e-book

Habtamu Abie, Davide Ferrario, Ernesto Troiano,
John Soldatos, Fabrizio Di Peppo, Aleksandar Jovanović,
Ilias Gkotsis, Evangelos Markakis (Eds.)

Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection

Virtual Workshop, June 24–25, 2020

Steinbeis-Edition

Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection

Virtual Workshop, June 24–25, 2020

Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo,
Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Eds.)

Steinbeis-Edition

Abstract

Modern critical infrastructures ("critical entities" in the terminology of the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. To face them successfully, aligned and integrated responses are needed, and this workshop has provided a great opportunity to do it: aligning and integrating not only the positions of single projects but also of many intended users of their results.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in seven different industrial sectors, such as finance, healthcare, energy, air transport, communications, industrial plants, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.

Specifically, novel techniques have been presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, resilience of critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures.

The workshop included two opening remarks, two keynote speeches, 11 project presentations, 2 roundtable and panel discussions and 10 thematic presentations. The audience included scientists and experts in the field of critical infrastructure protection, CISOs, CIOs, CERTs, CSIRTs, CSOs, cyber and physical security experts representing different sector and policy makers for Critical Infrastructure protection.

Table of Contents

Imprint

2021 Steinbeis-Edition

Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo,
Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Eds.)

Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection
Virtual Workshop, June 24–25, 2020

1st edition, 2021 | Steinbeis-Edition, Stuttgart
ISBN 978-3-95663-087-3

Layout: Steinbeis-Edition
Cover picture: Macrovector/shutterstock.com

218957-2021-10 | www.steinbeis-edition.de

Modern critical infrastructures ("critical entities" in the terminology of the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. To face them successfully, aligned and integrated responses are needed, and this workshop has provided a great opportunity to do it: aligning and integrating not only the positions of single projects but also of many intended users of their results.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in seven different industrial sectors, such as finance, healthcare, energy, air transport, communications, industrial plants, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.

Specifically, novel techniques have been presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, resilience of critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures. The workshop included two opening remarks, two keynote speeches, 11 project presentations, 2 roundtable and panel discussions and 10 thematic presentations. The audience included scientists and experts in the field of critical infrastructure protection, CISOs, CIOs, CERTs, CSIRTs, CSOs, cyber and physical security experts representing different sector and policy makers for Critical Infrastructure protection.

978-3-95663-087-3

Steinbeis-Edition