Privanova

RESEARCH & CONSULTING

ADVANCING CYBERSECURITY COLLABORATION: INTRODUCING THE LAW ENFORCEMENT CLUSTER

Privanova's contribution to the Fifth session of the Ad Hoc Committee (UN Convention on countering the use of ICTs for criminal purposes)

Vienna, 20-21/06/2023

CONTACT

privanova.com

contact@privanova.com

linkedin.com/company/privanova

Acknowledgments

On behalf of Privanova's team, we would like to express our gratitude for the opportunity to submit our written contribution to the Fifth intersessional consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, to be held on 20 and 21 June 2023 in Vienna.

We would like to thank the Committee Chair and the Secretariat for the organisation of the intersessional consultations with multi-stakeholders.

We would also like to express our appreciation for the support and ideas provided to us during the preparation of this contribution by the coordinators and consortium partners of Privanova's cybercrime-related EU-funded research projects including: CC-DRIVER [Grant ID 883543], TRACE [Grant ID 101022004], CYBERSPACE [Grant ID 101038738], MARVEL [Grant ID 957337], POLIIICE [Grant ID 101073795], and CYRENE [Grant ID 952690].

Finally, we would like to mention the support we have received from the coordinators of EU-funded projects, members of the Law Enforcement Cluster. Currently managed under Privanova's leadership as part of the CYBERSPACE project, the Law Enforcement Cluster includes the following interdisciplinary R&D initiatives of significance to the global law enforcement community: CC-DRIVER [Grant ID 883543], COPKIT [Gant ID 786687], DARLENE [Grant ID 883297], INSPECTr [Grant ID 833276], LOCARD [Grant ID 832735], PREVISION [Grant ID 833115], PROTAX [Grant ID 787098], CYBERSPACE [Grant ID 101038738], RAYUELA [Grant ID 882828], ROXANNE [Grant ID 833635], TRACE [Grant ID 101022004], POLIIICE [Grant ID 101073795], CYCLOPES [Grant ID 101021669], HEROES [Grant ID 101021801], Tools4LEAs [Grant ID 101036219], NOTIONES [Grant ID 101021853], STARLIGHT [Grant ID 101021797], FREETOOL [Grant ID 821947], GRACE [Grant ID 824521], LAW-GAME [Grant ID 101021714], CTC [Grant ID 101036276], CEASEFIRE [Grant ID 101073876] and EU-HYBNET [Grant ID 883054].

Introduction

Privanova, a pioneering research and development consultancy, serves at the juncture of privacy, technology, and policy. Specialising in the scrutiny of legal, technological, ethical, and policy-related issues within the field of cybercrime, it provides a distinct perspective deeply rooted in the expertise of its team of former UN, INTERPOL, and EU professionals engaged in large-scale, interdisciplinary research projects.

Under the auspices of Privanova's EU-funded CYBERSPACE project, operates the Law Enforcement Agency (LEA) Cluster, incorporating numerous cybercrime-focused projects. As the orchestrating entity, Privanova facilitates cooperation among these projects, aiming to foster shared learning, promote collaborative research, and increase the impact of collective findings.

The LEA Cluster stands as a unique collective operating at the intersection of privacy, technology, and policy, actively addressing the pressing challenges of cybercrime. By synthesising diverse expertise from various sectors – from academia to industry, law enforcement, and policy-making – we work to create an interdisciplinary dialogue that leads to practical, well-rounded solutions.

Our contribution to the Fifth Intersessional Consultation of the UN's Ad Hoc Committee builds upon our previous participation in the First Intersessional Consultation held in Vienna earlier this year. The document we present today seeks to engage with the key issues slated for discussion during the fifth session of the Ad Hoc Committee. These encompass international cooperation, provision of technical assistance, cybercrime prevention measures, and the practical aspects of implementing these strategies.

Our ambition is to provide a comprehensive and practical perspective on these issues, fuelled by our unique experiences and the innovative approaches we have developed within our wide-ranging, interdisciplinary research projects. We trust that our insights will make a valuable contribution to the ongoing discourse surrounding the use of information and communication technologies for criminal purposes.

Recommendations

Foster Interoperability of Cybercrime Prevention and Detection Platforms

The escalating complexity and frequency of cybercrime necessitate a coordinated and collaborative international response. We, the members of the Law Enforcement Agency (LEA) Cluster, recommend that the UN Ad Hoc Committee focus on fostering the interoperability of cybercrime prevention and detection platforms, building on the existing work and knowledge shared within our cluster.

The rapid advancement of technology has brought forth an array of sophisticated tools developed by diverse entities worldwide, including those created by EU-funded projects. However, the full potential of these tools can only be realised when there is compatibility and seamless interaction between them. As such, our recommendation calls for the establishment of global standards or protocols that ensure the interoperability of different platforms.

For instance, the CYBERSPACE project [Grant ID 101038738], funded by the EU through the Horizon 2020 program, is one initiative that has shown the significance of interoperable systems. By enabling LEAs to improve their cyberattack reporting mechanisms and collaboration efforts, the project has delivered a more effective response to cybercrime.[1]

Similarly, the TRACE project [Grant ID 101022004] is another demonstration of the value of interoperability. The project has successfully analysed illicit financial flows, using an interoperable platform that allows seamless integration of information from various sources.[2]

By focusing on interoperability, the UN Ad Hoc Committee can foster global cooperation and effectively respond to the challenges posed by cybercrime. It will aid in the optimal use of resources, knowledge, and expertise across countries, thus enhancing our collective ability to counter cyber threats.

---

[1] TRACE Project. (2023). Identifying, analysing and solving Illicit Money Flows. Retrieved from: https://cordis.europa.eu/project/id/101022004

[2] CYBERSPACE Project. (2023). Enhancing cybersecurity, improving cooperation and the reporting of cyberattacks in the EU. Retrieved from: https://cordis.europa.eu/project/id/101038738

Establishing a Unified System for Reporting Cybercrimes

Cybercrime, a universal threat with ever-growing implications, requires a consistent and globally unified approach to its reporting. The Law Enforcement Agency (LEA) Cluster recommends the establishment of a standardised, accessible, and globally unified system for reporting cybercrimes to the UN Ad Hoc Committee. This system should encourage victims to report incidents, ultimately leading to improved data and more effective strategies to combat these crimes, while ensuring privacy and safety.

The complexities of reporting cybercrime often deter victims, allowing cybercriminals to continue their activities undetected. Consequently, it is essential to streamline the reporting process, making it more accessible and comprehensible for all.

EU-funded projects like TRACE have been instrumental in providing solutions for the identification, analysis, and solving of illicit money flows. It has developed tools for reporting financial crimes, which can serve as a model for reporting cybercrimes.

Similarly, the CYBERSPACE project has focused on enhancing cybersecurity and improving cooperation in reporting cyberattacks within the EU. Lessons learnt from this project can inform the design of a globally unified reporting system.

The LEA Cluster, therefore, recommends the UN Ad Hoc Committee to consider prioritising the development of a unified, accessible and user-friendly cybercrime reporting system that safeguards the privacy of victims, while enabling improved data collection and strategic action against cybercriminal activities.

Privanova

RESEARCH & CONSULTING