ISCRAM 2023
University of Nebraska at Omaha's College of Information Science & Technology
Omaha, Nebraska, USA

TRACK: Cybersecurity, Crisis Response & Management and Societal Resilience

20th International Conference on INFORMATION SYSTEMS FOR CRISIS RESPONSE AND MANAGEMENT

"Theme: Building Humanitarian Technologies for our Emerging Future + Building Resilient Societies"

Workshops and Doctoral Symposium May 28th, 2023

Conference May 28th-31th, 2023

Omaha, Nebraska - USA
The University of Nebraska at Omaha (UNO)
http://ISCRAM2023.NET

INTRODUCTION TO THE TRACK

Societal security and resilience are associated with civil protection, often involving multiple agencies, including the police, fire services, health service, and volunteer organizations. With the impact of technology, digital security and resilience have become significant challenges for organizations, society, and governments. Cybersecurity is a critical capability within organizations, particularly relevant in critical infrastructure sectors, and is an important facet of the governance of nation-states. The power grid, the transport network and

information and communication systems are among the so-called "critical infrastructures" essential to maintaining vital societal functions. Damage or destruction of critical infrastructures by terrorism and criminal activity may negatively affect the security and citizens' well-being. Major cyberattacks on critical infrastructure s, such as power, gas, and water stations, as well as transportation control systems, have become the new face of cyberwarfare.

Lapses in cybersecurity increase the potential for such attacks to impact society at large. Ukraine, for example, suffered several successive power outages before the invasion due to a Supervisory Control and Data Acquisition (SCADA) cyberattack. After the invasion, Russian hackers compromised several important Ukrainian organizations, including nuclear power companies, media firms and government entities, according to Microsoft. On May 7, 2021, Colonial Pipeline suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline, and as a result, the company halted all pipeline operations to contain the attack. Overseen by the FBI, it paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million) to restore the system. Also, the U.S. government has indicated that cyber-terrorism has perpetrated several cyber-attacks on American nuclear power plants but did not share the details.

Artificial Intelligence (AI) and Machine Learning (ML) provide advanced cyber defense tools and detection methods of sophisticated and novel attacks, including insider threats and pre-existing infections, without the traditional time-consuming and unreliable technics like restrictions, rules, signatures, or lists of well-known vulnerabilities. But attackers can attack directly in the AI and ML model by manipulating inputs that change the learning results instead of directly attacking the cyber defense system. Also, they can use AI and ML to find weaknesses, learn what can be fixed, monitor what cannot be fixed, and understand how they can be attacked. These attacks pose security concerns because they could be used to attack ML systems, even if the adversary has no access to the underlying model. Attacker brings very slight modifications into the physical domain to subvert ML system, e.g., 3D printing special eyewear to fool facial recognition system or with a perturbation in the form of only black and white stickers, can attack a real stop sign, causing targeted misclassification of self-driving cars.

Emerging threats and unconventional attacks have exposed the limits of traditional risk assessment and risk mitigation efforts. In addition, general emergency management remains woefully oblivious to these growing threats. Failing to plan for cyber threats as part of emergency management procedures is detrimental to national security. Improving resilience from cyberattacks must become a priority for authorities around the globe. Specifically, cybersecurity needs the attention of all policymakers and emergency planners. To be truly effective, emergency management planners must incorporate cybersecurity into their framework. It must be noted that Integrating cybersecurity into an emergency management program is no different than any other risk or potential emergency incident. So, as this risk continues to increase, we will start to see more physical emergencies (industrial accidents, loss of power, nuclear and radiation accidents and incidents, etc..) triggered by cybersecurity attacks.

Thus, in this track, we invite theoretical and empirical papers using technical or social approaches that address the intersection of cybersecurity and crisis response/management and other emerging issues in this area. Research works that use a typical cybersecurity analysis approach but can show its relevance for emergency management are our interests. We welcome all research methodologies and thought pieces that challenge extant thinking. We also, in particular, invite papers that focus on the themes of ISCRAM 2023.

Keywords: Cybersecurity, emergency management, societal security, algorithms AI and machine learning

TRACK TOPICS

Possible topics of interest for this track include the following:

- Cybersecurity-emergency management cascading events

- Emergency management-cybersecurity cascading events
- Emerging Cybersecurity Issues affecting Societal Security
- Protecting data privacy and security that are relevant for emergency management
- Cybersecurity aspects of Societal Security
- Cybersecurity awareness in the emergency management context
- Qualitative and quantitative analysis concerning cybersecurity that are relevant for emergency management
- Economic analysis of investing in cybersecurity in emergency management organizations
- Case studies and teaching case that discuss the inter-relationship between cybersecurity and emergency management
- The use of machine learning and artificial intelligence and other technologies in cybersecurity-emergency management scenarios
- The inter-relationship between emergency management and security incident response, along with the forensic investigation of digital systems that within the emergency management ecosystem
- Critical infrastructure cyber incident response plan
- Emergency management services in the cybersecurity sector using best practices and effective measures
- Emergency management services in the cyber risk assessment using best practices and effective measures
- Education in emergency management services in cyber security
- Exercise in emergency management services in cyber security
- Lessons learned by cybersecurity and emergency management
- Emergency management cyber situational awareness (cyberinfrastructure resources, events, information, individual actions, emergency management tasks, future plans, etc.)
- The inter-relationship between emergency management and cybersecurity to mitigation, preparedness, response and recovery of incidents
- Emergency management framework that integrates cyber situational awareness (position, tools, methodologies, use cases)
- Guidelines and roadmap for cyber security concerns for each particular emergency management task
- Adversarial attacks and defenses and their relationship to emergency management

AUTHORS

To attract potential authors to submit papers in this track we will promote the track in each track-chair´s networks, social media of our institutions and our professional social media channels, AIS mailing lists, ISCRAM 2023 social media channels,

REVIEWER BOARD

- Dr. Per-Arne Andersen, Associate Professor in Cybersecurity and Researcher in Centre for Artificial Intelligence Research (CAIR) and CIEM at University of Agder Norway
- Sindisiwe Maguthswa, Researcher at Centre for Integrated Emergency Management at University of Agder, Norway
- Colonel (INF) Dimitrios Pissanidis PhD c., Hellenic National Defence General Staff, Stratopedo Papagou, Mesogeion 227-231, 15561 Athens, Greece, d.pissanidis@ist.edu.gr
- Major, Dimitrios Taketzis PhD c., Hellenic National Defence General Staff, Stratopedo Papagou, Mesogeion 227-231, 15561 Athens, Greece, d.taketzis@hndgs.mil.gr
- Police Captain Georgios Gkougkoudis PhD c., Operational Analyst at Europol, European Cybercrime Centre, Europol Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands, g.gkougkoudis@hellenicpolice.gr

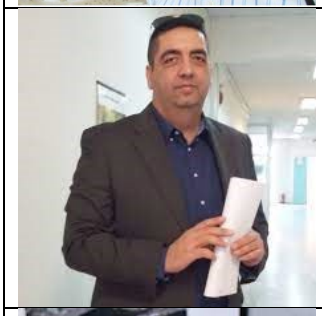
TRACK CHAIR

Prof. Lazaros Iliadis is a Professor of Applied Informatics, Democritus University of Thrace, School of Engineering, Department of Civil Engineering, Faculty of Mathematics, Programming and general courses, Lab of Mathematics and Informatics (ISCE). Head (elected) of the Civil Engineering Department and Member of the Deanery of the School of Engineering of the Democritus University of Thrace. Research interests cover several aspects of Computational Intelligence, Expert Systems, Multiagent Systems, Fuzzy Theory, Clustering, and Support Vector Machines, focusing mainly on applications in Decision Support Systems, Pattern Recognition, Neural Networks, Machine Learning, Intelligent Optimization and real-world problem solving.

CORRESPONDING-CHAIR

Dr. Konstantinos Demertzis is a Postdoctoral Researcher in Computational Intelligence in Cyber Security at the Democritus University of Thrace. He holds PhD in Computational Intelligence, MSc in Communication & Computer Networking Technologies, MSc in Cyber Security and Big Data and BSc in Military Studies with expertise in Informatics. He has five years of teaching experience at the level of Assistant Professor in undergraduate and postgraduate programs of various departments of Greek Universities. His research interests are Computational Intelligence, Big Data, Network Security, Malware Analysis and Critical Infrastructure Protection. He has published relevant research in many scientific journals and international conference proceedings.

The additional co-chairs have a wide range of experience in cybersecurity management, emergency management.

	**Track Chair** Prof. Lazaros Illiadis liliadis@civil.duth.gr Democritus University of Thrace, Greece
	**Corresponding Chair** Dr Konstantinos Demertzis* kdemertz@fmenr.duth.gr Democritus University of Thrace
	**Co-Chair** Prof. Jaziar Radianti jaziar.radianti@uia.no Dept of Information Systems, University of Agder Norway and Centre for Integrated Emergency Management

	**Co-Chair** Ass. Prof. Ioannis Dokas idokas@civil.duth.gr Democritus University of Thrace, Greece
	**Co-Chair** Asst. Prof. George Grispos ggrispos@unomaha.edu University of Nebraska at Omaha

**Corresponding Chair*

ISCRAM

ISCRAM 2023

University of Nebraska at Omaha's College of Information Science & Technology
Omaha, Nebraska, USA