CybAlliance WP2 Annual National and International Workshops Report 2023

Habtamu Abie, Chief Research Scientist, Sandeep Pirbhulal, Senior Research Scientist,
Norwegian Computing Center/Norsk Regnesentral, November 30, 2023

Abstract
The primary goal of CybAlliance is to build a long-term strategic alliance in advancing research and education on cybersecurity and privacy in healthcare. To achieve this goal, one of the objectives is to organize workshops/webinars and open seminars so that national and international collaborators can meet and discuss the strengths and opportunities of the domain. This objective will be performed under WP2 ("Research Cooperation") Task 2.2 ("Organize the annual workshop/webinar") which aims to organize annual partner and industrial workshops/webinars so that like-minded researchers and stakeholders from national and international collaborators can meet and discuss the strengths and opportunities of the domain. Also, different blogs and social media articles will be created to raise awareness of the potential development in a larger audience. This project through this task will provide networking opportunities and result dissemination platform for education, research, and innovation activities by organizing national and international academic and industrial workshops. This task has also contributed to developing INTPART synergies and healthcare projects collaboration. This report presents the results D2.2 ("Organize the annual national workshop") from this task performed in 2023.

1 Introduction

This report presents the progress and achievements of WP2 Task 2.2 whose aim is to organize annual workshop or webinar so that national and international collaborators can meet and discuss the strengths and opportunities of the cybersecurity and privacy in the telecare domain. The progress includes the organization of industrial and scientific workshops. Section 2 describes the annual industrial workshop. Sections 3, 4, 5, and 6 present CybAlliance and CoTecH Joint Workshop, Scientific Workshops, Webinar, and roundtable discussions, respectively, followed by section 7 Concluding Remarks and Future Work.

2 Annual Industrial Workshop 2023

2.1 Objectives and Organization

The objective of this industrial workshop was to bring together industry practitioners and academics in a joint platform that provide an opportunity for sharing best practices, exchanging new ideas, networking, and identifying areas of collaboration related to cybersecurity in healthcare and resilient infrastructures.

This industrial workshop is organized by two Research Council of Norway (RCN)-funded INTPART projects: International Alliance for Strengthening Cybersecurity and Privacy in

Healthcare (CybAlliance) - NORCICS spinoff and Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway – US Partnership (RECYCIN) and the target audience were CybAlliance and RECYCIN consortium partners, invited academia/industry guests and relevant stakeholders.

2.2 Industrial Workshop Agenda

The workshop was titled "Industrial Workshop on Cybersecurity in Digital Transformation of Healthcare and Resilient Infrastructures (CybAlliance – RECYCIN INTPART Synergy)". It was held on 13th September 2023 at Norsk Regnesentral (NR)/Norwegian Computing Center, Gaustadalléen 23A/B, 0373 Oslo, Norway.

The workshop program contains (i) presentations of two INTPART projects, CybAlliance and RECYCIN, and one Collaborative and Knowledge-building Project, CoTecH – Co-Created Health Technology, (ii) four Industry talks related to secure digitalization of healthcare, security of critical infrastructures, healthcare privacy, and resilience of critical infrastructures, (iii) two networking sessions, (iv) panel discussion on "the role of Artificial Intelligence/Machine Learning in cybersecurity of healthcare and critical infrastructures", and (v) collaboration Ideas session.

Industrial Workshop Agenda

Time	Session Title	Lead	Affiliation
09:30 – 09:45 (*CEST)	Welcome and Coffee	Habtamu Abie Sandeep Pirbhulal	Norsk Regnesentral (NR)
09:45 – 10:00	Opening	Wolfgang Leister Bjørn Axel Gran	NR Institute for Energy Technology (IFE)
10:00 – 10:10	CybAlliance Project	Sandeep Pirbhulal	NR
10:10 – 10:20	RECYCIN Project	Saba Chockalingam	IFE
10:20 – 11:00	Industry Talk 1: Cybersecurity in Critical Sectors — Lessons Learned	Joaquin Garcia-Alfaro	IMT (Institut Mines-Télécom)
11:00 – 11:40	Industry Talk 2: Holistic Cyber Security in relation to Multi-vendor Supply Chains in Critical Infrastructures	Shaun Reardon	DNV
11:40 – 12:40	**Lunch**		
12:40 – 13:20	Industry Talk 3: Is Privacy Enhancing Technologies and Design the Solution?	Einar Martin Aandahl	Ledidi

13:20 – 14:00	Industry Talk 4: Preparing Today's Critical Infrastructure for Increased Exposure to Cyber Threats	Nina Hesby Tvedt	Secure-NOK
14:00 – 14:15	**Networking/Coffee Break**		
14:15 – 14:25	CoTecH – Co-Created Health Technology	Janne Herholdt Dugstad	USN (University of South-Eastern Norway)
14:25 – 14:35	Collaboration Ideas: Editable link	Everyone	Everyone
14:35 – 15:15	Panel Discussion: The Role of Artificial Intelligence / Machine Learning in Cybersecurity of Healthcare and Critical Infrastructures	Habtamu Abie	Sokratis Katsikas *(NTNU)* Alan Saied *(Defendable/BI Norwegian Business School)* Shouhuai Xu *(University of Colorado Colorado Springs)* Sridhar Adepu *(University of Bristol/Reperion)*
15:15 – 15:40	Networking / Collaboration Ideas (Follow-up)	Everyone	
15:40 – 15:45	Concluding Remarks	Sandeep Pirbhulal Saba Chockalingam	NR IFE

Bjørn Axel Gran together with Wolfgang Leister gave an excellent opening talk to set the stage for this workshop. Bjørn Axel Gran emphasized the need for a holistic approach to cyber security (Human-Technology-Organization) in addition to the importance of academia and practitioners coming together for addressing real-world challenges. Wolfgang Leister presented us with Norsk Regnesentral DART's project portfolio involving relevant projects like SFI-NORCICS, Health Democratization, IoTSec.

We had four informative talks from Joaquin Garcia-Alfaro (Télécom SudParis), Shaun Reardon (DNV), Einar Martin Aandahl (Ledidi), and Nina Hesby Tvedt (Secure-NOK®). Joaquin Garcia-Alfaro highlighted the importance of going beyond Confidentiality-Integrity-Availability (CIA Triad) for securing ICS taking into account objectives like Controllability, Observability, and Operability. Shaun Reardon underlined that supply chain blind spots are appearing and shed some light on supply chain vulnerabilities through DNV's hashtag#EnergyCyberPriority2023. Einar Martin Aandahl addressed timely questions: "Why do we need to collaborate/share data in Healthcare? How can this be done ensuring Privacy?". Nina Hesby Tvedt provided ISA/IEC 62443 in a nutshell and how it can help protect yesterday's technology from tomorrow's threats.

Besides the industry talks and project talks (CybAlliance (Sandeep Pirbulal), RECYCIN

(Sabarathinam Chockalingam), and CoTech (Janne Dugstad)), we had an enlightening panel discussion.

2.3 Panel Discussions

The topic of the panel discussion was on "the role of Artificial Intelligence/Machine Learning in cybersecurity of healthcare and critical infrastructures" with the panelists Prof Sokratis Katsikas (NTNU), Dr. Alan Saied (Defendable/BI Norwegian Business School), Dr. Sridhar Adepu (University of Bristol/Reperion), and Dr. Shouhuai Xu (University of Colorado Colorado Springs) and moderated by Dr. Habtamu Abie (Norsk Regnesentral). The discussion was organized in three modules looking into (i) "Large Language Models (LLMs) (like ChatGPT) and Cyber Security in Critical Infrastructures", (ii) "Explainable AI (XAI) and Cyber Security in Critical Infrastructures", and (iii) "Testbeds in Cyber Security for Model Evaluation". The topics discussed at each module are as follows with some key takeaways that include: if LLMs/XAI can help defenders, it can also help attackers, and robustness of XAI against adversarial attacks is crucial:

(i) ChatGPT and Cyber Security in Critical Infrastructures

- Data privacy and compliance are paramount in healthcare. How can AI be applied while ensuring patient data protection and regulatory adherence?
- In what ways can AI help predict and prevent cyber-attacks on medical devices, such as IoT devices used in healthcare?
- What trends do you foresee in the future of AI and ML in critical infrastructures?
- How can ChatGPT and similar AI-powered chatbots contribute to enhancing cyber security in critical infrastructures?
    - What specific applications or use cases can you envision for ChatGPT in the context of cyber security within these critical infrastructures?
    - How does ChatGPT contribute to training personnel in critical infrastructures to recognize and respond to cyber security threats?
- What are the potential challenges and limitations of relying on chatbots like ChatGPT for cyber security in critical infrastructures?
    - Can threat actors use ChatGPT? If so, how?
    - What strategies can organizations employ to ensure that ChatGPT is resilient to adversarial attacks and remains secure in its operation?
- How can organizations ensure that the knowledge base of ChatGPT remains up to date with the evolving threat landscape in these critical sectors?
- What are the privacy and data security considerations when using AI chatbots in critical infrastructures?

(ii) Explainable AI and Cyber Security in Critical Infrastructures

- What is Explainable AI (XAI), and is it particularly important in the context of securing critical infrastructures against cyber threats? If so, why/why not?
    - Can the use of XAI improve confidence and trust in potential stakeholders?
    - What are the key challenges that XAI addresses when it comes to ensuring the security and resilience of critical infrastructures?
- Are there specific regulatory requirements or industry standards that mandate the use of XAI in critical infrastructure cyber security?
- Can threat actors exploit XAI? If so, how?

- How can organizations ensure the robustness and security of XAI models against adversarial attacks in critical infrastructures?

(iii) Model Evaluation and Testbeds in Cyber Security

- What are the primary challenges in evaluating the effectiveness of AI models in enhancing the cyber security of critical infrastructures?
- What are the advantages/disadvantages of using dedicated testbed environments for assessing the performance of AI-driven cyber security solutions in critical infrastructures?
- What role does scalability play in the design and deployment of testbeds for evaluating AI models for critical infrastructure cybersecurity?
- What key performance metrics should organizations focus on when using testbeds to assess the effectiveness of AI models in cybersecurity?

2.4 Collaboration Ideas Session

To continue the momentum and build on CybAlliance-RECYCIN industrial workshop especially in facilitating collaboration between industry and academia, we had a session to discuss collaboration ideas and potential platforms to establish the foundation for future research and collaboration. Following are some key ideas that were discussed:

- Supply Chain Cyber Security in Critical Infrastructures
- Dynamic and Adaptive Risk Management in Smart Homes and Critical Infrastructures
- Digital Twin for Cybersecurity & Secure Digital Twin in Healthcare and other Critical Infrastructures
- Health Data and Information Security
- Trust and Identity Management for Healthcare
- Decentralised Security Solutions for Healthcare Providers

This session will provide inputs to WP4 for developing and enhancing innovation activities at regional, national, and international levels.

2.5 Speakers and Panelists

Prof. Dr. Joaquin Garcia-Alfaro is a full professor at the Networks and Telecommunication Services Department at Télécom SudParis (Institut Mines-Télécom) and an adjunct research professor at Carleton University (Ottawa, Canada). His research interests include a wide range of cybersecurity problems, with an emphasis on the management of formal policies, analysis of vulnerabilities, and enforcement of countermeasures. He holds a double Ph.D. diploma in computer science and a research Habilitation from Sorbonne Université. He is involved in several research projects at National and European levels related to ICT security. He has served as general chair of conferences such as RAID and ATC, and in the technical committee of conferences such as ESORICS and AsiaCCS. He has been the recipient of several awards for excellence in his career. His work has also been disseminated in terms of patents, industrial transfer of proof-of-concept tools, and science divulgation magazines.

Shaun Reardon is the Head of Section for Industrial Systems Cyber Security at DNV and is based in Trondheim, Norway. Formerly a detective at Scotland Yard in London for over 26 years, he specialized in cyber-crime and digital forensics and has a wide range of experience including international organised crime, the UK National Hi-Tech Crime Unit, SO15 counter

terrorism and cyber threats to the critical national infrastructure. At DNV he is a principal consultant delivering cyber security services globally both onshore and offshore.

Dr. Einar Martin Aandahl is CEO of Ledidi. With a combination of extensive research experience and a deep interest in technology, he's always looking to combine the best of these worlds. Einar Martin is a medical doctor specialised in transplantation surgery and has broad research experience in immunology, oncology, and transplantation surgery. He holds a PhD from the University of Oslo in molecular and cellular immunology and has been a postdoctoral fellow at Rockefeller University in New York and at UCSF in San Francisco and a senior research fellow at the University of Oslo. Einar Martin has previously developed software solutions for organ allocation, clinical research projects and registries.

Nina Hesby Tvedt is a Chief Commercial Officer in Secure-NOK, a Norwegian provider of solutions and competencies specialized within industrial cybersecurity. She holds a M.Sc. in Telecom from Norwegian University of Science and Technology from 2004 and has held several technical and management positions within DNV and Nexia Management Consulting before joining Secure-NOK in 2016. Nina Tvedt has an extensive experience with resilience of critical cyber-infrastructure to disruptions and cyber-attacks in industries such as Electric Power, Telecom, Manufacturing, Aerospace, Finance, IT and Oil & Gas.

Prof. Sokratis K. Katsikas was born in Athens, Greece, in 1960. He received the Diploma in Electrical Engineering from the University of Patras, Patras, Greece in 1982, the Master of Science in Electrical & Computer Engineering degree from the University of Massachusetts at Amherst, Amherst, USA, in 1984 and the Ph.D. in Computer Engineering & Informatics from the University of Patras, Patras, Greece in 1987. Currently he is a Professor with the Dept. of Digital Systems of the University of Piraeus, Greece, General Secretary for Communications of the Greek Ministry of Infrastructures, Transport and Networks, and member of the pool of experts of the Institutional Evaluation Programme of the European University Association. He has served as Rector (2003-2006) and Vice-Rector (1997-2003) of the University of the Aegean, Greece, member of the Board of the Hellenic Quality Assurance Agency for Higher Education (2006-2008), member of the Board of the Hellenic Authority for Communications Privacy (2008-2009), Vice-President of the Greek Federation of Associations of University Faculty Members (2009) and national representative of Greece to the Programme Management Committee of the EC FP7 "People" Programme (2007-2009). His research interests lie in the areas of information and communication systems security and of estimation theory and its applications. He has authored or co-authored more than 150 journal publications, book chapters and conference proceedings publications in these areas. He is serving on the editorial board of several scientific journals, he has authored/edited 24 books and has served on/chaired the technical programme committee of numerous international conferences.

Dr. Alan Saied is the head of Cyber Threat Intelligence at Defendable with many years of experience in Cyber Security, Machine Learning and Artificial Intelligence. He is passionate about data, cyber threat Intel, and malware analysis coupled with computer forensics. Alan is also an Associate Professor at BI Norwegian Business School with primary focus on Cyber Security and Machine Learning. He believes that raising awareness through the means of demonstration can deliver better result.

Dr. Shouhuai Xu is the Gallogly Chair Professor in Cybersecurity, Department of Computer Science, University of Colorado Colorado Springs (UCCS). He introduced the Cybersecurity Dynamics approach as foundation for the emerging science of cybersecurity, with three pillars: first-principle cybersecurity modeling and analysis, cybersecurity data analytics, and cybersecurity metrics. His research has won several awards, including the 2019 worldwide adversarial malware classification challenge organized by the MIT Lincoln Lab, and the Association for the Advancement of Medical Instrumentation (AAMI) Best Research Article in 2023. He co-initiated the International Conference on Science of Cyber Security (SciSec) and is serving as its Steering Committee Chair. He has served as Program Committee co-chair for several international conferences. He is/was an Associate Editor of IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), IEEE Transactions on Information Forensics and Security (IEEE T-IFS), IEEE Transactions on Network Science and Engineering (IEEE TNSE), and Scientific Reports. More information about his research can be found at https://xu-lab.org.

Dr. Sridhar Adepu is a Lecturer in Cyber Physical Systems (CPS) Security at the University of Bristol. Previously, he worked as a researcher at CyLab-CMU (USA), UIUC (USA), and SUTD (Singapore). He was a key member of iTrust, a center for research in cyber security, where he operationalised CPS security testbeds for research and educational purposes, focusing on water treatment, water distribution, and smart grid systems. To benefit the global research community, he generated the initial dataset from an operational real-time CPS, which has been downloaded and utilized by over 5000 researchers from more than 50 countries worldwide. Dr. Adepu also organized a distinctive critical infrastructure cyber security exercise that was adopted by NATO (CCDCOE). He serves as the Principal Investigator for a KTP Innovate UK project centered on applied Artificial Intelligence for detecting anomalies caused by cyber-attacks in critical infrastructures. This project involves close collaboration with Synoptix Ltd. Additionally, Dr. Adepu holds the position of National Cyber Security Centre RITICS Fellow (23-24) with a focus on digital twins' security for critical infrastructures. He leads cyber security initiatives within the Supergen Energy Networks Hub in the UK, a significant consortium in the energy networks field. Furthermore, he co-leads the RESICS (Resilience and Safety to attack in ICS and CPS) project, funded by EPSRC in the UK. Notably, Dr. Adepu serves as the head of research for Reperion, an OT security company, and collaborates closely with numerous industrial partners in all of his research endeavours. His research adopts a multidisciplinary approach to address security issues associated with critical infrastructure, demonstrating excellence in applying cyber security and artificial intelligence fundamentals to enhance critical infrastructure security for broader impact.

3 CybAlliance and CoTecH Joint Workshop

The joint workshop titled “Workshop on Security and Privacy in the Healthcare” was held on November 6, 2023, at Norsk Regnesentral/Norwegian Computing Center (NR), Gaustadalléen 23A/B, 0373 Oslo, Norway, 4th floor, Alpa og Omega room.

The objectives of this joint workshop are (i) to meet with the researchers, academicians, and industry to discuss and identify real-world challenges and tentative solutions for security and privacy of healthcare systems, (ii) to facilitate healthcare stakeholders (i.e., hospitals,

municipalities, government sectors, service providers etc) to present real-world challenges in healthcare security and privacy, and (iii) to provide a widen network and collaboration opportunity based on two RCN projects: (a) Project 1: Kapasitetsbygging for digital helse og teknologi gjennom CoTecH - samskapt helseteknologi. Prosjektleder: Janne Herholdt Dugstad. Prosjekteier: Universitetet i Sørøst Norge (USN). Prosjektvarighet: 2022-2028, and (b) Project 2: Internasjonal allianse for å styrke cybersikkerhet og personvern i helsevesenet (CybAlliance). Prosjektleder: Sandeep Pirbhulal. Prosjekteier: Norsk Regnesentral (NR). Prosjektvarighet: 2023-2028.

Meeting Agenda

Time	Session Title	Lead	Affiliation
11:20 – 11:30	Welcome and Reception	Sandeep Pirbhulal Mohsen Toorani	NR USN
11:30 – 12:00	**Lunch**		
12:00 – 12:15	Opening	Wolfgang Leister Janne Herholdt Dugstad	NR USN
12:15 – 12:25	Securing healthy funding for cyber research in healthcare	Lasse Gullvåg Sætre	RCN/NFR
12:25 –12:35	Introduction to CybAlliance	Sandeep Pirbhulal	NR
12:35 – 12:45	Introduction to CoTecH	Janne Herholdt Dugstad	USN
12:45 – 13:10	Talk 1 (CoTecH): Helselogistikk i skyen From Stakeholders about security/privacy challenges in healthcare	Dag Ausen	DNV Imatis
13:10 – 13:35	Talk 2 CybAlliance): Guarding the health of supply chains: Cybersecurity Rx for healthcare	Lasse Andre Lundstad	DNV
13:35 – 13:50	**Coffee**		
13:50 – 14:15	Talk 3 (CybAlliance): Is Information Security Different in Healthcare?	Bian Yang	NTNU
14:15 – 14:40	Talk 4 (CoTecH): Older people's digital insecurity	Yngve Thommesen	Pensionist Forbundet
14:40 – 15:05	Talk 5 (CybAlliance): Exploring Synthetic Data Generation at Cancer Registry of Norway: Motivation, Research Efforts and Preliminary Research Results	Narasimha Raghavan	Kreftregisteret
15:05-15:10	Potential Proposal Opportunity: Video in Healthcare: Really for All?	Till Halbach	NR

15:10 – 15:40	Networking in Groups (based on pre-defined questions)- Menti	Mohsen Toorani Sandeep Pirbhulal	All
15:40 – 15:55	**Coffee**		
15:55 – 16:20	Talk 6 (CybAlliance): Human Interactive Robotics for Healthcare and Resilient Societies	Sabarathinam Chockalingam	IFE
16:20 – 16:55	Panel Discussion with Stakeholders: How to improve security and privacy of Norwegian Healthcare infrastructures	Janne Herholdt Dugstad (Moderator) Dag Ausen Staal A. Vinterbo Yngve Thommesen Hege Rokke	USN DNV Imatis NTNU Pensionist Forbundet Drammen commune
16:55-17:00	Closing Remarks	Sandeep Pirbhulal Mohsen Toorani	NR USN

4 Scientific Workshops 2023

The aim of the scientific workshops is to provide networking opportunities and results dissemination platform for education, research, and innovation activities. The organization and support of these workshops has increased the presence and visibility of the CybAlliance project both nationally and internationally and attracted a lot of attention and collaborations.

4.1 CybAlliance Flagship Workshop – SUNRISE 2023

Habtamu Abie, Vasileios Gkioulos, Sokratis Katsikas, Sandeep Pirbhulal, 1st Workshop on SecUre aNd Resilient digItal tranSformation of healthcarE (SUNRISE 2023) co-located with the 35th Norwegian ICT Conference for Research and Education (NIKT 2023) and will take place on 27-30 November 2023 at the University of Stavanger, Norway.

Abstract: Digital transformation in healthcare is the leveraging of advanced technologies to improving the delivery of care to patients and to coping with new requirements of such delivery, most notably the shift from hospital care to home care. While patient-needs-centric, it also necessarily requires changes and improvements of healthcare-related processes. Whereas various benefits of this transformation are broadly acknowledged, the increased connectivity; the huge volume of -sensitive- health information; and the lack of sufficient cybersecurity awareness and culture among both healthcare professionals and patients result in increased cybersecurity risk and make digital healthcare attractive to cyber criminals and prone to cybersecurity attacks such as phishing, ransomware, distributed denial-of-service attacks, and malware. The increasing connection of medical devices to the Internet, hospital networks and other medical devices expands the attack surface making the patient safety risks higher. The recent COVID-19 pandemic highlighted the interdependence and co-evolutionary dynamic of the cybersecurity and privacy risks in healthcare. All these have raised the need to develop

new solutions to increase the cybersecurity and resilience of the healthcare sector and its supply chain.
The workshop “Secure and Resilient Digital Transformation of Healthcare” will provide a discussion platform for researchers in the field and an opportunity to share novel research on the topic. The target audience also includes healthcare professionals and managers of healthcare organizations. The workshop is organized the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) project as its flagship workshop and is supported by the Center for Research-based Innovation (SFI) Norwegian Center for Cybersecurity in Critical Sectors (NORCICS) project, and the AI-Based Scenario Management for Cyber Range Training (ASCERT) project.

Program
09:00 – 09:10: **Opening Session:** Introduction to the Workshop
Chair: Sandeep Pirbhulal

09:10 – 09:50: **INVITED KEYNOTE 1**
Chair: Sandeep Pirbhulal
Invited Keynote Talk Title: Healthcare 4.0: Data Analytics, Digital Transformation and Cyber Security Perspective
Speaker: Sanjay Mishra, IFE Halden, Norway

09:50 – 10:30: **SESSION 1:** Cybersecurity Skills and Access Control in Healthcare
Chair: Sandeep Pirbhulal

- Training on social media cybersecurity skills in the healthcare context
  Mario Fernández Tárraga, Alejandro David Cayuela-Tudela, **Pantaleone Nespoli**, Joaquin Garcia-Alfaro and Felix Gomez Marmol
- Blockchain-based Access Control for Electronic Health Records
  Khandoker Tahmid Sami and Mohsen Toorani

10:30 – 10:40: **Networking** and Coffee Break

10:40 – 11:20: **INVITED KEYNOTE 2**
Chair: Sandeep Pirbhulal
Invited Keynote Talk Title: Methodology for Automating Attacking Agents in Cyber Range Training Platforms
Speaker: Pantaleone Nespoli, IMT, France

11:20 – 12:00: **SESSION 2**: Privacy Risks, and Resilience in Healthcare Systems
Chair: Sandeep Pirbhulal

- Threat Modeling Towards Resilience in Smart ICUs
  Matteo Große-Kampmann, Christian Baumhör and Thomas Henning
- Characterizing Privacy Risks in Healthcare IoT Systems
  Shuai Li, **Alessio Baiocco** and Shouhuai Xu

12:00 - **CLOSING SESSION**: Conclusion & Planning
Chair: Sandeep Pirbhulal

Keynote Speakers

Dr. Sanjay Misra, a Sr. member of IEEE and ACM Distinguished Lecturer, is a Senior Scientist at the Institute of Energy Technology (IFE), Halden, Norway. Before joining IFE, he was associated with the Computer Science and Communication department of Østfold University College, Halden, Norway. He holds a PhD. in Information & Knowledge Engg (Software Engg) from the University of Alcala, Spain & M.Tech. (Software Eng) from MLN National Institute of Tech, India. His expertise is in Applied Informatics (Cyber Security, Health Informatics, Software Engineering Applications, and Intelligent systems using AI and computational techniques) and has been published (- around 150 JCR/SCIE) in top journals like Computers and Security, Information Processing and Management, Engineering Applications of Artificial Intelligence, Expert Systems, and Applications, etc. He has been amongst the top 2% of scientists in the world (published by Stanford University) for the last three consecutive years, ranked no 2 in the whole of Africa in computer science (as per Elsevier: Scival analysis during 2017-2022) and got several awards for outstanding publications (2014 IET Software Premium Award (UK)), TUBITAK-Turkish Higher Education, and Atilim University). He is Editor in Chief of Int J of Human Capital & Inf Technology Professionals (IGI), IT Personnel and Project Management (IGI), and editor in various SCIE journals (Nature: Scientific Report ((Impact Factor: 4.996), Elsevier: Alex. Engineering ((Impact Factor: 6.626, Q1 7/92)), edited several special issues and 80 books from Springer (65 LNCSs, 4 LNEEs, 3 LNNSs, 3 CCISs), 10 IEEE proceedings and several books. He delivered more than 100 keynotes and invited talks and public lectures at reputed conferences and institutes (he traveled to more than 60 countries).

Dr. Pantaleone Nespoli is a postdoctoral researcher working together with the Department of Information and Communication Engineering at the University of Murcia, Spain, and the SCN team of the SAMOVAR laboratory at Institut Polytechnique de Paris. His research is focused on cybersecurity and cyber defense training, with a particular interest in the detection and response to intrusions, and disinformation in social networks. More info at https://webs.um.es/pantaleone.nespoli

4.2 CybAlliance Supporting Workshops

SecIndustry 2023: Sandeep Pirbhulal, Habtamu Abie, Halvor Holtskog, Sokratis Katsikas, SecIndustry 2023 (The 2nd Workshop on Cybersecurity in Industry 4.0) held in conjunction with the 18th International Conference on Availability, Reliability and Security (ARES) 2023, 30th August 2023. The workshop is supported by the Center for Research-based Innovation (SFI) Norwegian Center for Cybersecurity in Critical Sectors (NORCICS) and the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) project and attracted two keynotes, 9 technical presentations and 3 presentations of supporting and related projects, (i) two (2) keynote speeches by Dr Sabine Delaitre of The Wick, innovation unit of BOSONIT on DocExploit´s Cybersecurity Suite or how to be aware of the security level of your code to build and maintain a more secure one? and by Aditya Raj, Senior Technology Consultant - Distributed Ledger Technology/Blockchain, Fujitsu, Berlin, on Decentralized Trust for Industry 4.0, (ii) nine (9) technical presentations on “Risks, Threats, Forensics and Honeynet in Industrial Control Systems” and on “Cybersecurity, Digital Twin and Obfuscation”, and (iii) three (3) presentations of supporting and related projects (1) Center for Research-based Innovation, Norwegian Center for Cybersecurity in Critical Sectors (NORCICS) by Sokratis Katsikas, NORCICS Director, (2) International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) by Sandeep Pirbhulal, Project Manager, and (3) Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway – US Partnership (RECYCIN) by Saba Chockalingam, Project Manager

CPS4CIP 2023: Habtamu Abie and Silvio Ranise, Luca Verderame, Enrico Cambiaso, Rita Ugarelli, and Isabel Praça, CPS4CIP 2023 (The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection) co-located is co-located with the 28th European Symposium on Research in Computer Security (ESORICS 2023) that takes place 25-29 September 2023. The workshop is supported by the projects of the European Cluster for Securing Critical Infrastructures (ECSCI), Horizon Europe project based on ECSCI EU-CIP (European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection), and three national projects: NORCICS (Norwegian Center for Cybersecurity in Critical Sectors) project funded by the Research Council of Norway under the Center for Research-based Innovation (SFI), RESTABILISE4.0 (Restabilise and Energy: Specialization of Enabling Technologies for Balancing Energy Infrastructures and Systems) project Confunded by START4.0 - Competence Center for security and optimization of strategic infrastructures, CybAlliance (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare) project funded by the Research Council of Norway under the INTPART International Partnerships for Excellent Education, Research and Innovation program. The workshop attracted 9 technical presentations: 3 papers "Approaches and Methodologies for Security Risk Assessment", 4 papers on "Methods for Intrusion and Malware Detections", and 2 papers on "XAI for Security, Privacy and Attack Detection", and 6 ECSCI Supporting Projects Results Presentations

SecAssure 2023: Basel Katt, Habtamu Abie, Sandeep Pirbhulal, Ankur Shukla, SecAssure 2023 (2nd International Workshop on System Security Assurance) co-located with the 28th European Symposium on Research in Computer Security (ESORICS 2023) that took place 25-29 September 2023. The workshop is supported by the Center for Research-based Innovation (SFI) Norwegian Center for Cybersecurity in Critical Sectors (NORCICS) and the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) project. The workshop attracted 5 technical presentations in the areas of cyber range, fork-awareness in Coverage-guided fuzzing, distributed ledger security, trust assumptions in voting systems, and security assurance.

5 Webinar: 5G-Enabled IoT and Digital Twins: Cybersecurity and Resilience

Abstract: "The fifth generation of wireless technology (5G) is the backbone of modern IoT-based critical sectors and it offers several benefits, including high speed, low latency, and greater availability. IoT devices and their related systems are expected to grow in number over the next few years. The 5G-enabled IoT has applications in a wide range of domains, such as transportation, healthcare, smart cities, and energy; however, it is also prone to cybersecurity threats. As a result, efficient and end-to-end security solutions are needed to ensure data integrity, confidentiality, and availability of 5G-enabled IoT networks. Digital twins (DTs), as

virtual representations of a physical object, process, or service, are also receiving significant attention from academia and industry. DT technology is more efficient than simulations since it uses real data to mimic processes; it also provides significant benefits, such as saving costs and enhancing the decision-making process in a variety of application domains. DT technology can help organizations and industries to identify potential cyber threats, such as sensor attacks, spoof-node attacks, hardware manipulation attacks, energy manipulation attacks, sniffing, distributed denial of service, sensitive data leakage, and fault tolerance, by creating virtual clones. However, by creating a DT of any system, the potential attack surface effectively doubles. Therefore, the cybersecurity of 5G-enabled IoT systems employing DT technology, and the opportunities for DTs themselves to mitigate cybersecurity risks, must be considered". This abstract can be found in detail from https://www.mdpi.com/about/announcements/5806

This webinar discussed 5G-enabled IoT and DT technology with respect to cybersecurity and resilience. The webinar is supported by the Center for Research-Based Innovation (SFI), the Norwegian Center for Cybersecurity in Critical Sectors (NORCICS), the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance), and the European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (EU-CIP) projects. What innovation this webinar has resulted can be found in the WP4 annual report.

Webinar Chairs:

- General chair: Dr. Sandeep Pirbhulal, Norsk Regnesentral (Norwegian Computing Center, NR), 0373 Oslo, sandeep@nr.no
- Co-chair: Dr. Ankur Shukla, Institute for Energy Technology, 1777 Halden, Norway,Ankur.Shukla@ife.no
- Co-chair: Dr. Habtamu Abie, Norsk Regnesentral (Norwegian Computing Center, NR), 0373 Oslo, abie@nr.no

Speakers:

- Mr. Emiliano Marquesini, Digital Smart Group, Barcelona, Spain, emiliano@digitalsmartgroup.com
  Presentation: "5G High-Performance Mobile Broadband Kit for IoT and OT-Cybersecurity Mission-Critical Applications and Infrastructure"
- Prof. Joaquin Garcia-Alfaro, Télécom SudParis, Paris, France, joaquin.garcia_alfaro@telecom-sudparis.eu
  Presentation: "Digital Twins and Cybersecurity in Critical Sectors"

6 Roundtable Discussion on Security and Secure Information Exchange in the Healthcare Sector

The roundtable discussion was held Norsk Regnesentral, address Gaustadalléen 23 a, 0349 Oslo, Room: Alfa Omega, Date: 26/01/2023, with the areas of discussion, Cybersecurity in Healthcare, Secure information exchange in Healthcare, Funded projects' collaboration Activities, and Healthcare providers participation in the NESIOT project and the following agenda:

Time (CET)	Duration	Item	Presenter
09:00	20'	Welcome and round the table introductions	ALL
09:20	20'	HEIR Project Presentation	Prof. Hervé Debar
09:40	20'	NORCICS Presentation	Prof. Sokratis Katsikas
10:00	40'	EU-CIP/ ECSCI / NESIOT Presentation	Dr. Habtamu Abie
10:40	20'	**BREAK**	
11:00	20'	CybAlliance	Dr. Sandeep Pirbhulal
11:20	20'	CyberCNI	Prof. Joaquin Garcia Alfaro
11:40	20'	CVPIP	Prof Maryline Laurent
12:00	**60'**	**Lunch Break**	
13:00	20'	JCOP, PHOENI2X - Secure Information Exchange	Dr. Vasileios Mavroeidis
13:20	20'	B-CRATOS	Prof Ilangko Balasingham
13:40	30'	Potential Involvement of NSE/NOKLUS in NESIOT	ALL
14:10	40'	Open Discussion and Collaboration Opportunities	ALL
14:50	30'	Future Collaboration/Co-Innovation Ideation Slot	ALL
15:20	10'	Any other Business - End of the meeting	ALL

The participating projects are:

[NESIOT] The NESIOT (Norwegian Ecosystem for Secure IT-OT Integration) ecosystem is one of the pillars which supports the IT-OT Integration focus area of NORCICS.
More information will soon be available at: https://www.ntnu.edu/norcics

[HEIR] The HEIR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883275 (HEIR).
More information at: https://heir2020.eu/

[NORCICS] The NORCICS (Norwegian Centre for Cybersecurity in Critical Sectors) project has received funding from the Research Council of Norway under The Centre for Research-based Innovation (SFI) scheme
More information at: https://www.ntnu.edu/norcics

[EU-CIP] The EU-CIP project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.
More information at: https://www.eucip.eu/

[CybAlliance] The CybAlliance (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare) project has just been awarded grant from the Research Council of Norway under the "INTPART International Partnerships for Excellent Education, Research and Innovation.
More information at: https://www.forskningsradet.no/en/call-for-proposals/2022/intpart-international-partnerships

[JCOP] The JCOP project has received funding from the European Health and Digital Executive Agency of the European Commission under the Connecting Europe Facility (CEF) programme. Grant Agreement No. INEA/CEF/ICT/A2020/2373266.
More information at: https://jcop.eu/

ECSCI Projects

[ECSCI] The ECSCI cluster is a cluster of 25 EU funded R&D projects, kicked off during the H2020 Work Programme.
More information at: https://www.finsec-project.eu/ecsci

[B-CRATOS] B-CRATOS (Empowering independence through wireless Brain-Connect inteRfAce TO machineS) is an interdisciplinary project reinventing Brain-Machine-Body connectivity awarded funding in the Horizon 2020 FET – Open 2020 cut-off. It unites 1 SME, 3 research institutes and 3 universities. In total, 25 specialists in Neuroscience, Electronics, Biomedical engineering, and AI will work together for 4 years to meet our ambitious goals
More information at: https://www.b-cratos.eu/

[PHOENI2X] The PHOENI2X project has received funding from the European Union's Horizon Research and Innovation Programme under Grant Agreement nº 101070586.
More information at: **https://phoeni2x.eu/**

More information at: https://cybercni.fr/

7 Concluding Remarks and Future Work

This CybAlliance WP2 ("Research Cooperation") National and International Workshops Report 2023 presented the CybAlliance Task 2.2 ("Organize the annual workshop/webinar") progress and achievements D2.2 ("Organize the annual national workshop") in 2023. The achievements include the organization of Industrial Workshop on Cybersecurity in Digital Transformation of Healthcare and Resilient Infrastructures, CybAlliance and CoTecH joint workshop on "Security and Privacy in the Healthcare", CybAlliance flagship 1st Workshop on SecUre aNd Resilient digItal tranSformation of healthcarE (SUNRISE 2023), 3 Supporting Workshops (SecIndustry 2023, CPS4CIP 2023, SecAssure 2023), webinar on 5G-Enabled IoT and Digital Twins: Cybersecurity and Resilience, and roundtable discussion on security and secure information exchange in the healthcare sector.

The project through this task has provided networking opportunities and results dissemination platform for education, research, and innovation, and increased the presence and visibility of the CybAlliance project both nationally and internationally and attracted a lot of attention and collaborations. At the international level the CybAlliance project collaborated with the European Cluster for Securing Critical Infrastructures (ECSCI) a cluster of 35 EU funded projects, **E**U-CIP - European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection 20 partners including the coordinators of recent EU projects in resilient infrastructures in different sectors that are part of ECSCI, and CIPRE-Critical Infrastructure Protection & Resilience Europe which brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe. At the national level CybAlliance project

collaborated with the Norwegian Ecosystem for Secure IT-OT Integration (NESIOT) which brings together multiple stakeholders such as sensor/devices manufacturers, telecom operators, cloud and data analysis solution providers, industrial system operators etc., and to exploit enabling technologies and the secure application of those technologies, and the CoTecH - Co-created Health Technology with a total of 28 partners from the health industry, health services, users and research actors in Viken and Vestfold and Telemark counties, as well as from Sweden and Ireland collaborating on new health technology. In terms of collaboration on innovation the CybAlliance project collaborated on the development and submission of 3+ project proposals to advance digital security in healthcare. Details can be found in “CybAllaince WP4 Annual Report 2023 Innovation and Long-term Sustainability”.

As a future work in 2024 this task will continue to organize an annual workshop, webinar or roundtable discussion, so that researchers can meet and discuss the strengths and opportunities of the cybersecurity and privacy in the telecare domain to maximize the impact of the CybAlliance project on education, research, and innovation.