Cyber-Social Security Through Social Sensing: An Interdisciplinary Approach to Cyberbullying and Urban Security

Luca Mainetti
Università Del Salento
Lecce, Italy
luca.mainetti@unisalento.it

Carmelo Ardito
LUM Giuseppe Degennaro
Casamassima (BA), Italy
ardito@lum.it

Donatella Curtotti
Università degli Studi di Foggia
Foggia, Italy
donatella.curtotti@unifg.it

Tommaso Di Noia
Politecnico di Bari
Bari, Italy
tommaso.dinoia@poliba.it

Angelo Corallo
Università Del Salento
Lecce, Italy
angelo.corallo@unisalento.it

Eugenio Di Sciascio
Politecnico di Bari
Bari, Italy
eugenio.disciascio@poliba.it

Patrizia Guida
LUM Giuseppe Degennaro
Casamassima (BA), Italy
guida@lum.it

Wanda Nocerino
Università degli Studi di Foggia
Foggia, Italy
wanda.nocerino@unifg.it

***Abstract*— The *CSS – Cyber Social Security* research project described in this abstract paper aims to tackle cyberbullying and urban security challenges through an innovative "Social Sensing" approach, leveraging data from social networks and urban sensors. By integrating diverse data sources, the project provides a comprehensive understanding of social dynamics and risky behaviors. Key partners, including *Università Del Salento, Università LUM Giuseppe Degennaro, Politecnico di Bari,* and *Università degli Studi di Foggia,* contribute specialized expertise in data extraction, analysis, and legal compliance. The project is structured into phases of data extraction, behavior analysis, and preventive measures, ensuring privacy compliance. This interdisciplinary effort combines computer science, psychology, law, and engineering to address cyber-social risks effectively. The outcomes of the project include advanced analytical tools, guidelines for data privacy, and strategies for early detection and prevention of cyberbullying.**

Keywords*— *Social Sensing, Cyberbullying Prevention, Urban Security, Data Analytics, Interdisciplinary Research.

I. INTRODUCTION

Cyberbullying has emerged as a significant global issue [1], exacerbated by the widespread use of social networks providing new avenues for such behavior to manifest 0. Traditional measures are often insufficient to address the complexities of this phenomenon, which transcends the digital and physical realms. The proposed research project under the extended university partnership SERICS, focusing on "Spoke 3 - Attacks and Defences," aims to fill this gap by leveraging the innovative paradigm of "Social Sensing." This approach involves the collection, analysis, and interpretation of data generated by users through their online and offline social interactions.

The motivation behind this project is twofold. Firstly, it seeks to understand the intricate dynamics of social behavior and identify potential risks associated with cyberbullying and urban security. Secondly, it aims to develop effective preventive measures by integrating diverse data sources, including social networks, environmental cameras, and messaging platforms like Telegram. This holistic approach promises to provide a multi-dimensional perspective crucial for comprehending and mitigating cyber-social risks.

The remaining of this paper is organized as it follows. Section II characterizes the project from different perspectives, i.e., originality, methodology, organization and approach. Section III introduces the main activities of the project that are carried out by the partners described in Section IV. Section V briefly concludes the paper.

This work is funded by the CSS – Cyber Social Security project. Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 3 "Attacks and Defences" (Universita' degli Studi di Cagliari) ammesso a finanziamento con Avviso Pubblico nr 341 del 15-02-2022 "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU – CUP: F53C22000740007.

II. PROJECT DESCRIPTION

Cyberbullying has become a pervasive issue worldwide. The project stands out by addressing this problem through the integration of social and urban data, offering a novel perspective that aligns with recent findings in the field of social dynamics and cybersecurity. This approach not only addresses the immediate issue of cyberbullying but also contributes to a broader understanding of how digital interactions reflect offline behaviors. The following subsections describe project characteristics.

A. Originality

The originality of the CSS project lies in the application of the Social Sensing paradigm to manage cyber-social risks. Unlike traditional approaches that treat cyber and urban data in isolation, CSS integrates these data streams to gain comprehensive insights into social behaviors. This innovative methodology is particularly relevant in addressing the dual challenges of cyberbullying and urban security, which are increasingly intertwined in the digital age.

B. Methodology

The project employs a robust methodological framework designed to monitor relational, communicative, and behavioral aspects through diverse data sources. By using social networks, environmental cameras, and Telegram channels, the project captures a wide range of social interactions. These interactions are analyzed to identify correlations between digital and urban behaviors, particularly focusing on violent actions. This structured approach ensures a thorough understanding of the social landscape, enabling targeted interventions.

C. Organization

The project is organized into several phases, each contributing to a comprehensive understanding and management of cyber-social risks. Initially, data extraction focuses on gathering information from social and urban sensors. This is followed by detailed data processing to

identify patterns and correlations. The final phase involves the development and implementation of predictive models and preventive strategies, ensuring compliance with privacy regulations throughout the process.

D. InterdisciplinaryApproach

CSS exemplifies an interdisciplinary approach by integrating computer science, psychology, law, engineering, and social sciences. This synergy allows for a comprehensive analysis of cyber-social risks, utilizing diverse methodologies to address complex issues effectively.

Strategically addressing cyber-social risks, the project focuses on identifying, analyzing, and responding to these threats. This structured approach ensures a thorough understanding of the social and urban contexts, aiming at proposing effective and targeted solutions.

Combining data from various sources provides a nuanced understanding of cyberbullying and urban security. This comprehensive perspective ensures that both online and offline dynamics are considered, leading to well-rounded solutions.

III. Project Activities

The project activities are structured to ensure thorough coverage different aspects of cyber-social risk management. Each work package, described in the following subsections, is designed to address a specific component of the research.

A. Innovations for Cyber Social Detection

The initial phase focuses on developing methods for extracting data from both social and urban sensors. This involves identifying relevant data sources and creating algorithms to gather this information reliably. The extraction process aims to ensure robustness and accuracy, accommodating various data formats from social networks, messaging apps, and urban sensors.

B. Innovations for Cyber Social Response

Once the data is extracted, the next phase involves processing and analyzing these data streams to understand social behaviors and urban dynamics. Advanced algorithms and tools are developed to identify behavioral patterns and potential threats. This phase emphasizes the creation of metrics and instruments for evaluating online social behavior and urban security trends. The objective is to detect and respond to cyber-social risks effectively.

C. Innovations for Cyber Social Prevention

In the final phase, the project aims to develop preventive measures and protocols. This includes designing systems for real-time monitoring and rapid response to potential threats. It also involves establishing guidelines to ensure compliance with privacy regulations and ethical standards. The prevention strategies are informed by the insights gained from the previous phases, ensuring they are grounded in a deep understanding of the cyber-social landscape.

IV. Project Partners and Their Contributions

Each partener has defined roles and responsibilities in the project. By combining their unique strengths, these partners work synergistically to address the project goals comprehensively. Their collaboration ensures that the project leverages a broad spectrum of expertise, from technical innovation to legal compliance and psychological insights, thus providing a robust framework for managing cyber-social risks.

A. Università Del Salento (UNISALENTO)

CORE Lab and CRLab at UNISALENTO specialize in data analysis and algorithm development for social data extraction. Their primary contribution involves developing prototypes for social sensor data extraction. They also play a significant role in processing and analyzing social data, leading the effort in defining response protocols and prevention strategies.

B. Università degli Studi di Foggia (UNIFG)

The Department of Law at UNIFG ensures that all activities comply with legal standards, focusing on privacy and data protection. They develop guidelines for ethical data management and contribute to the formulation of prevention strategies, ensuring that the project outputs are both effective and compliant with legal requirements.

C. LUM Giuseppe Degennaro (LUM)

The Departments of Law and Engineering at LUM focus on data privacy, security, and legal frameworks, ensuring GDPR compliance. LUM Enterprise provides digital solutions and supports technology transfer. Their contributions include identifying data sources, developing extraction methodologies, and ensuring legal compliance. They also bring expertise in human-centered design and contribute to the development of user interfaces for the system.

D. Politecnico di Bari (Poliba)

SisInf Lab at Poliba brings expertise in AI and machine learning. They lead the development of algorithms and infrastructure for urban data extraction. POLIBA plays a crucial role in analyzing urban data and integrating the findings into the overall platform, ensuring that the project leverages cutting-edge technological solutions.

V. Conclusion

The CSS project, through a multidisciplinary and holistic approach and by integrating advanced methodologies and technologies, seeks to provide comprehensive solutions to the challenges of cyberbullying and urban security, ensuring ethical compliance and contributing to the socio-economic and cultural development of the country. It is highly coherent with the themes and objectives of the iCities 2024 conference. It addresses critical issues related to smart cities, data analytics, cybersecurity, interdisciplinary research, and social impacts, promising to generate fruitful discussion at the conference.

References

[1] N. Davidovitch and R. Yavich, "The association between social media use, cyberbullying, and gender," Problems of Education in the 21st Century, vol. 81, pp. 776-788, 2023. doi: 10.33225/pec/23.81.776.

T. K. H. Chan, C. M. K. Cheung, and Z. W. Y. Lee, "Cyberbullying on social networking sites: A literature review and future research directions," Information & Management, vol. 58, no. 2, 2021. doi: 10.1016/j.im.2020.103411.