Critical Infrastructure Security

WIT*PRESS*

WIT Press publishes leading books in Science and Technology.
Visit our website for the current list of titles.
www.witpress.com

WIT*eLibrary*

Home of the Transactions of the Wessex Institute, the WIT electronic-library provides the international scientific community with immediate and permanent access to individual papers presented at WIT conferences.
Visit the WIT eLibrary athttp://library.witpress.com

Critical Infrastructure Security

Assessment, Prevention, Detection, Response

Edited by

Francesco Flammini

WIT PRESS Southampton, Boston

Editor:

Francesco Flammini

Published by

WIT Press
Ashurst Lodge, Ashurst, Southampton, SO40 7AA, UK
Tel: 44 (0) 238 029 3223; Fax: 44 (0) 238 029 2853
E-Mail: witpress@witpress.com
http://www.witpress.com

For USA, Canada and Mexico

WIT Press
25 Bridge Street, Billerica, MA 01821, USA
Tel: 978 667 5841; Fax: 978 667 7582
E-Mail: infousa@witpress.com
http://www.witpress.com

British Library Cataloguing-in-Publication Data

A Catalogue record for this book is available
from the British Library

ISBN: 978-1-84564-562-5
eISBN: 978-1-84564-563-2

Library of Congress Catalog Card Number: 2010943114

The texts of the papers in this volume were set individually by the authors or under their supervision.

Printed in Great Britain by Lightning Source UK.

To Liana

Contents

Part IV Monitoring and Surveillance Technologies

Preface

The security of critical infrastructures is a paramount issue in modern society. In fact, infrastructures like those for transportation, energy, telecommunication, banking, etc. whose operability is essential for the well-being of a large number of individuals are nowadays exposed to severe threats, both natural (earthquakes, landslides, flooding, etc.) and intentional (thefts, vandalism, terrorism, etc.). In recent years, the scientific community has addressed the issue of Critical Infrastructure Security (CIS) through conferences, journals and other publications. However, in most cases, the published material fails to address the CIS issue as a multi-faceted and multi-disciplinary problem which needs to be analysed in an integrated manner both at the organizational and technological levels, and looking at digital ("cyber") as well as physical security.

The purpose of this book is to provide a comprehensive picture of the state-of-the-art and trends in methods and tools for infrastructure protection, focusing on the following topics:

- *Assessment*, that is the understanding of risks and vulnerabilities as well as expected results of possible mitigations. This can be achieved by analysis, modelling and simulation.
- *Prevention*, that is the reduction of risk by predicting threat effects. This can be achieved by means of deterrence and other "passive" countermeasures (e.g. security by design).
- *Detection*, that is the capability of real-time recognition of abnormal conditions or behaviours. This can be achieved by means of "active" sensors and other technological tools.
- *Response*, that is the quick reaction to threats. This can be achieved by adopting early warning, situational awareness and decision support systems.

Most of the current best practices are based on intrusion detection / access control, people scanning and video surveillance designs which are often weak and poorly effective since they are not rigorous enough and frequently not systematically guided by risk analysis principles. This book provides the necessary balance between the analysis aspects, which involve people (personnel, operators, adversaries, etc.) taking into account organizational and interdependency effects, and the technological tools (smart-detectors, information networks, control software, etc.), which are required to implement modern integrated surveillance and security management systems. Therefore, the topics presented in the volume progress smoothly from security evaluation methods and tools to security enhancement approaches and technologies.

It is the Editor's belief that the book provides the most up to date compendium of Critical Infrastructure Security and he is grateful to all authors for their excellent contributions.

The Editor, 2012