



Habtamu Abie, Ilias Gkotsis, Manos Athanatos,  
Rita Ugarelli, Denis Čaleta, Lorenzo Lodi,  
Fabrizio Di Peppo, Aleksandar Jovanović (Eds.)

# Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience

Virtual Workshop, April 27–29, 2022

# **Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience**

Virtual Workshop, April 27–29, 2022

Habtamu Abie, Ilias Gkotsis, Manos Athanatos, Rita Ugarelli, Denis Čaleta,  
Lorenzo Lodi, Fabrizio Di Peppo, Aleksandar Jovanović (Eds.)

## Imprint

2023 Steinbeis-Edition




Habtamu Abie, Ilias Gkotsis, Manos Athanatos, Rita Ugarelli, Denis Čaleta, Lorenzo Lodi, Fabrizio Di Peppo, Aleksandar Jovanović (Eds.)

Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection  
Virtual Workshop, April 27–29, 2022

1st edition, 2023 | Steinbeis-Edition, Stuttgart  
ISBN 978-3-95663-285-3

Layout: Habtamu Abie, Ilias Gkotsis | Technical Editing: Steinbeis-Edition  
Cover picture: Hilch/Shutterstock.com, edited by Steinbeis-Edition

License for Figures 60 and 61:  CC BY-NC

The platform provided by Steinbeis makes us a reliable partner for company startups and projects. We provide support to people and organizations, not only in science and academia, but also in business. Our aim is to leverage the know-how derived from research, development, consulting, and training projects and to transfer this knowledge into application – with a clear focus on entrepreneurial practice. Over 2,000 business enterprises have already been founded on the back of the Steinbeis platform. The outcome? A network spanning over 6,000 experts in approximately 1,100 business enterprises – working on projects with more than 10,000 clients every year. Our network provides professional support to enterprises and employees in acquiring competence, thus securing success in the face of competition. Steinbeis-Edition publishes selected works mirroring the scope of the Steinbeis Network expertise.

222728-2023-02 | [www.steinbeis-edition.de](http://www.steinbeis-edition.de)

# Abstract

Modern critical infrastructures (or “critical entities” as now defined in 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. Addressing them successfully, need coordinated and integrated responses, which must be disseminated and exploited further to the EU funded projects’ frameworks or individual research studies’ reports, through raising awareness initiatives, such as the 2nd ECSCI Workshop on CIP.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in several 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, ethical and legal aspects of cybersecurity, combating hybrid threats to critical infrastructure, cyber and physical threats detection, increased automation for detection, prevention and mitigation measure, information and knowledge sharing, standards and regulations for the protection of critical infrastructures, common platforms for cascading effects on the different critical infrastructures, combined safety and security solutions, cyber security awareness, and the landscape of advanced combined cyber and physical threats.

The workshop included three opening remarks, three keynote speeches, twenty-one project presentations, two roundtable and panel discussions, twenty-one thematic presentations, and closing remarks. 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 sectors and policy makers for critical infrastructure protection.

# Table of Contents

1. Organizing committee.....	10
2. Program Agenda .....	11
3. Welcome and Opening Remarks.....	17
3.1 Opening Remarks.....	17
3.2 The ECSCI Cluster Achievements .....	18
4. Keynotes.....	21
4.1 Cybersecurity investments and good practices for cyber risk management in critical infrastructure .....	21
4.2 The evolution of security and resilience of critical infrastructures in a challenging environment .....	21
5. Project Presentations.....	22
5.1 Security and trust assessment in CPS / IOT architectures .....	22
5.2 Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures.....	24
5.3 Cyber Securing Energy Data Services.....	28
5.4 Privacy-preserving AI in Systems Medicine with Federated Learning.....	31
5.5 Shielding the power grid from cyberattacks.....	33
5.6 Securing the e-commerce ecosystem from cyber, physical and cyber-physical threats.....	36
5.7 Empowering a Pan-European Network to Counter Hybrid Threats .....	40
5.8 Securing critical financial infrastructure .....	43
5.9 Intelligent Management of Processes, Ethics and Technology for Urban Safety .....	45
5.10 Improving resilience of sensitive industrial plants and infrastructures.....	49
5.11 Improving the cyber security of the European electrical power energy systems .....	52
5.12 Protection of Critical Infrastructures from advanced combined cyber and physical threats...	56
5.13 Cascading cyber-physical threats and effects.....	58
5.13.1 PRECINCT Framework Specification for systematic CI security and resilience management.....	59
5.13.2 Cross-Facility collaborative cyber-physical Security and Resilience management Platform.....	59
5.13.3 Vulnerability Assessment Tool - Serious Games.....	59
5.13.4 CI Digital Twins.....	60
5.13.5 PRECINCT Living Labs (LLs) .....	60
5.13.6 Resilience Improvement Workflows.....	60
5.14 Resilience enhancement and risk control for communication infrastructures .....	62
5.15 Security of air transport infrastructure of Europe .....	66
5.16 Scalable, trusted, and interoperable platform for secured smart GRID.....	71

5.17 An integrated, yet installation specific, solution for the resilience of gas infrastructure against cyber and physical threats.....	75
5.18 Cyber-security protection in healthcare IT ecosystem .....	79
5.19 Protection of critical water infrastructures .....	81
5.20 A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats .....	85
6. Panel and Round Tables Discussions .....	89
6.1 Introduction .....	89
6.2 E-commerce: Eyup Kun (ENSURESEC): Evolution of the Cybersecurity Responsibilities: From NIS-to-NIS Directive 2 and its impact on E-commerce .....	89
6.3 Airports and ports: Maria Avramidou and Maja Nišević (PRAETORIAN): The Cybersecurity of airports and ports under the proposed NIS2 and CER Directives.....	90
6.4 Medical Devices: The impacts of the NIS2 Directive proposal on medical device manufacturers and the challenges concerning incident reporting/notification .....	91
6.5 Conclusion .....	92
7. Thematic Presentations .....	93
7.1 Ethical and legal aspects of cybersecurity .....	93
7.1.1 Abstract.....	93
7.1.2 The complementing instruments of the Rule of Law.....	93
7.1.3 Code of Engagement for Threat Intelligence Sharing .....	93
7.1.4 IoT risks models for Critical Infrastructure Protection.....	94
7.1.5 Conclusion .....	96
7.2 Combating Hybrid Threats to Critical Infrastructures.....	96
7.2.1 Abstract on the EU-Hybnets projects' main objectives.....	96
7.2.2 Innovations to counter Hybrid Threats: Critical Infrastructures.....	98
7.2.3 Conclusions and Future Work.....	99
7.2.4 Acknowledgements.....	100
7.3 Increased automation for detection, prevention and mitigation measures .....	100
7.4 Information sharing techniques, rules, and repository to exchange knowledge .....	102
7.4.1 Tools verification and authorization .....	104
7.4.2 Customer identity and credential (age) verification .....	104
7.4.3 Decentralized Identities tool implementation.....	105
7.4.4 Conclusions: Security and Privacy considerations .....	106
7.5 Standards and Regulations for the Protection of Critical Infrastructures .....	106
7.5.1 Industrial Cybersecurity Testing Methodology on LSPs.....	106
7.5.2 Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released .....	110
7.5.3 Standards and NIS compliance.....	113
7.5.3.1 The AI4HealthSec Project.....	113

7.5.3.2 Main idea .....	113
7.5.3.3 Results.....	114
7.5.3.4 Conclusions .....	114
7.5.3.5 Acknowledgements.....	115
7.6 Common Platform for Cascading Effects on the Different Critical Infrastructures .....	115
7.6.1 Synergies and Challenges towards the integration of Safety and Security requirements in Critical Infrastructure Protection: Examples from the SecureGas and Infrastress projects ..	115
7.6.2 Simulation Framework for Cascading Effects among Urban Critical Infrastructures .....	118
7.6.3 Simulation Framework for Cascading Effects among Urban Critical Infrastructures .....	119
7.7 Combined Safety and Security for European Critical Infrastructures.....	122
7.7.1 Integrated Security, Safety and Risk Assessment for CIs .....	122
7.7.2 Pan-European cybersecurity information and incidents sharing and management for Energy Infrastructures .....	125
7.8 Cyber Security Awareness.....	126
7.9 Advanced Combined Cyber and Physical Threats.....	129
7.9.1 Visible and Emerging Vulnerabilities in Critical Energy Infrastructures.....	129
7.9.2 Modeling cyber and physical threats in IT&OT integrated systems .....	131
8. Concluding Remarks and Planning.....	134
8.1 Closing Remarks .....	134
8.2 Conclusions and Planning .....	134
8.2.1 Day 1 .....	134
8.2.2 Day 2 and Day 3 .....	135
8.3 Concluding Remarks.....	135
Acknowledgements.....	136
References .....	137

## List of Figures

Figure 1 - ECSCI 25 member projects and collaboration activities .....	19
Figure 2 - ANASTACIA high-level conceptual architecture .....	23
Figure 3 - ANASTACIA integration, demonstration and exploitation in a nutshell .....	24
Figure 4 - CyberSANE Incident Handling Warning and Response System for the European Critical Infrastructures ecosystem.....	27
Figure 5 - The CyberSANE system architecture overview.....	27
Figure 6 - CyberSEAS ecosystem .....	29
Figure 7 - The overall FeatureCloud system provides access to 3rd-party developers, isolates app execution on the hospital infrastructure and enables non-developers to use existing apps with their own data.....	32
Figure 8 - EnergyShield tools presentation.....	34
Figure 9 - EnergyShield toolkit .....	35
Figure 10 - ENSURESEC conceptual architecture .....	37
Figure 11 - View of the ENSURESEC Global Dashboard .....	38
Figure 12 - EU-HYBNET T2.2 latest research results on pan-European security practitioners and other relevant actors' gaps and needs, "threats" to counter hybrid threats.....	41
Figure 13 - Ideas & Innovations proposed to counter Hybrid Threats, EU-HYBNET Deliverable 4.4 .....	42
Figure 14 - FINSEC Reference Architecture.....	44
Figure 15 - IMPETUS basic Architecture .....	46
Figure 16 - The role of COSSEC in IMPETUS project .....	48
Figure 17 - InfraStress Integrated Framework: main modules .....	50
Figure 18 - PHOENIX Key Challenges, Pillars and Technologies.....	53
Figure 19 - PHOENIX Platform Architecture.....	54
Figure 20 - PHOENIX Large Scale Pilot Locations .....	55
Figure 21 - PRAETORIAN solution .....	57
Figure 22 - PRAETORIAN pilot sites.....	57
Figure 23 - Interdependencies between Critical Infrastructures.....	58
Figure 24 - PRECINCT Living Labs .....	60
Figure 25 - PRECINCT Workflow for CI Resilience Improvement.....	60
Figure 26 - PRECINCT Workflow for Operational Response Improvement .....	61
Figure 27 - RESISTO architecture .....	63
Figure 28 - STCL functional control flow and the main modules developed .....	64
Figure 29 - Security management as proposed by SATIE .....	68
Figure 30 - SealedGRID consortium .....	71
Figure 31 - SealedGRID architecture .....	73
Figure 32 - SecureGas High Level Reference Architecture .....	76
Figure 33 - SecureGas Advanced components .....	77
Figure 34 - SecureGas Business Cases.....	78
Figure 35 - SPHINX Architecture .....	79
Figure 36 - Pilot execution Methodology.....	80
Figure 37 - The STOP-IT platform architecture .....	82
Figure 38 - 7SHIELD objectives.....	86
Figure 39 - 7SHIELD high level architecture.....	87
Figure 40 - Pilot Use Cases of the 7SHIELD project.....	88
Figure 41 - CONCORDIA Platform for Threat Intelligence .....	94
Figure 42 - Overview of different layers of risks that can occur in cyber-physical systems .....	95
Figure 43 - Ideas and Innovations proposed to counter Hybrid Threats, EU-Hybnet Deliverable 3.3.....	98



Figure 44 - “Ecosystem” of Cybersecurity Tools: Replacing a Firewall .....	101
Figure 45 - IOTA Identity Roles .....	103
Figure 46 - Secure Age Verification in online shopping .....	104
Figure 47 - SSI Bridge Network of Trust .....	105
Figure 48 - PHOENIX Large Scale Pilots .....	107
Figure 49 - Example of DNV test program for LSP1 .....	109
Figure 50 - PHOENIX LSP1 Windfarm Test Site .....	109
Figure 51 - A representation of the standards analysis results per measure and section .....	114
Figure 52a - Comparison of Infrastress methodology (H2020 Infrastress).....	118
Figure 52b - Comparison of Infrastress methodology (H2020 Infrastress) .....	118
Figure 52c - Comparison of Infrastress methodology (H2020 Infrastress).....	118
Figure 53 - Test Case about drone inspection (H2020 SecureGas).....	118
Figure 54 - How RINA intent resilience management for CI operators .....	119
Figure 55 - Illustration of the Intra- and Inter-Domain Simulation Model .....	120
Figure 56 - Future concept for cascading effects simulation in PRECINCT .....	121
Figure 57 - i-RISK scientific workflow .....	123
Figure 58 - i-RISK user interface.....	123
Figure 59 - Risk assessment examples .....	124
Figure 60 - I2SP – Distributed Incidents Information Sharing Platform.....	125
Figure 61 - I2SP – Control Centre: Homepage and Full Report.....	126
Figure 62 - SIEM as a standalone tool.....	127
Figure 63 - Agents Dashboard.....	127
Figure 64 - Logs, Events & Alerts from the Infrastructure Endpoint to SOC analysts.....	128
Figure 65 - SANS Survey 2021 - OT ICS Cybersecurity Nozomi Networks.....	130
Figure 66 - Certification of Gratitude and Appreciation .....	136

## List of Tables

Table 1 - Brief description of tools developed in IMPETUS .....	46
Table 2 - SATIE Innovation Elements .....	67

## 1. Organizing committee

The 2nd ECSCI workshop organizing committee consists of the following members:

- Habtamu Abie, Norsk Regnesentral / Norwegian Computing Center,  
E-mail: [habtamu.abie@nr.no](mailto:habtamu.abie@nr.no)  
Website: <https://home.nr.no/~abie/>  
Orcid ID: <https://orcid.org/0000-0003-0866-5050>
- Ilias Gkotsis, SATWAYS Ltd  
E-mail: [i.gkotsis@satways.net](mailto:i.gkotsis@satways.net)  
Orcid ID: <https://orcid.org/0000-0003-2228-1387>  
<https://www.linkedin.com/in/ilias-gkotsis-b7b84348/>
- Manos Athanatos, FORTH,  
E-mail: [athanat@ics.forth.gr](mailto:athanat@ics.forth.gr)  
<https://www.linkedin.com/in/manosathanatos/>  
Orcid ID: <https://orcid.org/0000-0002-1182-7922>
- Rita Ugarelli, SINTEF AS  
E-mail: [rita.ugarelli@sintef.no](mailto:rita.ugarelli@sintef.no)  
Orcid ID: <https://orcid.org/0000-0002-2096-8591>
- Denis Čaleta, President of the Board, Institute for Corporate Security Studies,  
E-mail: [denis.caleta@ics-institut.si](mailto:denis.caleta@ics-institut.si)  
Website: [www.ics-institut.si](http://www.ics-institut.si)
- Lorenzo Lodi  
E-mail: [lorenzo.lodi@zanasi-alessandro.eu](mailto:lorenzo.lodi@zanasi-alessandro.eu)  
Website: <https://www.zanasi-alessandro.eu>  
Orcid ID: <https://orcid.org/0000-0002-7600-621X>
- Fabrizio Di Peppo, GFT Italia,  
E-mail: [fabrizio.dipeppo@gft.com](mailto:fabrizio.dipeppo@gft.com)  
Website: <https://www.gft.com>
- Aleksandar Jovanović, Steinbeis EU-VRI  
E-mail: [jovanovic@risk-technologies.com](mailto:jovanovic@risk-technologies.com)  
Website: [www.eu-vri.eu](http://www.eu-vri.eu) and [www.risk-technologies.com](http://www.risk-technologies.com)

## 2. Program Agenda

The three-day workshop program agenda includes open remarks, keynote speeches from the ENISA, ECSO, and JRC, 21 presentations on H2020 project results, 2 roundtable and panel discussions, 21 thematic presentations, and closing remarks.

- ECSCI (European Cluster for Securing Critical Infrastructures) Workshop
- Venue: Virtual Meeting
- Dates: 27th-29th of April 2022

### Day 1: Wednesday, April 27th, 2022 (09:00-18.00)

#### Invited Talks, Project Presentations & Thematic Presentations

<b>Welcome and opening of the day</b>	
<i>Chair: Habtamu Abie, Norsk Regnesentral</i>	
09:00 - 09:10	Welcome and opening remarks: Habtamu Abie (Norsk Regnesentral) and Boryana HRISTOVA - ILIEVA from DG CNECT Unit H.2 – Cybersecurity and Digital Privacy Policy
09:10 - 10:00	<b>Invited Talk:</b> Cybersecurity investments and good practices for cyber risk management in critical infrastructure by Athanasios Drougkas, ENISA
10:00 - 10:20	Coffee Break
<b>Session 1: The results of EU research on CI protection (part 1)</b>	
<i>Chair: Manos Athanatos, FORTH</i>	
10:20 - 10:40	ANASTACIA ( <a href="http://www.anastacia-h2020.eu">www.anastacia-h2020.eu</a> ): Security and trust assessment in CPS / IOT architectures - Stefano Bianchi, Algowatt
10:40 - 11:00	CyberSANE ( <a href="http://www.cybersane-project.eu">www.cybersane-project.eu</a> ): Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures by Thanos Karantjias, MAGGIOLI
11:00 - 11:20	FeatureCloud ( <a href="http://featurecloud.eu">featurecloud.eu</a> ): Privacy-preserving AI in Systems Medicine with Federated Learning by Julian Matschinske, University of Hamburg
11:20 - 11:40	EnergyShield ( <a href="http://energy-shield.eu">energy-shield.eu</a> ): Shielding the power grid from cyberattacks by Otilia Bularca, SIMAVI
11:40 - 12:00	ENSURESEC ( <a href="http://www.ensuresec.eu">www.ensuresec.eu</a> ): Securing the e-commerce ecosystem from cyber, physical and cyber-physical threats by Luís Júdice Sousa, INOV
12:00 - 12:20	EU-HYBNET ( <a href="http://euhybnet.eu">euhybnet.eu</a> ): Empowering a Pan-European Network to Counter Hybrid Threats by Päivi Mattila, Laurea
12:20 - 12:40	CyberSEAS ( <a href="https://cyberseas.eu/">https://cyberseas.eu/</a> ): Cyber Securing Energy Data Services by Paolo Roccetti, Head of Cysec research unit, Engineering (ENG)
12:40 - 13:00	FINSEC ( <a href="http://www.finsec-project.eu">www.finsec-project.eu</a> ): Securing critical financial infrastructure - Fabrizio Di Peppo, GFT
13:00 - 14:00	Lunch Break
<b>Session 2: Cybersecurity and respective ELSI</b>	
<i>Chair and moderator: Erik Kamenjašević, KU Leuven CiTiP</i>	

14:00 - 15:00	<b><u>Cybersecurity and the NIS2 Directive: regulatory aspects and sectoral perspectives</u></b> Panel by KU Leuven CiTiP researchers involved in SAFECARE/ENSURESEC/ PRAETORIAN <ul style="list-style-type: none"> <li>• Eyup Kun (ENSURESEC): Evolution of the Cybersecurity Responsibilities: From NIS-to-NIS Directive 2 and its impact on E-commerce</li> <li>• Maria Avramidou and Maja Nišević (PRAETORIAN): The Cybersecurity of airports and ports under the proposed NIS 2 and CER Directives.</li> <li>• Elisabetta Biasin (SAFECARE): Medical Device Cybersecurity under the NIS2 and the AI Act</li> </ul> <i>Moderator: Erik Kamenjašević</i>
15:00 - 15:20	<b><u>Ethical and legal aspects of cybersecurity</u></b> <ul style="list-style-type: none"> <li>• By Dimitra Stefanatou (Arthur van der Wees), Arthur's Legal B.V</li> </ul>
15:20 - 15:40	Coffee Break
<b>Session 3: The results of EU research on CI protection (part 2)</b> <i>Chair: Rita Ugarelli, SINTEF</i>	
15:40 - 16:00	IMPETUS (www.impetus-project.eu): Intelligent Management of Processes, Ethics and Technology for Urban Safety by Joe Gorman, SINTEF Digital
16:00 - 16:20	InfraStress (www.infrastress.eu): Improving resilience of sensitive industrial plants & infrastructures - Gabriele Giunta, Engineering
16:20 - 16:40	PHOENIX (phoenix-h2020.eu): Improving the cyber security of the European electrical power energy systems by Ganesh Sauba, DNV
16:40 - 17:00	PRAETORIAN (praetorian-h2020.eu): Protection of Critical Infrastructures from advanced combined cyber and physical threats by Eva María Muñoz Navarro, ETRA I+D
17:00 - 17:20	SealedGRID (www.sgrid.eu): Scalable, trusted, and interoperable platform for secured smart GRID by Christos Xenakis, University of Piraeus
17:20 - 17:40	<b>Conclusions and Collaboration Planning of Day 1</b> <i>Chair: Habtamu Abie, Norsk Regnesentral</i>

**Day 2: Thursday, April 28th 2022 (9:00-17.00)**  
**Invited Talks, Project Presentations & Thematic Presentations**

<b>Welcome and Session 1</b> <i>Chair: Ilias Gkotsis, Satways Ltd</i>	
09:00 - 09:10	Welcome and opening remarks: Ilias Gkotsis (Satways) and Max Brandt from DG Migration and Home Affairs - D2 Counter-Terrorism
09:10 - 10:00	<b>Invited talk:</b> Moving towards a trustworthy and resilient European cyber security ecosystem by Roberto Cascella, ECSO
<b>Session 2: The results of EU research on CI protection (part 3)</b> <i>Chair: Ilias Gkotsis, Satways Ltd</i>	
10:00 - 10:20	SPHINX (sphinx-project.eu): Cyber-security protection in healthcare IT ecosystem by Evangelos Markakis, Hellenic Mediterranean University-HMU
10:20 - 10:40	STOP-IT (stop-it-project.eu): Protection of critical water infrastructures by Rita Ugarelli, SINTEF
10:40 - 11:00	7SHIELD (www.7shield.eu): A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats by Gerasimos Antzoulatos, Centre for Research and Technology-Hellas – CERTH
11:00 - 11:20	Coffee Break
<b>Session 3: The results of EU research on CI protection (part 4)</b> <i>Chair: Denis Caleta, ICS-Ljubljana</i>	
11:20 - 11:40	SecureGas (www.securegas-project.eu): An integrated, yet installation specific, solution for the resilience of gas infrastructure against cyber and physical threats by Celina Solari (Clemente Fuggini), RINA Consulting
11:40 - 12:00	PRECINCT (www.precinct.info): Cascading cyber-physical threats and effects by Antonis Mygiakis & Aristea Zafeiropoulou, Konnecta Systems
12:00 - 12:20	RESISTO (www.resistoproject.eu): Resilience enhancement and risk control for communication infrastructures - Bruno Saccomanno, Leonardo – Società per azioni
12:20 - 12:40	SAFECARE (www.safecare-project.eu): Safeguarding critical health infrastructure by Philippe Tourron (APHM - Hôpitaux universitaires de Marseille) and Isabel Praça (ISEP - Institut Superior de Engenharia do Porto)
12:40 - 13:00	SATIE (www.satie-h2020.eu): Security of air transport infrastructure of Europe by Tim Stelkens-Kobsch, German Aerospace Center (DLR)
13:00 - 14:20	Lunch Break
<b>Session 4: Combating hybrid and cyber-physical threats</b> <i>Chair: Habtamu Abie, Norsk Regnesentral</i>	
14:20 - 14:40	<b><u>Combating Hybrid Threats to Critical Infrastructures</u></b> <ul style="list-style-type: none"> <li>Innovations to counter hybrid threats by Souzanna Sofou, Satways (EU-HYBNET)</li> </ul>
14:40 - 15:00	<b><u>Cyber and Physical Detection</u></b>

	<ul style="list-style-type: none"> <li>● PRAETORIAN (praetorian-h2020.eu): Risk scenarios modelling and assessment in a combined attack approach by Frederic Guyomard, EDF Labs Paris (EDF)</li> </ul>
15:00 - 15:40	<b><u>Round table discussions</u></b> <ul style="list-style-type: none"> <li>● Frederic GUYOMARD, EDF Labs Paris (EDF)</li> <li>● Nineta Polemi, University of Piraeus</li> </ul> <i>Moderator: Christos Tselios, Citrix</i>
15:40 - 16:00	Coffee break
<b>Session 5: Increased automation and information sharing</b> <i>Chair: Ilias Gkotsis, Satways Ltd</i>	
16:00 - 16:20	<b><u>Increased automation for detection, prevention and mitigation measures</u></b> <ul style="list-style-type: none"> <li>● <u>Vasileios Mavroeidis, University of Oslo</u></li> </ul>
16:20 - 16:40	<b><u>Information sharing techniques, rules, and repository to exchange knowledge</u></b> <ul style="list-style-type: none"> <li>● Decentralized Identities and the role of this technology in CI protection and information sharing by Michele Nati, IOTA</li> </ul>
16:40 - 17:00	<b>Conclusions and Collaboration Planning Day 2</b> <i>Chair: Ilias Gkotsis, Satways Ltd</i>

**Day 3: Friday, April 29th 2022 (9:00-17.00)**  
**Invited Talk & Common Thematic Presentations**

<b>Welcome and Session 1</b> <i>Chair: Habtamu Abie, Norsk Regnesentral</i>	
09:00 - 09:10	Welcome and opening remarks - Giannis Skiadaresis from DG Migration and Home Affairs, Unit B4 - Innovation and Security Research
09:10 - 10:00	<b>Invited talk:</b> The evolution of security and resilience of critical infrastructures in a challenging environment by Georgios Giannopoulos, JRC
<b>Session 2: Standards and regulations</b> <i>Chair: Loredana Mancini, Inlecom Systems</i>	
10:00 - 11:20	<b><u>Standards and Regulations for the Protection of Critical Infrastructures</u></b> <ul style="list-style-type: none"> <li>• PHOENIX – Industrial Cybersecurity Testing Methodology on LSPs by Ganesh Sauba, DNV</li> <li>• Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released by CISA and NIST in the United States by Ilesh Dattani, Assentian</li> <li>• Standards and NIS compliance by Argyro Chatzopoulou, TÜV TRUST IT GmbH</li> <li>• InfraStress: New DIN 91461 standard SPEC document on stress-testing resilience of critical infrastructures by A. Jovanović, Steinbeis EU-VRi, G. Giunta, Ch. Grunewald</li> </ul>
11:20 - 11:40	Coffee break
<b>Session 3: Platform for cascading effects</b> <i>Chair: Isabel Praça, GECAD/ISEP</i>	
11:40 - 13:00	<b><u>Common Platform for Cascading Effects on the Different Critical Infrastructures</u></b> <ul style="list-style-type: none"> <li>• SmartResilience: A methodology and a platform for indicator-based self-generation of cascading scenarios in infrastructure-of-infrastructures by Aleksandar Jovanović (Steinbeis EU-VRi)</li> <li>• Synergies and Challenges towards the integration of Safety and Security requirements in Critical Infrastructure Protection: Examples from the SecureGas and InfraStress projects by Clemente Fuggini (RINA Consulting)</li> <li>• Simulation Framework for Cascading Effects among Urban Critical Infrastructures by Stefan Schauer (AIT Austrian Institute of Technology GmbH)</li> <li>• Mitigating attacks in Collaborative Manufacturing Environments by Adrien Bécue (Head of Innovation, Airbus Cyber Security)</li> </ul>
<b>Session 4: Safety and security, a holistic approach</b> <i>Chair: Rita Ugarelli, SINTEF</i>	
13:00 - 14:00	<b><u>Combined Safety and Security for European Critical Infrastructures</u></b> <ul style="list-style-type: none"> <li>• Hybrid threats and critical infrastructure protection by Päivi Mattila, Laurea</li> <li>• Integrated Security, Safety and Risk Assessment for CIs and will be made by Antonis Kostaridis (SATWAYS)</li> <li>• Pan-European cybersecurity information and incidents sharing and management for Energy Infrastructures by Sofia Tsekeridou (Netcompany-Intrasoft)</li> </ul>
14:00 - 14:40	Lunch Break

<b>Session 5: Cybersecurity awareness</b> <i>Chair: Habtamu Abie, Norsk Regnesentral</i>	
14:40 - 15:40	<b><u>Cyber Security Awareness</u></b> <ul style="list-style-type: none"> <li>• Framework for Cybersecurity Awareness in the Industrial Domain at EDF by Frederic Guyomard (EDF Lab Paris)</li> <li>• Meta-computing in Cybersecurity by Arasaratnam Arasilango (Tech Inspire LTD)</li> <li>• Cyber security awareness in critical infrastructures by Christos Angelidis (konnektable)</li> </ul>
<b>Session 6: Cyber and physical threats</b> <i>Chair: Isabel Praça, GECAD/ISEP</i>	
15:40 - 16:40	<b><u>Advanced Combined Cyber and Physical Threats</u></b> <ul style="list-style-type: none"> <li>• Visible and Emerging Vulnerabilities in Critical Energy Infrastructures by G. Stergiopoulos (Univ. of the Aegean), D. Gritzalis (Athens Univ. of Economics &amp; Business)</li> <li>• Modeling cyber and physical threats in IT&amp;OT integrated systems by Sokratis Katsikas (Director Norwegian Center for Cybersecurity in Critical Sectors (NORCICS), Norwegian University of Science and Technology - NTNU)</li> <li>• Risk Methodology Approach for Combined Cyber and Physical Threats by M. Mohamed (HIBTI)</li> </ul>
16:40 - 17:00	<b>Conclusions and Collaboration Planning Day 3:</b> Giannis Skiadaresis from DG Migration and Home Affairs, Unit B4 - Innovation and Security Research <i>Chair: Habtamu Abie, Norsk Regnesentral</i>

*Enhancing resilience is a team effort...*

*Thank you for your participation!*



## **Catalogue of the projects participating in the 2nd ECSCI workshop**

ANASTACIA project website - [www.anastacia-h2020.eu](http://www.anastacia-h2020.eu)

CONCORDIA project website - [www.concordia-h2020.eu](http://www.concordia-h2020.eu)

CyberSANE project website - [www.cybersane-project.eu](http://www.cybersane-project.eu)

CyberSEAS project website - [www.cyberseas.eu](http://www.cyberseas.eu)

FeatureCloud project website - [www.featurecloud.eu](http://www.featurecloud.eu)

EnergyShield project website - [www.energy-shield.eu](http://www.energy-shield.eu)

ENSURESEC project website - [www.ensuresec.eu](http://www.ensuresec.eu)

EU project website -HYBNET – [www.euhybnet.eu](http://www.euhybnet.eu)

FINSEC project website - [www.finsec-project.eu](http://www.finsec-project.eu)

IMPETUS project website - [www.impetus-project.eu](http://www.impetus-project.eu)

InfraStress project website - [www.infrastress.eu](http://www.infrastress.eu)

PANOPTIS project website - [www.panoptis.eu](http://www.panoptis.eu)

PHOENIX project website - [www.finsec-project.eu](http://www.finsec-project.eu)

PRAETORIAN project website - [www.praetorian-h2020.eu](http://www.praetorian-h2020.eu)

PRECINCT project website - [www.precinct.info](http://www.precinct.info)

RESISTO project website - [www.resistoproject.eu](http://www.resistoproject.eu)

SAFECARE project website - [www.safecare-project.eu](http://www.safecare-project.eu)

SATIE project website - [www.satie-h2020.eu](http://www.satie-h2020.eu)

SealedGRID project website - [www.sgrid.eu](http://www.sgrid.eu)

SecureGas project website - [www.securegas-project.eu](http://www.securegas-project.eu)

SmartResilience project website - [www.smartresilience.eu-vri.eu](http://www.smartresilience.eu-vri.eu)

SPHINX project website - [www.sphinx-project.eu](http://www.sphinx-project.eu)

STOP project website - [www.stop-it-project.eu](http://www.stop-it-project.eu)

7SHIELD project website - [www.7shield.eu](http://www.7shield.eu)

“Over the past decade, the EU has progressively tailored its research and innovation capacity to EU security policy priorities. This capacity plays a key role in addressing the current security challenges and is already helping us in finding solutions to several of the most pressing issue.” (EC staff working document “Enhancing security through research and innovation”, 2021) One of these security priorities is linked with strengthening the resilience of critical and digital infrastructures, which is now supported, at the policy level, by entering into force the two key directives of the EC, that of CER and NIS-2.

These two directives, but also recent attacks against critical infrastructures such as the acts of sabotage against the Nord Stream pipeline, underline the need for coordinated and integrated responses, not only at the policy level but also at the operational level through research and innovation outcomes (as indicated in the aforementioned EC staff working document), which must be disseminated and exploited further to the EU-funded projects’ frameworks or individual research studies’ reports, through raising awareness initiatives, such as the 2nd ECSCI Workshop on CIP.

In the frame of this workshop, the different approaches to security in several different industrial sectors (e.g. finance, healthcare, energy, transport, communications, water) were presented. 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 (related to security modelling, IoT security, artificial intelligence, combating hybrid threats, increased automation for threats detection, prevention and mitigation measures, information and knowledge sharing, etc.).

The workshop proceedings aim to share with scientists, experts, policy-makers and other interested stakeholders in the field of critical infrastructure protection, resilience and security, the knowledge, outcomes and lessons learned, deriving from the keynote speeches, the twenty-one thematic presentations, and the panel discussions.