NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 51

Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures

Edited by
Konstantin Dimitrov

IOS
Press

NATO
OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

CYBER DEFENCE IN INDUSTRY 4.0 SYSTEMS AND RELATED LOGISTICS AND IT INFRASTRUCTURES

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in cooperation with NATO Emerging Security Challenges Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series D: Information and Communication Security – Vol. 51
ISSN 1874-6268 (print)
ISSN 1879-8292 (online)

Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures

Edited by

Konstantin Dimitrov

Head of Department "Logistics Engineering", Technical University, Sofia, Bulgaria

IOS Press

Amsterdam • Berlin • Washington, DC

Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Research Workshop on Cyber Defence in Industry 4.0
Systems and Related Logistics and IT Infrastructures
Jyvaskyla, Finland
16–21 October 2017

ISBN 978-1-61499-887-7 (print)
ISBN 978-1-61499-888-4 (online)
Library of Congress Control Number: 2018952149

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

For book sales in the USA and Canada:
IOS Press, Inc.
6751 Tepper Drive
Clifton, VA 20124
USA
Tel.: +1 703 830 6300
Fax: +1 703 830 2300
sales@iospress.com

LEGAL NOTICE
The author(s) of this publication is/are solely responsible for its content. This
publication does not reflect the opinion of the publisher. The publisher cannot be held
liable for any loss or damage that may occur because of this publication.

PRINTED IN THE NETHERLANDS

Preface

The general objectives of this book include the development of strategies, concepts and tools for the creation and implementation of cyber systems and cyber platforms capable of providing enhanced cyber security and interoperability, smart intrusion prevention, adaptive cyber defence, smart recovering (if needed) of the systems states, smart monitoring, control and management of Industry 4.0 complexes and related logistics systems (composed respectively of connected industrial and logistics modules of 4th generation, e.g., robotic equipment, logistics modules and units, technologic equipment, etc.), as well as their IT infrastructure(s).

The reality is that it is extremely difficult to provide full cyber defence and/or intrusion prevention of the smart networks that connect intelligent industrial and logistics modules, since the more intelligent the systems are, the more vulnerable they become. Therefore, the main efforts of the scientific publications developed in this book are focused on development and implementation of strategies, concepts and tools capable of providing intrusion prevention and cyber defence of smart IT infrastructure(s), but mostly of system core, that controls the entire Industry 4.0 and/or logistics networks, and (if necessary) the reconfiguration of the systems states in the smart infrastructures.

This publication focuses on the creation of concepts for smart environments and cyber platforms, which form the so-called “web of everything” and are (respectively) capable of providing generic turnkey solutions in a variety of application fields – e.g., creation of ecosystems which are based on “Cyber Platform(s) for Connected Smart Objects” and are capable to interconnect, to control and to provide ***adaptive cyber defence and intrusion prevention*** (and even without human intervention) of connected 4G smart devices and embedded systems that can be integrated into smart IT infrastructures and service platforms and respectively – be implemented in the 4G industrial “world” (e.g., Industry 4.0 systems, intelligent logistics systems, intelligent transport, etc.). Therefore, the proposed concepts for Cyber-physical platforms (CPP) include also their openness to any type of simulation, optimization, and model-creation services (modules) that might appear in the future, i.e., CPP which could be open, scalable, with high-capacity and capable of transition from ***flexibility*** *to* ***agility*** in the simulated processes and the created generic models.

This publication also focuses on the development of strategies and concepts for industrial deployment of the proposed CPP across multiple sectors (such as industrial and logistics processes), with the support of identified participants who are capable to act as technology and IT infrastructure integrators.

All scientific publications developed in this book were presented during an Advanced Research Workshop (ARW), with the title “*Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*”.

The ARW took place in Jyvaskyla, Finland in the time period: October 16 – October 21, 2017, and was sponsored by NATO Emerging Security Challenges Division, SPS Programme, Project G5172.

A Note on the Editor:

Prof. Dr. Eng. Konstantin DIMITROV is Head of Department "Logistics Engineering", Technical University, Sofia, Bulgaria. E-mail: *kdimitrov@tu-sofia.bg*

Teaching and Research activities of Prof. Konstantin Dimitrov include:

Knowledge-based intelligent systems; implementation of neural, neuro-fuzzy and genetic systems for adaptive control, decision-making and reconfiguation of process/system behaviour; reliability and fault diagnosis of industrial systems; logistics engineering.

Prof. Konstantin Dimitrov is the author of more than 100 scientific publications, 6 books and 3 monographs. He is also a Director of many research and industrial projects and PhD Theses.

Contents

Industry and government are increasingly r[illegible]gent – or "smart" – and interconnected computer infrastructure, but the reality is that it is extremely difficult to provide full cyber defense and/or intrusion prevention for the smart networks that connect intelligent industrial and logistics modules, since the more intelligent the systems are, the more vulnerable they become.

This book presents papers from the NATO Advanced Research Workshop (ARW) on Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures, held in Jyvaskyla, Finland, 16-21 October 2017.

The main focus of the 11 papers included here is the creation and implementation of cyber systems and cyber platforms capable of providing enhanced cyber security and interoperability for smart IT infrastructure. Topics covered include: smart intrusion prevention; adaptive cyber defense; smart recovery of systems; and the smart monitoring, control and management of Industry 4.0 complexes and related logistics systems such as robotic equipment, logistics modules, units and technologic equipment, as well as their IT infrastructure.

ISBN 978-1-61499-887-7

9 781614 998877

www.iospress.nl

ISBN 978-1-61499-887-7 (print)
ISBN 978-1-61499-888-4 (online)
ISSN 1874-6268 (print)
ISSN 1879-8292 (online)