PRECINCT

PRECINCT Conference

on

Critical Infrastructure Protection, Cybersecurity and Crisis Management

Day 1 – May 16th

AGENDA

Time	**Topic**	**Speaker**
9:00 – 9:30	Welcome and Registration	**PRECINCT Consortium**
9:30 – 10:00	Opening of the Conference	**Ms. Natalja Miolato**, *Project Advisor at the Research Executive Agency*
10:00 – 11:00	Protecting Critical Infrastructures facing Hybrid Threats	Chair: **Dr. Stefan Schauer,** *Senior Researcher for Security & Communication Technologies at AIT* Speakers: • **Dr. Päivi Mattila,** *Director of Security Research Program & EU-HYBNET project coordinator* • **Gilda de Marco,** *R&D - European Projects at Insiel* • **Rafa Company,** *Director of Safety and Security at Valencia Port*
11:00 – 11:15	Audience Q&A	**Dr. Stefan Schauer,** *Senior Researcher for Security & Communication Technologies at AIT*
11:15 – 11:30	EU-CIP: a novel pan European knowledge network for Resilient Infrastructures.	**Dr. Gabriele Giunta,** *Head of the Smart Transport and Infrastructures Unit with the IS3 R&D Lab at ENGINEERING*
Coffee break		
11:30 – 12:30	Living Lab Methodology - Innovative Threat Response	Chai: **Mrs. Shirley Delannoy,** *Researcher, VIAS Institute* Speaker: • **Thomas de Meester,** *Innovation Specialist/Product Owner, IMEC*
12:30 – 12:45	Audience Q&A	**Mrs. Shirley Delannoy,** *Researcher, VIAS Institute*
Lunch break		
13:45 – 14:00	Practical Information on the Break-Out Sessions	**Dr. Giovanni Nisato,**

PRECINCT

		Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways
14:00 – 15:30	**Break-out session #1**: *Cybersecurity Datasets: Challenges and Opportunities*	**Dr. Erkuden Rios,** *Director of Cybersecurity R&I projects at TECNALIA/Coordinator of AI4CYBER*
	Break-out session #2: *Critical Infrastructure Resilience through Public Transport*	**Mrs. Carmela Canonico,** *Safety & Security Manager at UITP*
	Break-out session #3: *PRECINCT's 2nd Training & Capacity Building Programme*	**Mrs. Marisa Escalante,** *Project Manager at TECNALIA*
Coffee break		
15:45 – 17:15	**Break-out session #4**: *Standardization in PRECINCT & STRATEGY and future policy recommendations*	**Mrs. Loredana Mancini,** *PRECINCT Impact Manager* **Dr. Georgios Sakkas,** *Research Associate at KEMEA*
	Break-out session #5: *Validation of security tools for CI protection*	**Mr. Tim Stelkens-Kobsch,** *Aviation Security Researcher at DLR,* **Mrs. Eva Muñoz Navarro,** *Project Manager at Grupo Etra*
	Break-out session #6: *PRECINCT's 2nd Training & Capacity Building Programme*	**Mrs. Marisa Escalante,** *Project Manager at TECNALIA*
17:15 – 17:30	Conclusions – End of Day 1	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*

Day 2 – May 17th

AGENDA

Time	Topic	Partner Responsible
8:30 – 9:00	Welcome and Registration	**PRECINCT Consortium**
9:00 – 9:15	Opening of Day 2	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*
9:15 – 9:30	Keynote speech	**Mr. Giannis Skiadaresis,** *Area Coordinator for Strengthened Security Research and Innovation (SSRI), DG HOME*
9:30 – 10:30	Panel Discussion on Innovation Uptake for Critical Infrastructure Protection	Chair: **Mr. Mark Miller**, *CEO of Conceptivity & Vice-Chair of EOS* Speakers: • **Mr. Giannis Skiadaresis,** *Area Coordinator for Strengthened Security*

		Research and Innovation (SSRI), DG HOME • **Dr. Takis Katsoulakos** *Managing Director for Inlecom Commercial Pathways* (TBC) • **Mr. Isto Mattila** *R&D Director at Laurea University of Applied Sciences & CEO of Dicitur Ltd* • **Dr. Giovanni Nisato** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*
10:30 – 10:45	Audience Q&A	**Mr. Mark Miller**, *CEO of Conceptivity & Vice-Chair of EOS*
Coffee Break		
10:45 – 11:45	The Resilience of Critical Entities: a New EC Directive	Chair: **Dr. Georgios Sakkas,** *Research Associate at KEMEA* • **Dr. Erkuden Rios,** *Director of Cybersecurity R&I projects at TECNALIA; Coordinator of AI4CYBER* • **Dr. Aikaterini Poustourli,** *Scientific Fellow of STRATEGY; Satways Ltd.)* • **Mr. Paolo Venturoni,** *CEO of the European Organisation for Security*
11:45 – 12:30	Resilience in Cybersecurity	**Dr. Sandra König,** *Scientist/Researcher in Safety and Security at AIT*
12:30 – 13:00	After PRECINCT, DYNABIC	**Dr. Erkuden Rios,** *Director of Cybersecurity R&I projects at TECNALIA*
13:00 – 13:10	Closing of the Conference	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons*

Break-out Session Descriptions:

BOS #1: "Cybersecurity Datasets: Challenges and Opportunities"

The session, developed by AI4CYBER is dedicated to discuss on the difficulties and opportunities of using and sharing cybersecurity related datasets for cybersecurity research and cybersecurity solution development. When using models and algorithms to develop AI-based cybersecurity solutions, the learning requires big amounts of well-structed and sanitized data which are sometimes difficult to get.

Some literature works include open datasets, but they are difficult to reuse as a basis of further research. Creating the datasets synthetically is often hard because it is not easy to replicate the nature of the attacks and getting realistic results is challenging.

In the workshop we will discuss on available open datasets, sources of datasets, reusable datasets, means and principles for sharing datasets, etc.

Suggested attendees:

Cybersecurity researchers dealing with AI used in threat detection, threat simulation, code testing, incident response, etc.

BO #2: Critical Infrastructure Resilience through Public Transport

This session will address the cooperation between different stakeholders operating critical infrastructure and public transport, with a special focus on how PT can improve resilience of the CI in case of disruption.

The discussion will start with a presentation that will highlight the interconnections between critical infrastructures and different modes of transport, and how a smooth cooperation can ease daily logistics and improve resilience in case of any obstacle. Then, the activities of the PRECINCT Living Labs 3 and 4 will be presented, with a focus on resilience management of interconnected transport critical infrastructure and the interdependencies/cascading effects of the full range regional transport.

After the presentations, the panel of experts will address the topics emerged during the workshop, touching upon cooperation, cybersecurity, IT tools and the added value of the PRECINCT Ecosystem Platform.

Suggested attendees:

Public Transport Operators, Physical and cyber security operators, etc.

BOS #3 & BOS #6: "PRECINCT's 2nd Training & Capacity Building Programme"

These two sessions are dedicated to deliver the second session of the PRECINCT Training and Capacity building programme. The main objectives of this training are: i) to present the

PRECINCT's concepts, innovation and tooling of the project to a wide audience and ii) to get feedback from the stakeholders that attend the meeting. This second session of the PRECINCT Training will be focused on presenting two relevant flows in PRECINCT. The first one has the objective of explaining how PRECINCT supports the detection of attacks and how processes this information to support in the decision of potential recovery actions or mitigation actions (Root cause Analysis, Complex event processing & Situation awareness UI), the second one is designed to show the different tools that support CI in the understanding of how a potential cyber-physical threat can be derivate in different cascading effects (Digital Twins & Resilience and supervisory control). Finally, some tools developed in PRECINCT to support these two flows will be also presented (Knowledge Graph, PRECINCT Blueprints Directory and Big Data Infrastructure Services).

Suggested attendees:

CI stakeholder, CI operators, Cybersecurity engineers and so on.

BOS #4: "Standardisation in PRECINCT & STRATEGY and Future Policy Recommendations"

"Standardisation in Precinct and Strategy, and future policy recommendations" The session, developed by EOS and Inlecom is dedicated to discuss how standards and policy can support Critical Infrastructure protection and collaboration. Status of the art and literature in this area will be presented. Users will evidence their needs, in particular those emerged during the Living Lab and in their experiences. The different Stakeholder and the community of experts, that already joined the Precinct working group on standard; will discuss the status of the art, the opportunities of improvement and the pitfalls. Specific elements will be presented from Strategy project with an overview of the standardization activity for Cis, where they will outline the methodological approach for identifying high impact standardization concepts (considering the perspective of end-users) with regards to Cis and also showcase indicative examples for enhancing interoperability

Suggested attendees:

Standardisation experts (in the CIP domain), Physical and cyber security operators, researchers dealing with critical infrastructure protection, etc.

BOS #5: "Validation of security tools for CI protection"

The session, developed by PRAETORIAN, is dedicated to explain and discuss a validation framework that can be used for the validation of security tools. The validation framework ensures that the operational requirements of end-users are met. During the validation experiments, both objective and subjective data from the systems and operators are collected and subsequently assessed in data analysis. Due to the variety of scenarios and domains addressed in the context of CI protection the preparations, conduction and analysis are very complex. Moreover, recommendations on improvements to better meet the expectations for the technical performance of the tools before deployment and

demonstration must be a key outcome of the validation. That is why such validations are very relevant and require strong involvement of the end-users.

In the workshop we will present the validation framework proposed in the H2020 PRAETORIAN project, how we prepared it, how we conducted it, how we evaluate it and the main results/lessons learnt. Q&A and hands-on exercises will be also included.

Suggested attendees:

Physical and cyber security operators, researchers dealing with physical/cyber security tools, etc.

Practicalities

Dear all,

We are excited to welcome you to the PRECINCT Conference taking place in Brussels, Belgium, on May 16th & 17th, 2023.
As part of the welcome pack, we are including some useful information.

Conference

The Conference will start with a welcome and a general introduction at 9:30 CET.
Registrations on place start at 9:00 CET.
For those who will join on-line, the zoom links can be found below, as well as in an email sent to registered participants.

Day 1's conclusion will be at 17:30 CET.

Day 2's will take place from 9:00 – 13:00 CET

Venue

"*Maison des associations internationales*" will host the Conference. It is a unique meeting and networking place for international organisations in Brussels. PRECINCT's Conference will primarily take place in the "Brussels" Room, a fully equipped space with a capacity of 200 participants and with a state-of-the-art live streaming and videoconference equipment.

The venue is located in Rue Washington 40, Ixelles, Brussels.

Covid-19

There are no longer any COVID-19 travel restrictions in place for EU citizens travelling to Belgium.
The use of masks is no longer mandatory on public transportation (Tram, bus, metro etc); however it remains strongly recommended.
Masks are not required to enter the workshop; however, they are welcome in order to ensure the health and safety of yourself and others.

For more information, please visit the official page Home | Coronavirus COVID-19 (info-coronavirus.be)

PRECINCT

Arrival in Brussels

- For those arriving from the **Brussels International Airport (Zaventem)**:

- By Taxi or Uber/Bolt (approximately 40-60 euro, 30 mins)
- By bus number 12 (Airport Line) from the Airport to Schuman. From Schuman bus number 60 (direction Uccle Calevoet) and get off at the bus stop Washington (1 hour, 12 euro)
- By train from the Airport to Gare Centrale.

From Gare Centrale you have few options:
- Bus 38 (direction Héros) and get off at the bus stop Vleurgat (25 mins, 2.10 / 2.60 euro)
- Tram 93 (direction Legrande) and get off at the tram stop Vleurgat (25 mins, 2.10/2.60 euro)

- For those arriving from **Charleroi Airport**:

- By Taxi/Uber/Bolt (80 – 100 euro, 1 hour)
- By Flibco to Gare du Midi (1 hour, 14 Euro)

- For Those arriving from **Gare du Midi (Train Station):**

- Bus 136 (direction Groot-Bijgaarden – Alsemberg) and get off at the bus stop Lepoutrelaan (20 mins, 2.10/2.60 euro)
- Tram 81 (direction Montgomery) and get off at the tram stop Trinité (20 mins, 2.10/2.60 euro)

Please note that for Trains you need to buy the proper ticket at the vendor machines in the station.
For bus and trams, it Is possible to pay directly with your credit card on the voiture.

For more information, please visit the official Brussels Transports website STIB-MIVB - Brussels Intercommunal Transport Company

Useful Contacts

Vincent Perez de Leon – Huet (EOS) +32 499719421
Giacomo Bianchi (EOS) +32 499 71 94 21

PRECINCT

Information Sheet

PARTICIPANT INFORMATION SHEET

Introduction

You have been invited to take part in a workshop/Conference. Before making a decision on whether you want to participate or not, please read this document carefully. Please ask all the questions you may have, including around risks and benefits, so you can be sure to understand all the proceedings of the workshop.

Description of the project

By signing the attached informed consent form, I understand that I am consenting to participate in the PRECINCT project funded by the European Union (Grant Agreement number 101021668) and co-ordinated by Inlecom Commercial Pathways. I am aware that the purpose of the activities in which I am participating is to establish an Ecosystem Platform for connecting stakeholders of interdependent CIs and Emergency Services to collaboratively and efficiently manage security and resilience by sharing data, Critical Infrastructure protection models and new resilience services.

The partners of the consortium are: Inlecom Commercial Pathways Company, University College Dublin, National University of Ireland, Dublin, AIT Austrian Institute Of Technology GMBH – AIT, Research Driven Solutions Limited - Research Driven Solutions Limited, Barcelona Supercomputing Center - CENTRO NACIONAL DE SUPERCOMPUTACION – BSC, AKKA HIGH TECH, MONTIMAGE EURL – MI, NUROGAMES GMBH, CONCEPTIVITY SARL – CONCEPTIVITY, European Organisation for Security – EOS, Fundacion Tecnalia Research & Innovation – Tecnalia, Engineering - INGEGNERIA INFORMATICA SPA – ENG, Confederation Of Organisations In Road Transport Enforcement AISBL – CORTE, KONNECTA Systems Limited, VLTN GCV – VLTN, WATER-LINK OV - WATER-LINK, POLITIEZONE VAN ANTWERPEN - Antwerp Police Department, VIAS INSTITUTE - Institut Belge Pourla Securite Routiere ASBL, KENTRO MELETON ASFALEIAS - Center For Security Studies Centre D'etudes De Securite, INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA - Institute For Corporative Security Studies Ljubljana, SLOVENSKE ZELEZNICE DOO - SZ DOO, PROMETNI INSTITUT LJUBLJANA DOO – PI, JAVNO PODJETJE LJUBLJANSKI POTNISKI PROMET D.O.O. – LPP, TELEKOM SLOVENIJE DD - TELEKOM SLOVENIJE, d. d., ELEKTRO LJUBLJANA PODJETJE ZADISTRIBUCIJO ELEKTRICNE ENERGIJE D.D. - Elektro Ljubljana, d.d., Municipality Of Ljubljana, AE SYN. - LEITOYRG. KAI EKMETALLEYS. ELEYTHERIS LEO.

PRECINCT

ELEYSINAS - STAYROY - AERODROMIOY SPATON KAI DYTIKIS PERIFER. LEO. YMITOY ATTIKES DIADROMES - ATTIKES DIADROMES, Promotion of Operational Links With Integrated Services, Association Internationale – POLIS, Union Internationale Des Transports Publics – UITP, FONDAZIONE ISTITUTO SUI TRASPORTI E LA LOGISTICA – ITL, ATHENS International Airport S.A. - DIETHNIS AEROLIMENAS ATHINON AE, ATTIKO METRO AE - ATTIKO METRO AE, Luxembourg Institute Of Science And Technology – LIST, FSTECHNOLOGY SPA, INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM – IMEC, DUN Laoghaire Rathdown County Council – DLRCOCO, LEPIDA SCPA - LEPIDA SPA, Aeroporto Guglielmo Marconi Di Bologna SPA, KATHOLIEKE UNIVERSITEIT LEUVEN - KU Leuven, Secretaria De Inteligencia Estrategica De Estado - Presidencia De La Republica Oriental Del Uruguay - SIEE

The PRECINCT project duration is from 01/10/2021 to 30/09/2023.

Information about your involvement

I understand that my responses to any workshop/Conference/webinar discussion may be recorded and that physical copies of such recordings will be safely stored under lock and key by the PRECINCT partner leading the concerned activities. In this case, the Data Controller for this activity will be Giacomo Bianchi (giacomo.bianchi@eos-eu.com). I understand that all the original data provided will be deleted five years after the project funding comes to an end.

I understand that, when the information I provide is used for the writing of the deliverable, the consortium will remove my name and all identifying features of that information so that my identity and experiences remain confidential (unless attribution is required and I have consented to it). I understand that I can request a copy of the data I have provided.

Personal information received will be stored in separate files in a secure manner (including password protection where required). Under the General Data Protection Regulation 2016/679, the consortium has an obligation to inform me of the purpose of the collection, use, storage and retention of the information I have provided. I understand that the project will only collect information that is relevant to its activities. Personal information will be stored on internal servers, and accessible to only the partners involved in PRECINCT. The project will not transfer my personal information to third parties (i.e., people outside the project). The partners will password-protect any and all records with personal data. All

computers will also have password protection to prevent access by unauthorised users. Only members of the research staff will have access to the passwords. The Ethics and Data Protection Officer (EDPO) shall act as data controller for the project. In this case the EDPO is Jenny Rainbird (jenny.rainbird@inlecomsystems.com).

I understand that my responses may result in incidental and secondary findings, i.e., some information that was not the focus or primary purpose of the question(s). In such cases, I understand that I may opt out of my consent for PRECINCT's use of the incidental findings. Otherwise, I understand that PRECINCT will manage the incidental findings in the same way as the principal findings, i.e., that the information will be deleted within five years after EU project funding comes to an end and that any use of such information will be anonymised. The consortium will report incidental findings to the project's Ethics Board and, if necessary or if the Ethics Review Panel so chooses, it can evaluate incidental findings.

I understand that I have the following rights.

My Rights

GDPR

I understand that I can withdraw my consent to the PRECINCT project for its processing of my personal data at any time.

Article 7

I understand that I can request access to my personal data processed by the PRECINCT project, and information about the processing.

Article 15

I have the right to receive the personal data that I have provided to the PRECINCT project in a structured, commonly used, machine readable format, where the project has processing this data in an automated way.

Article 20

I understand that if my personal data held by PRECINCT is inaccurate, I can request that it be rectified and that this amendment should be processed without undue delay. Similarly, if I feel my personal data is incomplete, I have the right to its completion and can provide a supplementary statement.

Article 16

I understand that I have the right to be 'forgotten' by requesting that my personal data be erased.

Article 17

I understand that I can request that the processing of my personal data be restricted in certain circumstances, such as where I am contesting its: accuracy; lawfulness; or that the processing of my personal data is no longer necessary for the purposes I gave my consent.

Article 18

I am aware of my right to lodge a complaint with a supervisory authority.

Article 57

I have been given the contact details of the research team and I have been informed that I am free to contact Jenny Rainbird, PRECINCT Project Coordinator, with any queries relating to my data or the project itself. The Coordinator's email address is PRECINCT_PM@inlecomsystems.com

PRECINCT

Learn about our Partner Projects in the Conference!

AI4CYBER

The AI4CYBER project (https://ai4cyber.eu) is an EU-funded research project of the Horizon Europe Programme, Grant Agreement No. 101070450, and it aims to establish an Ecosystem Framework of next generation AI-based services for supporting critical system developers and operators to efficiently manage system robustness, resilience, and appropriate response in the face of advanced and AI-powered cyberattacks. The project will thus deliver a collection of innovative resilience and autonomous response services that leverage AI models and Big Data, aimed to be encapsulated in cybersecurity tools to ensure a continuum of system protection.

DYNABIC

The DYNABIC project (https://dynabic.eu/) is a EU funded-research project working in the areas of Critical Infrastructure Protection and dynamic response against cyber-physical threats, as well as in the creation of Digital Twins for business continuity analysis and situational awareness. The goal is to increase the resilience and business continuity capabilities of European critical services in the face of advanced cyber-physical threats. This objective will be pursued by delivering new socio-technical methods, models and tools to support resilience through holistic business continuity risk management and control in operation, and dynamic adaptation of responses at multiple planes of action: system, human and organization planes.

EU-CIP

EU-CIP (https://www.eucip.eu/) is an EU funded project aiming with the main goal of establishing a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs). In this direction, the partners have already established the European Cluster for Securing Critical infrastructures (ECSCI), which brings together 22 projects that collaborate in CI Resilience. EU-CIP will leverage the capacity, organization, community, and achievements of the ECSCI cluster towards establishing an EU-wide knowledge network with advanced analytical and innovation support capabilities.

EU-HYBNET

EU-HYBNET (https://euhybnet.eu/) is an EU funded project aiming at enriching the existing European networks countering hybrid threats and ensuring long term sustainability. This will be achieved by defining the common requirements of European practitioners' and other relevant actors in the field of hybrid threats. Ultimately, this can fill knowledge gaps, deal with performance needs, and enhance capabilities or research, innovation and training endeavours concerning hybrid threats. EU-HYBNET will monitor developments in research and innovation activities as applied to hybrid threats; so to indicate priorities for innovation

uptake and industrialization and to determine priorities for standardization for empowering the Pan-European network to effectively counter hybrid threats. EU-HYBNET will establish conditions for enhanced interactions with practitioners, industry, and academia for a meaningful dialogue and for increasing membership in the network.

PRAETORIAN

The PRAETORIAN project (https://praetorian-h2020.eu/) is a EU funded-research project working in the area of Critical Infrastructure Protection against combined cyber-physical threats. PRAETORIAN strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project will provide a multidimensional (economical, technological, policy, societal) yet installation-specific toolset. The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

STRATEGY

The STRATEGY EU funded project (https://strategy-project.eu/about/) aims to build and implement a pan-European pre-standardisation framework and to map, test and validate new and existing standards across eight thematic streams in crisis management: Search and rescue, Critical infrastructure protection, Response planning, Command and control, Early warning and Rapid damage assessment, Chemical, Biological, Radiological, Nuclear and high-yield Explosive threats (CBRN-E), Training, Terminology/Symbology. The ultimate project goal is to strengthen the resilience of the EU against all types of natural & man-made disasters (multi-hazard approach), by ensuring first responders' safety and empowering their operational capacity through standardisation that may support next generation solutions and procedures, ensuring an effective and efficient collaborative response to crises.

SUNRISE

SUNRISE (https://sunrise-europe.eu/) aims to ensure greater availability, reliability, and continuity of critical infrastructures including transport, energy, water, and healthcare to safeguard Europe's lifeline services in pandemics and other major threats. During its lifetime, SUNRISE will bring together 18 critical infrastructure (CI) operators and authorities from across Europe to enable active collaboration across borders, sectors and public and private stakeholders. It will also develop a suite of technologies and strategic solutions to be better prepared and equipped to adequately manage future risks created by pandemics.