author Index	393

Abstract. The authors of this paper consider recent developments involving terrorist use of the internet and cyberspace for a range of purposes, as well as renewed concerns relating to potential terrorist attacks against critical infrastructure and their control systems. Following from an overview of recent trends, they discuss public and private efforts to respond to existing and emerging threats. The authors anchor these within the context of current efforts to manage a range of interrelated cyber security challenges, focusing predominantly on the international and regional response, as well as efforts by industry actors to deal with terrorist use of their products and services.

Keywords: Terrorism, counter-terrorism, internet, ICT, cyberspace, Islamic State, al Qaeda, law enforcement, United Nations, private sector, norms, practices.

1. Introduction

As far back as 1990, experts at a United Nations (UN) conference on the implications of technology for international security in Sendai, Japan, forecast some of the difficulties UN member states would confront in efforts to manage the diffusion of political, scientific and technological power enabled by the information technology revolution. The report emerging from the conference stressed that the international community was not well positioned to deal constructively with some of the disruptive side-effects stemming from the diffusion of science and technology throughout the world, noting that the very distribution of technologies that we encourage may also give strength to certain forces which we wish to suppress - notably terrorism, sub-national violence, ethnic and religious intolerance [2].

Corresponding author. Department of War Studies, 6th Floor, King's College London, Strand, London, WC2R 2LS, UK. Email: seminor.havanagh@kcl.ac.uk.

¹ Since there is no universal agreement on a definition of terrorism, the authors have chosen to lean on the EU Council Common Position 2001/931/CFSP and the Council Framework Decision 2002/475/JHA which define 'terrorist offences' as acts committed with the aim of 'seriously intimidating a population', 'seriously compelling a government or international organization to perform or abstain from performing any act', or 'seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization'. For a broader discussion of the definitions issue, see the document published by the European Parliament in November 2013 [1].