First International Workshop on Cybersecurity in Healthcare and Medicine held in Dubrovnik as a part of IEEE MeditCom 2023

Hrvoje Belani

Ministry of Health, Directorate for e-Health, Zagreb, Croatia

e-pošta: hrvoje.belani@miz.hr

The 2023 IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) was held from September 4th to 7th 2023 in Hotel Kompas in Dubrovnik, Croatia. The aim of IEEE MeditCom is to "bring together researchers and visionaries in academia, research labs and industry from all over the world to the shores of the Mediterranean Sea, with a technical program that addresses many of the outstanding challenges that exist in the areas of communications and networking" (1). The first two MeditCom editions took place in Athens, Greece (2021, 2022), and the next one will take place in Madrid, Spain (2024). "The IEEE MeditCom 2023 program featured six keynotes and two panels, in which industry leaders and prominent academics gave their vision on the future of wireless communications networks, and 12 technical sessions presenting research results" (2). Prior to the start of the main conference, the program began on September 4th with two half-day tutorials ("Unlocking New Horizons: SDN and Blockchain Synergy in IoT Networks" and "Interplay of AI and Wireless for 6G IoT") and two half-day workshops on the following topics: "Key Technology Enablers for 6G: AI and Intelligent Metasurfaces" and "Cybersecurity in Healthcare and Medicine".

One of two accepted MeditCom 2023 workshops was the First International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), for which the initial proposal has been drafted by the Working Group on Information Security and Cybersecurity within the Croatian Society for Medical Informatics (Croatian acronym: HDMI). Before the final submission of the four-page workshop proposal, six workshop co-organizers have been assembled from three countries in southern Europe: Hrvoje Belani, Directorate for e-Health, Ministry of Health, Zagreb, Croatia; Krešimir Šolić, Department of Medical Statistics and Informatics; Josip Juraj Strossmayer University of Osijek, School of Medicine, Osijek, Croatia; Kristina Fišter, Andrija Štampar School of Public Health, University of Zagreb, School of Medicine, Zagreb, Croatia; Ana Madevska-Bogdanova, Faculty of Computer Science and Engineering, Saints Cyril and Methodius University, Skopje, Republic of North Macedonia; Toni Perković, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Split, Croatia; Tatjana Lončar-Turukalo, Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia.

The first CyHeMe workshop aimed to fosters discussion related to information security and cybersecurity resulting from the need to build secure, reliable and robust systems and services that not only support healthcare and medicine, but also foster well-being, encourage patients and the population in general to live according to healthy lifestyle recommendations, and address the specific safety needs of an aging population. This multidisciplinary workshop aimed to bring together practitioners and researchers from relevant disciplines. Among other objectives, CyHeMe aimed to: 1) develop approaches that support multiple perspectives of information security and cybersecurity in healthcare and medicine; 2) develop or refine methods for achieving and raising cybersecurity of systems and services that promote well-being or health; and 3) identify open research and industry challenges, as well as validation objectives for proposed solutions.

In this workshop, the organizers aimed to raise important questions such as, but not limited to: What are the engineering and management techniques, tools, and processes that are applicable for addressing cybersecurity for e-health? How can we help important stakeholders, such as healthcare and medical professionals, patients, care-givers and policy makers, identify and manage current and emerging cybersecurity risks? How to assess and manage vulnerabilities of users, infrastructure, systems and devices, processes and operations, and policies for healthcare and medicine? Which advanced security techniques need to be applied in health-related and medicine-intensive systems design and implementation? Which are the methods for achieving and raising cybersecurity of systems and services that promote well-being or health? How to address the widening attack space on medical devices and IoT solutions employing emerging technologies? How to gain high-level cybersecurity awareness and become empowered to create and maintain cybersecurity culture in healthcare organizations?

The workshop theme is very timely, as e-health cybersecurity and medical information security show to be of growing importance to healthcare and medicine domains. This theme has been partly covered by the following conferences and workshops in recent years: ENISA eHealth Security Conference 2020 Online Series; Digital Health Informatics Workshop at the 8th Annual Conference of the Industrial Electronics Society (IECON 2022); e-CYberHealth 2022 in Cyprus. Also, some related industry-oriented events will be organized in 2023: HealthSec Summit USA 2023 in Boston, USA; 2nd Annual Healthcare Cyber Security Conference in Sydney, Australia; 7th Annual Medical Device Cybersecurity Conference in Chicago, USA. However, this workshop aimed at novel and sound contributions from both research and public advocacy communities, as well as government and industry experts, while maintaining scientific rigor. Preference have been given to submissions that emphasize informed, topic-relevant and technically sound descriptions of important challenges and problems as opposed to just proposed solutions.

CyHeMe call for papers has been announced at the conference website (1) as well as distributed via social networks and relevant mailing lists, and also to academic and interest groups organizers have identified. By the deadline ten submissions have been received through the EDAS Conference and Journal Management System (3), and among them six full papers (up to 6 pages in IEEE double-column format) have been revised and accepted to be presented at the workshop, after the single blind reviews conducted by at least three reviewers for each paper. The initial CyHeMe program committee had 20 members, and paid special attention to geographical distribution, expertise, seniority, and gender balance. All three Croatian co-organizers are active members of the HDMI Working Group on Information Security and Cybersecurity, as well as the program committee member Mira Hercigonja-Szekeres, University Hrvatsko Zagorje, Krapina, Croatia.

The workshop program has consisted of six 15-minutes presentations. There have been 15 participants at the workshop in total, coming from six countries: Serbia, Republic of North Macedonia, Slovakia, Slovenia, Denmark and Croatia. The workshop agenda has been organized as follows:

- Session 1 on “Human Factors in e-Health Cybersecurity” (14:00-15:30) chaired by Toni Perković from the University of Split, Split, Croatia, with the following four presentations:
  - “Patients' perception of data security in healthcare information systems” (4);
  - “Securing Patient Information in Connected Healthcare Systems in the Age of Pervasive Data Collection” (5);
  - “The Art as a form if raising awareness of data protection in Healthcare and Medicine” (6);
  - “Investigating Privacy and Security Concerns in a Running eHealth Information System” (7).
- Session 2 on “Technical Aspects of e-Health Cybersecurity” (16:00-17:30) chaired by Hrvoje Belani from the Ministry of Health, Zagreb, Croatia, with the following two presentations.
  - “An Investigation of a Replay Attack on LoRaWAN Wearable Devices” (8);
  - “Ontology-Based Cybersecurity for Well-Being, Aging and Health: A Scoping Review” (9).

The workshop has been closed with the one-hour keynote talk on “Emerging Digital Technologies and Risks: Where are the Security Issues when Using AI, Blockchain, and Telemedicine in e-Health?” given by Associate Professor Martin Žagar, PhD, EMBA, a scientific advisor in computer science from the Rochester Institute of Technology (RIT) in Croatia. The workshop atmosphere is shown in Figure 1.

Figure 1. CyHeMe workshop session 1 (on the left) and session 2 (on the right) (photo credit: Hrvoje Belani)

The abstract of the keynote talk, given by prof. Žagar, as shown in Figure 2, has been the following: “We are eyewitnesses of digital transformation in every aspect of our lives, when talking about emerging technologies in e-health, such as Artificial Intelligence (AI), Blockchain, and telemedicine, we talk about numerous benefits in terms of improving patient care, data management, and healthcare efficiency. However, these technologies also introduce specific cybersecurity risks that need careful consideration.

AI systems in e-health often rely on vast amounts of patient data for training and decision-making. This data may include sensitive medical records or diagnostic images. The improper handling of this data, such as insufficient or improper encryption, could lead to data breaches and unauthorized access. AI systems can also be vulnerable to adversarial attacks, where malicious inputs are designed to deceive the AI algorithms, leading to inaccurate diagnoses or treatment recommendations, or may inherit biases present in the training data, leading to unequal treatment or misdiagnoses for certain patient groups. From the Blockchain perspective, smart contracts used in e-health applications may contain vulnerabilities that could be identified by attackers to manipulate transactions or gain access to sensitive data. While blockchain is known for its security and immutability, privacy risks may arise when personal health information is stored on a public blockchain, potentially leading to de-anonymization. Blockchain applications in e-health could also involve supply chain tracking of medical devices or identity management, which could be targeted by attackers to disrupt the healthcare supply chain or engage in identity theft. Finally, telemedicine relies on secure networks for real-time communication between healthcare providers and patients. Weak encryption or vulnerabilities in communication protocols could lead to eavesdropping and unauthorized access to telemedicine sessions. Patient data transmitted during telemedicine sessions may be intercepted, compromising patient privacy and confidentiality.”

DIGITAL TRANSFORMATION IN HEALTHCARE:
INTEGRATING AI, BLOCKCHAIN, AND TELEMEDICINE
Telemedicine Advancement:
Importance: Telemedicine allows remote access to healthcare services, improving accessibility and convenience.
Benefits: Increased reach to rural areas, reduced healthcare costs, timely consultations.
Challenges: Limited physical examination, unequal access to digital infrastructure, reimbursement challenges.

Figure 2. The keynote lecturer assoc. prof. Martin Žagar from Rochester Institute of Technology in Croatia (photo credit: Hrvoje Belani)

This inaugural CyHeMe workshop has taken place on-site, with all the authors presented their research live. The workshop has been executed as a multidisciplinary, half-day workshop and attracted practitioners and researchers across disciplines: information security and cybersecurity, medicine, health sciences, software engineering, computer sciences, art, digital health, digital forensics, criminalistics, public security. Participants from government, public, academic and civil sectors have investigated challenges and exchanged knowledge to ensure the convergence of current and future cybersecurity efforts in health and medicine. The workshop have examined some of the critical factors that enhance information security and cybersecurity of systems and services that promote health and well-being through not only technical, but also organizational and user-driven mechanisms.

The co-organizers, some of them are shown in Figure 3, have rated the first edition of the CyHeMe workshop a success, with 60% paper acceptance rate and authors of six accepted papers coming from four countries in Southern Europe: Croatia, Republic of North Macedonia, Serbia and Slovenia. The organizers would like to express their gratitude to following 15 reviewers of ten paper submissions to the workshop for professionally conducted review and selection processes: Kristina Drusany Starič (Slovenia), Kosjenka Dumančić (Croatia), Mira Hercigonja-Szekeres (Croatia), Hyunbum Kim (South Korea), Tatjana Lončar-Turukalo (Serbia), Ana Madevska Bogdanova (Republic of North Macedonia), Toni Perković (Croatia), Marco Di Renzo (France), George N. Rouskas (USA), Jingtao Sun (Japan), Josip Šabić (Croatia), Krešimir Šolić (Croatia), Vladimir Trajkovik (Republic of North Macedonia), Apostolos Xenakis (Greece), Ivona Zakarija (Croatia).

Figure 3. Some of the CyHeMe workshop co-organizers and authors (on the left; from left to right: Hrvoje Belani, Breda Sturm, Kristina Drusany Starič, Ana Madevska Bogdanova, Tatjana Lončar-Turukalo, Vladimir Trajkovik and Fedor Lehocki) and with a few of the workshop participants at the dinner in "Dubravka 1836" restaurant near the Pile gate to the Old Town (on the right) (photo credit: Hrvoje Belani)

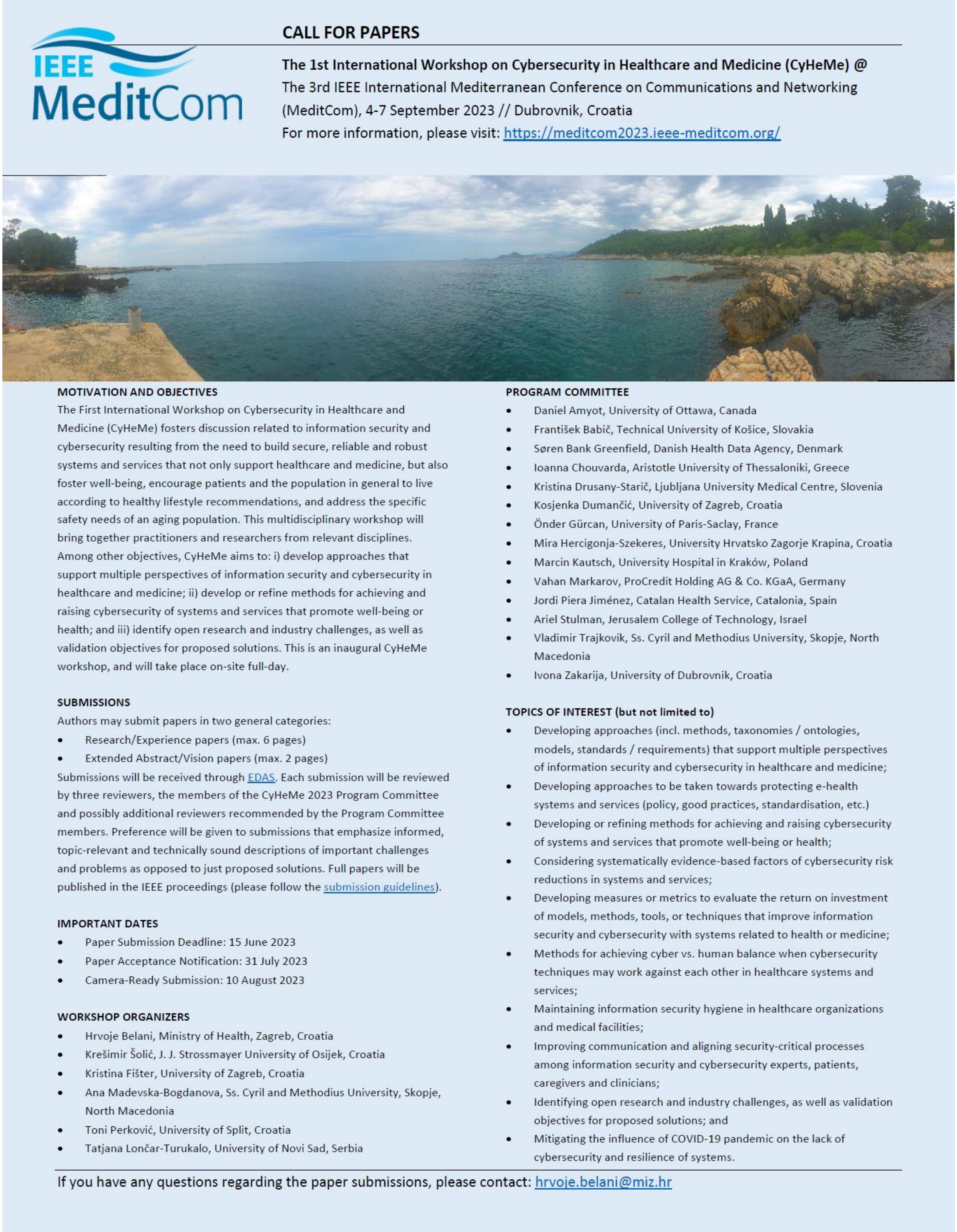
The workshop topics have been a great fit for MeditCom 2023, namely on a "wide range of research topics, spanning both theoretical and systems research along with vertical technologies", especially as e-health and digital medicine crosscut many disciplines and boundaries not conventionally covered in communications and networking. The workshop organizers would like to thank MeditCom 2023 to the organizing, technical program and steering committees for their commitment, assistance and collaboration in making this workshop a reality. The hotel venue, the conference organization and running smoothly have represented a very pleasant working environment for the workshop organizers and participants.

The organizers plan to prepare and realize the second CyHeMe edition in 2024, in the form of an international scientific workshop or a special session within an international scientific conference thematically aligned with the topics of cybersecurity in healthcare and medicine. There are already plans for the third CyHeMe edition in 2025, along with the considerations to make a joint publication in a form of a larger paper, a collection of papers or a book. Cybersecurity in healthcare and medicine will become even more mission-critical in years to come, and therefore needs to be researched thoroughly.

References

1. 2023 IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) website, URL: https://meditcom2023.ieee-meditcom.org/ (access date: September 15, 2023)
2. 2023 IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) Welcome from the General Chairs, URL: https://edas.info/web/ieeemeditcom2023/ (access date: September 15, 2023)
3. 2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) EDAS Conference and Journal Management System, URL: https://edas.info/newPaper.php?c=30709 (access date: September 15, 2023)
4. Antoliš K, Jakšetić D. Patients' perception of data security in healthcare information systems. In: Proc. of the 3rd IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) - 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), September 4-7, 2023, Dubrovnik, Croatia, pp. 24-28 (DOI in preparation)
5. Dimitrievski A, Lončar-Turukalo T, Trajkovik V. Securing Patient Information in Connected Healthcare Systems in the Age of Pervasive Data Collection. In: Proc. of the 3rd IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) - 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), September 4-7, 2023, Dubrovnik, Croatia, pp. 29-33 (DOI in preparation)
6. Drusany Starič K, Sturm B. The Art as a form if raising awareness of data protection in Healthcare and Medicine. In: Proc. of the 3rd IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) - 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), September 4-7, 2023, Dubrovnik, Croatia, pp. 34-38 (DOI in preparation)
7. 7. Denkovski V, Stojmenovska I, Gavrilov G, Radevski V, Trajkovik V. Investigating Privacy and Security Concerns in a Running eHealth Information System. In: Proc. of the 3rd IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) - 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), September 4-7, 2023, Dubrovnik, Croatia, pp. 39-44 (DOI in preparation)
8. Perković T, Šabić J, Zovko K, Šolić P. An Investigation of a Replay Attack on LoRaWAN Wearable Devices. In: Proc. of the 3rd IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) - 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), September 4-7, 2023, Dubrovnik, Croatia, pp. 45-49 (DOI in preparation)
9. Belani H, Šolić P, Perković T, Zovko K. Ontology-Based Cybersecurity for Well-Being, Aging and Health: A Scoping Review. In: Proc. of the 3rd IEEE International Mediterranean Conference on Communications and Networking (IEEE MeditCom 2023) - 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe), September 4-7, 2023, Dubrovnik, Croatia, pp. 50-55 (DOI in preparation)

Appendix A: CyHeMe Call for Papers



IEEE MeditCom

CALL FOR PAPERS

The 1st International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe) @
The 3rd IEEE International Mediterranean Conference on Communications and Networking (MeditCom), 4-7 September 2023 // Dubrovnik, Croatia
For more information, please visit: https://meditcom2023.ieee-meditcom.org/

MOTIVATION AND OBJECTIVES

The First International Workshop on Cybersecurity in Healthcare and Medicine (CyHeMe) fosters discussion related to information security and cybersecurity resulting from the need to build secure, reliable and robust systems and services that not only support healthcare and medicine, but also foster well-being, encourage patients and the population in general to live according to healthy lifestyle recommendations, and address the specific safety needs of an aging population. This multidisciplinary workshop will bring together practitioners and researchers from relevant disciplines. Among other objectives, CyHeMe aims to: i) develop approaches that support multiple perspectives of information security and cybersecurity in healthcare and medicine; ii) develop or refine methods for achieving and raising cybersecurity of systems and services that promote well-being or health; and iii) identify open research and industry challenges, as well as validation objectives for proposed solutions. This is an inaugural CyHeMe workshop, and will take place on-site full-day.

SUBMISSIONS

Authors may submit papers in two general categories:

- Research/Experience papers (max. 6 pages)
- Extended Abstract/Vision papers (max. 2 pages)

Submissions will be received through EDAS. Each submission will be reviewed by three reviewers, the members of the CyHeMe 2023 Program Committee and possibly additional reviewers recommended by the Program Committee members. Preference will be given to submissions that emphasize informed, topic-relevant and technically sound descriptions of important challenges and problems as opposed to just proposed solutions. Full papers will be published in the IEEE proceedings (please follow the submission guidelines).

IMPORTANT DATES

- Paper Submission Deadline: 15 June 2023
- Paper Acceptance Notification: 31 July 2023
- Camera-Ready Submission: 10 August 2023

WORKSHOP ORGANIZERS

- Hrvoje Belani, Ministry of Health, Zagreb, Croatia
- Krešimir Šolić, J. J. Strossmayer University of Osijek, Croatia
- Kristina Fišter, University of Zagreb, Croatia
- Ana Madevska-Bogdanova, Ss. Cyril and Methodius University, Skopje, North Macedonia
- Toni Perković, University of Split, Croatia
- Tatjana Lončar-Turukalo, University of Novi Sad, Serbia

PROGRAM COMMITTEE

- Daniel Amyot, University of Ottawa, Canada
- František Babič, Technical University of Košice, Slovakia
- Søren Bank Greenfield, Danish Health Data Agency, Denmark
- Ioanna Chouvarda, Aristotle University of Thessaloniki, Greece
- Kristina Drusany-Starič, Ljubljana University Medical Centre, Slovenia
- Kosjenka Dumančić, University of Zagreb, Croatia
- Önder Gürcan, University of Paris-Saclay, France
- Mira Hercigonja-Szekeres, University Hrvatsko Zagorje Krapina, Croatia
- Marcin Kautsch, University Hospital in Kraków, Poland
- Vahan Markarov, ProCredit Holding AG & Co. KGaA, Germany
- Jordi Piera Jiménez, Catalan Health Service, Catalonia, Spain
- Ariel Stulman, Jerusalem College of Technology, Israel
- Vladimir Trajkovik, Ss. Cyril and Methodius University, Skopje, North Macedonia
- Ivona Zakarija, University of Dubrovnik, Croatia

TOPICS OF INTEREST (but not limited to)

- Developing approaches (incl. methods, taxonomies / ontologies, models, standards / requirements) that support multiple perspectives of information security and cybersecurity in healthcare and medicine;
- Developing approaches to be taken towards protecting e-health systems and services (policy, good practices, standardisation, etc.)
- Developing or refining methods for achieving and raising cybersecurity of systems and services that promote well-being or health;
- Considering systematically evidence-based factors of cybersecurity risk reductions in systems and services;
- Developing measures or metrics to evaluate the return on investment of models, methods, tools, or techniques that improve information security and cybersecurity with systems related to health or medicine;
- Methods for achieving cyber vs. human balance when cybersecurity techniques may work against each other in healthcare systems and services;
- Maintaining information security hygiene in healthcare organizations and medical facilities;
- Improving communication and aligning security-critical processes among information security and cybersecurity experts, patients, caregivers and clinicians;
- Identifying open research and industry challenges, as well as validation objectives for proposed solutions; and
- Mitigating the influence of COVID-19 pandemic on the lack of cybersecurity and resilience of systems.

If you have any questions regarding the paper submissions, please contact: hrvoje.belani@miz.hr