# CyberSec-Buddy

- *Juan Arraiza*
- *jarraiza@vicomtech.org*
- *Vicomtech*
- Role: *Proposal coordinator (provisional)*

- Proposal activity: SU-DS03-2018 – subtopic (b)

*NOTE: could also be interested in subtopic (a), though not decided yet*

# «Cyber buddy» to help SMEs&MEs on cyber security and privacy

*A virtual «buddy» that will guide the user along the way. The guidance will be based on knowledge and best practices from the whole community in the areas of:*

- *Risk awareness: based on information sharing using existing formats and protocols such as STIX and TAXII*
- *Risk assessment: based on tools to conduct Cyber Security Maturity Models (CSMM) and GDPR compliance assessments*
- *Monitor risks: based on Indicators of Compromise (IoC) and MITRE ATT&CK adversarial technics and tactics*
- *Forecast risks: based on reports from various trusted sources and discover relationships and cascade effects between risks*
- *Training: based on chatbot, e-learning, and  cyber range exercises*
- *Recommendations: based on best practices from CSMM and GDPR assessment toolkits*

Juan Arraiza – jarraiza@vicomtech.org

# Project participants

- Proposed coordinator: *Open (Vicomtech could, but large/SME company preferable)*
- Partners / Other participants:
  - *A Cyber Security Centre (ES) – Public Entity -* CERT/CSIRT
  - *A Cyber Security company (ES) – SME – cyber security technology and service provider*
  - *Vicomtech (ES) – RTO – applied research on cyber security technologies; cyber security testbed (including access to cyber range)*
  - *A University (IE) – UNIV – E-learning materials over a Learning Management System*

- Looking for partners with the following expertise/ technology/ application field:
  - *A Cyber Insurance company*
  - *End-user SMEs&MEs*
  - *CERTs/CSIRTs*
  - *Cyber Security companies*

# COEFFECT: Cost-efficient cybersecurity toolkit for medium, small and micro enterprises

- *Georgios Gardikis, PhD*
- *ggar@space.gr*
- *SPACE Hellas SA*
- *Proposal coordinator*

- *Proposal activity: SU-DS-03-2019: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises*
  - *(b): Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection*

# Proposal idea/content

- *Project mission: deliver a low (or zero)-cost cybersecurity toolkit for SMEs & Mes*
- *Specific results:*
  - *COEFFECT Platform: open-source Big Data/Machine Learning platform for detecting and classifying anomalies (possible cybersecurity incidents and zero-day threats). Offered as on-prem (community edition) or as-a-Service*
  - *COEFFECT Hub: cloud platform for community-based exchange of ML algorithms & rules (detection/classification) for the COEFFECT platform*
  - *COEFFECT Risk-Assessment Tool: cloud-based service for SME risk assessment (also leveraging feeds from the Platform)*

# Project participants

- *Proposed coordinator: SPACE Hellas (GR - midcap), large ICT system integrator, expertise on data integration, cybersecurity and big data analytics*
  - *Coordinator of the EU SHIELD project on cybersecurity and big data*
- *Partners/Other participants:*
  - *3 SMEs, 2 Research Institutes (TBC)*
- *Looking for partners with the following expertise/technology/ application field:*
  - *Advanced ML techniques for cybersecurity, incl. Deep Learning*
  - *End-users / SMEs willing to host pilots in their premises*
- *Commitment to open-source (no proprietary solutions please!)*

DEMOKRITOS
NATIONAL CENTER FOR SCIENTIFIC RESEARCH

# <Information sharing & Game Theory in defending secuirty, privacy and personal data>

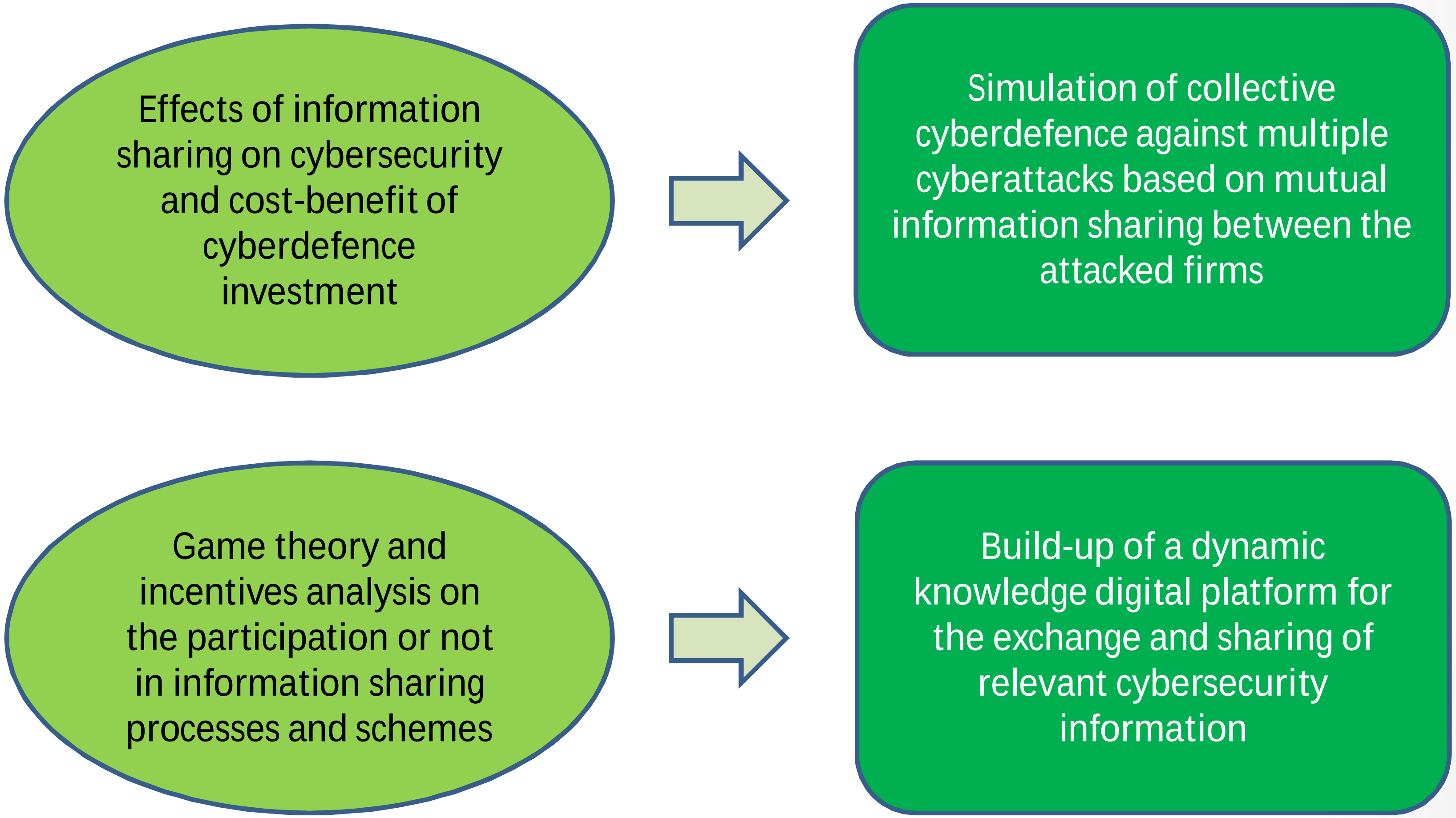
- *Stelios C. A. Thomopoulos*
- *scat@iit.demokritos.gr*
- *NCSR Demokritos*
- Role: *WP leader and S/T provider*

SU-DS03-2019-2020

*(b): Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection*

Dr. Stelios C.A. Thomopoulos
Head of Integrated Systems Laboratory
Email: scat@iit.demokritos.gr
Phone number: (+30) 210 650 3155
Mobile: (+30) 6944 98669

# Proposal idea/content



Effects of information sharing on cybersecurity and cost-benefit of cyberdefence investment

Simulation of collective cyberdefence against multiple cyberattacks based on mutual information sharing between the attacked firms

Game theory and incentives analysis on the participation or not in information sharing processes and schemes

Build-up of a dynamic knowledge digital platform for the exchange and sharing of relevant cybersecurity information

# Project participants

- Proposed Coordinator/WP Leader: *NCSRD*
- NCSRD's expertise on:
  - *Simulation Methods for modelling and validating cyberattackers' and cyberdefenders' behaviour.*
  - *Data Mining and Statistical Analysis Techniques for getting out related to cybercrime insights, from relevant datasets.*
  - *Theoretical and empirical economic analysis methods for econometric modelling of the factors affecting the economic conditions and behaviour of all the implicated, in the domains cybercrime.*
  - *Command and control/ Front-end development*
  - *Risk analysis*

- Looking for partners with the following expertise/ technology/ application field:
  - *SMEs and MEs*
  - *Informatics Technology*
  - *GDPR/Ethics Monitoring Experts*

# Security for enterprises

- *Tatiana Silva [tatiana.silva@treetk.com](mailto:tatiana.silva@treetk.com)*

- *Tree Technology - [www.treetk.com](http://www.treetk.com) (former Treelogic)*
  - *Spanish SME, experts on Big Data and Artificial Intelligence*
  - *Team experienced on 30+ EU projects* | *8 EU projects in SEC*

- Role: *WP Leader*

  *Experts in Deep Learning and AI supporting cybersecurity*

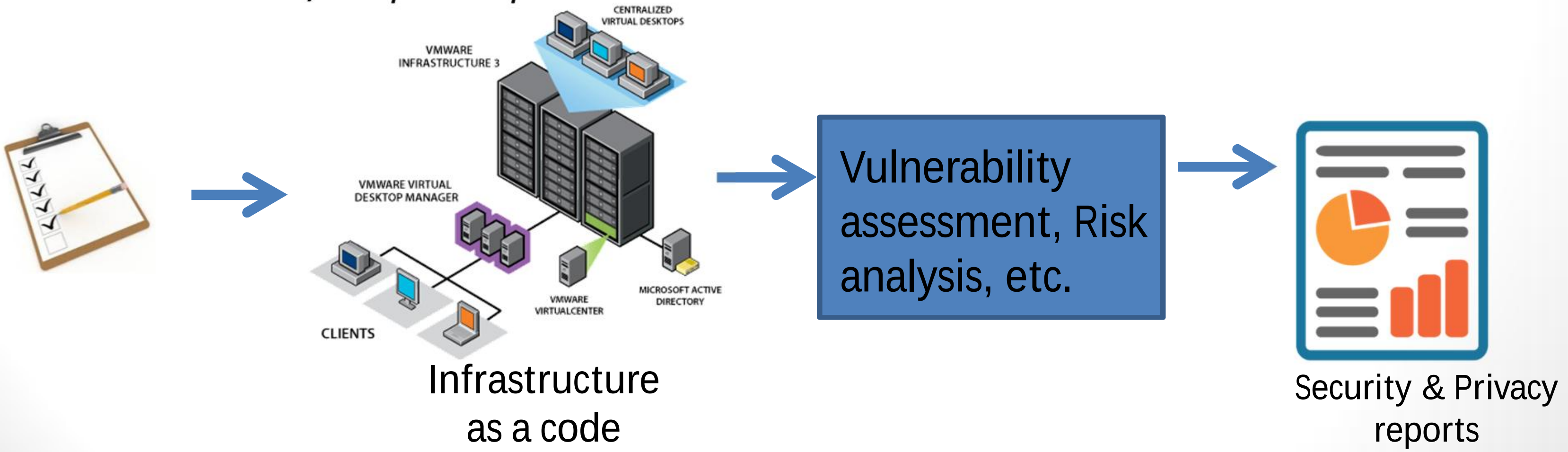
  *Background on ransomware detection: RAMSES project (<https://ramses2020.eu/>)*

- Proposal activity: *SU-DS03-2019, Sub-topic b) Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection*

# Proposal idea / content

*Security as a service solution for SMEs & MEs for increasing their level of cybersecurity awareness*

- *Defense system based on Big data & AI for increasing cybersecurity awareness*
  - *Simulation of different IT/OT SMEs/MEs infrastructures with code (Infrastructure as a code).*
  - *Detection of patterns using Deep Learning techniques (e.g. Phishing emails)*
  - *Data breaches and data integrity attacks (ransomware)*
  - *Integration with CERTs/CSIRTS for Threat Intelligence and Incident/Response processes*


CENTRALIZED VIRTUAL DESKTOPS
VMWARE INFRASTRUCTURE 3
VMWARE VIRTUAL DESKTOP MANAGER
CLIENTS
VMWARE VIRTUALCENTER
MICROSOFT ACTIVE DIRECTORY

Vulnerability assessment, Risk analysis, etc.

Infrastructure as a code

Security & Privacy reports

# Project participants

- Proposed Coordinator: TBD
- Partners:
  - Tree Technology – expert in Big Data and AI
- Looking for partners:
  - *Coordinator? (To Be Decided)*
  - *Cybersecurity companies*
  - *Cyber-range*
  - *SMEs/MEs as end-users*
  - *Ethical and legal experts*
  - *CERTs*/CSIRTs***
  - *Insurance companies*

**CERT, Computer Emergency Response Team*
***CSIRT, Computer Security Incident Response Team*

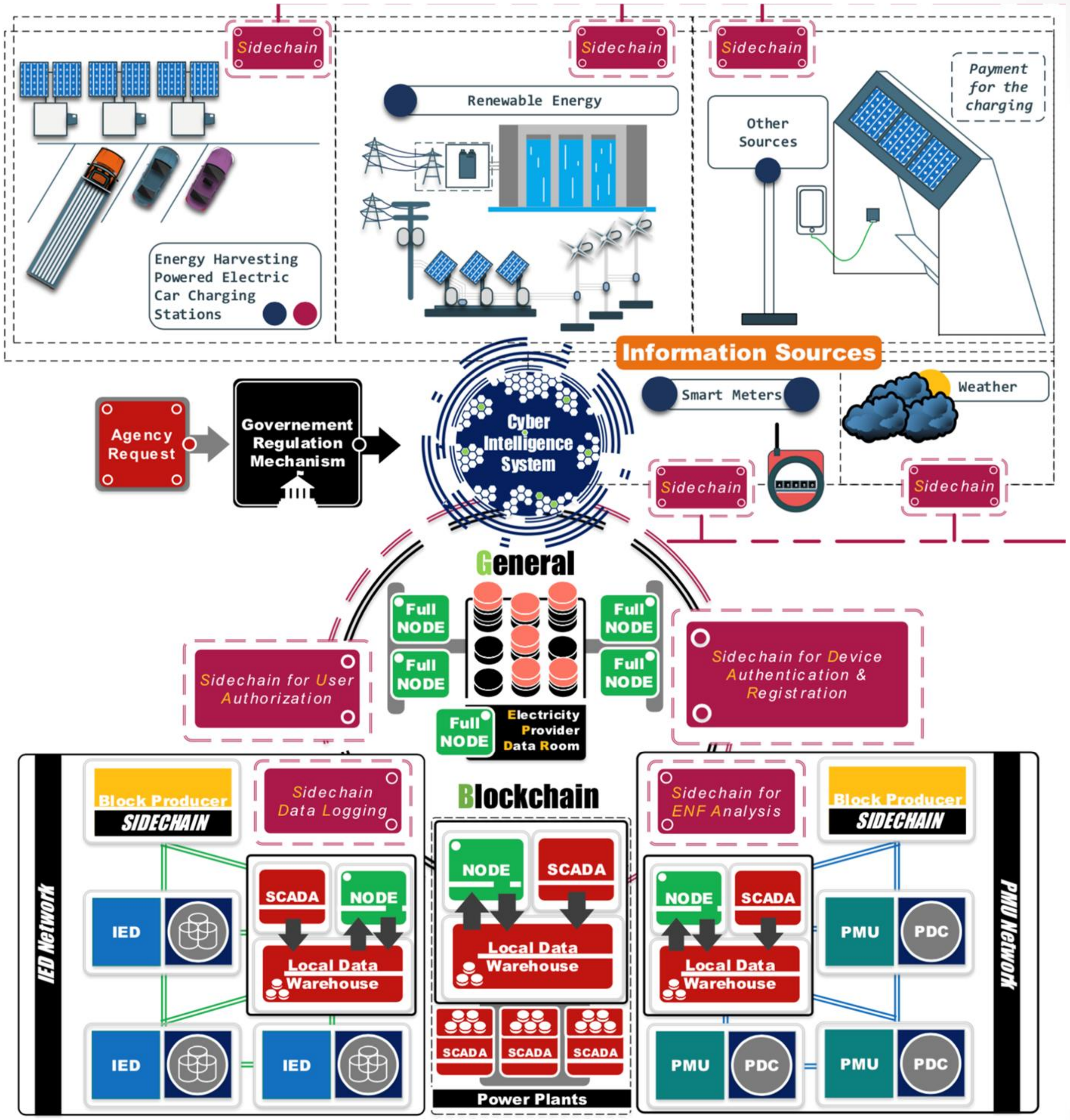
# SEwDLT

- *Igor Kotsiuba*
- *i.kotsiuba@gmail.com*
- *PIMEE NAS of Ukraine*
- Role: *WP leader, S/T provider*

- Digital security, privacy, data protection and accountability in critical sectors SU-DS05-2018-2019
- Technologies to enhance border and external security SU-BES02-2018-2019-2020

# Proposal idea/content

- In Bitfury R&D we possess in-depth knowledge of the blockchain infrastructure and underlying architecture. That knowledge and R&D capabilities are essential for developing new methods for security and safety of critical infrastructure, IIoT, energy.
- In PIMEE NAS of Ukraine we are NCP ”Secure Society” as well as 100+ Scientists R&D Institute for Security and Safety of Critical Infrastructure.
- We are focusing on both ad-hoc design of CI and the wonderful applications that blockchain(DLT) has in store. We are thinking about how we can encourage innovation while at the same time guaranteeing security of Critical Infrastructure, Energy Grids, eHealth and Border Security of Ukraine, thus EU member states.


Sidechain
Sidechain
Sidechain
Renewable Energy
Other Sources
Payment for the charging
Energy Harvesting Powered Electric Car Charging Stations
Information Sources
Smart Meters
Weather
Agency Request
Governement Regulation Mechanism
Cyber Intelligence System
Sidechain
Sidechain
General
Full NODE
Full NODE
Full NODE
Full NODE
Full NODE
Electricity Provider Data Room
Sidechain for User Authorization
Sidechain for Device Authentication & Registration
Block Producer SIDECHAIN
Sidechain Data Logging
Blockchain
Sidechain for ENF Analysis
Block Producer SIDECHAIN
IED Network
IED
IED
IED
SCADA
NODE
Local Data Warehouse
NODE
SCADA
Local Data Warehouse
SCADA
SCADA
SCADA
Power Plants
NODE
SCADA
Local Data Warehouse
PMU
PDC
PMU
PDC
PMU
PDC
PMU Network

# Project participants

- Proposed coordinator: *TBD*
- Partners / Other participants:
- Bitfury – Full stack Blockchain infrastructure provider – Netherlands
- PIMEE NAS of Ukraine  is leading research institute in the field of modeling and simulation in industry, particularly in energy sector.

- Looking for partners with the following expertise/ technology/ application field:
  - *Border Security*
  - *ICT cybersecurity, privacy, data protection experts*

# Data Security Solutions for SU-DS-05, subtopics a & b

- Tanel Ojalill
- tanel.ojalill@guardtime.com
- Guardtime:
  - Estonia, SME, 150+ FTE employees
  - One of the world largest blockchain technology companies
  - Dedicated and experienced R&D & H2020 teams with 5 running IA&RIA projects

- Role: WP leader or S/T provider; partner for proposal writing and consortium building

- Proposal activity: SU-DS05-2019, sub-topic a & b

# Guardtime’s possible contribution

Developing beyond state of the art cyber and data-centric security solutions, which are enabled by:

- KSI® Blockchain Technology and other Distributed Ledger Technologies,  allowing us to:
  - guarantee data integrity whilst preserving privacy (e.g. sensitive personal data, sign and tie consent, data processing logs, archives)
  - provide real-time threat detection, privacy and data protection warnings
  - ensure regulatory compliance, audit, accountabiliy and compliance (e.g. GDPR, eIDAS)
  - provide traceability and supply chain security solutions
  - ... implement a **horizontal technology with a wide application area**, different use-cases in various domains and industries

- Cyber Range Solutions and Exercises
  - Training organisations and testing infrastructure for enhanced cyber resilience
  - “*Proposals should also include ... the delivery of specific social aspects of digital security related to training, in particular practical, operational and hands-on training*”

Mr. Tanel Ojalill; tanel.ojalill@guardtime.com

# Access to project partners

- Wide network of potential partners in the healthcare and transportation industries:
  - End-users (e.g. hospitals)
  - Public authorities
  - S/T providers (e.g. cyber security solution providers, IT integrators, RTOs)

- Looking for partners with the following expertise/technology/ application field:
  - Project coordinators
  - Complementing technology providers and research partners e.g. for cryptography, DLTs, cyber security and privacy technologies

Mr. Tanel Ojalill; tanel.ojalill@guardtime.com

# Secure Transport Digital Twin

- *Juan Arraiza*
- *jarraiza@vicomtech.org*
- *Vicomtech*
- Role: *Proposal coordinator (provisional)*

- Proposal activity: SU-DS05-2019 – subtopics (a)

# Secure Transport Digital Twin

Develop a «Secure Transport Digital Twin», a simulation environment for a multimodal operator to identify new vulnerabilities, to test risks and to validate mitigated impact of deployed cybersecurity measures

- *<u>Access management</u>: Exchange of privacy and personal data, including all potential information sources: vehicles (V2X), mobile devices, booking applications, route management services and operators, infrastructure operation, etc*
- *<u>Assurance and protection</u>: Based on risk information sharing using existing formats and protocols such as STIX, TAXII and ATT&CK and its application to physical and logical infrastructures covering IT and OT dimensions*
- *<u>Standarization</u>: Contribution to working groups for the definition and validation of best practices and standards in the multi-modal transport domain*

# Project participants

- Proposed coordinator: *Open (Vicomtech could, but large/SME company preferable)*
- Partners / Other participants:
  - *A Cyber Security Centre (ES) – Public Entity -* CERT/CSIRT
  - *A Cyber Security company (ES) – SME – cyber security technology and service provider*
  - *Vicomtech (ES) – RTO – applied research on cyber security technologies; cyber security testbed (including access to cyber range)*
  - *A multimodal transport operator (ES) – large – business knowledge and validation of technologies*

- Looking for partners with the following expertise/ technology/ application field:
  - *A Cyber Insurance company*
  - *Modelling and Simulation software companies*
  - *CERTs/CSIRTs*
  - *Cyber Security companies*
  - *Standarization bodies and* inspection, verification, testing and certification companies

# SecMoveL

- *Christian Derler*
- *christian.derler@joanneum.at*
- *JOANNEUM RESEARCH, Cyber Security and Defence*
- Role:  *WP leader, S/T provider*

- Proposal activity: SU-DS05-2018-2019 Digital security, privacy, data protection and accountability in critical sectors
- *Sub-topic (a) [2019]: Digital security, privacy and personal data protection in multimodal transport*

# SecMoveL – Proposal idea

- *Use of AI in multimodal transport is envolving*
- *Attack surface would increase enormously*
- *Malicious use of AI opens up new opportunities for hackers*

- *Goal: Protect AI based systems against cyber attacks in multimodal transport*
  - *Formal methods for test & verification*
  - *AI based cyber incident detection*
  - *Security tools for designing AI based systems*

- *Reference:* »The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation«, see https://arxiv.org/abs/1802.07228

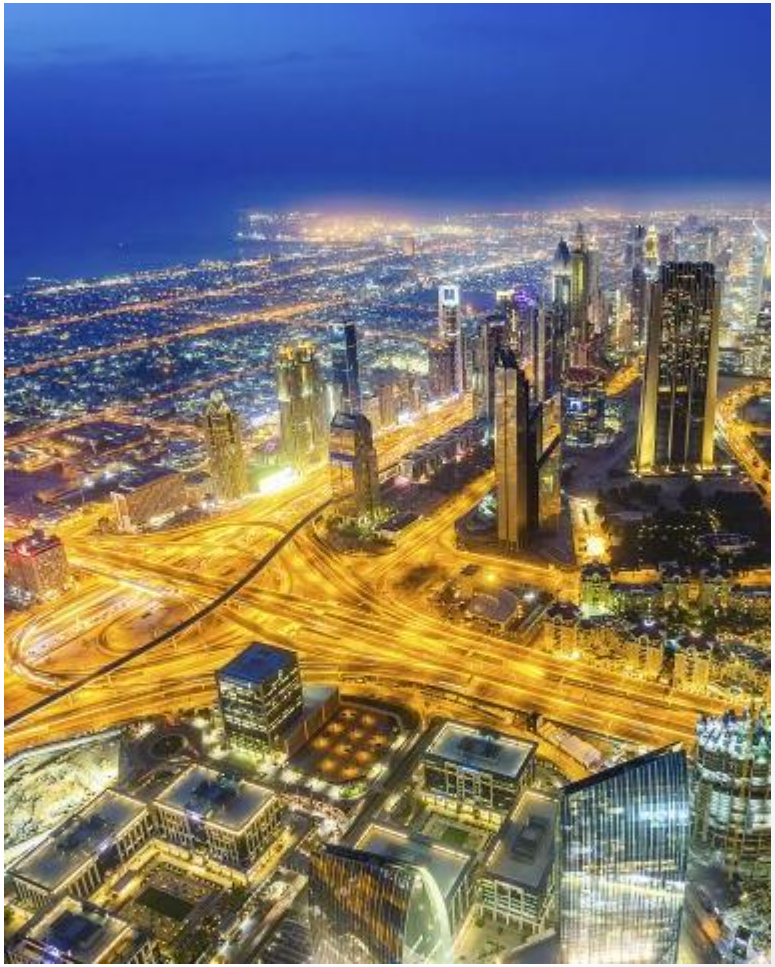


Image: iStock

# Project participants

- Proposed coordinator: *tbd*
- Partners / Other participants:
    - Automotive test & measurement technologies / INDUSTRY / AT
    - Security by design technology provider / INDUSTRY / DE
    - Formal verification / UNIVERSITY / IT
- Looking for partners with the following expertise/ technology/ application field:
    - Transport infrastructure operators
    - Scientific partners: Security by Design, Security at Runtime
    - <….>

# SU-DS-05-2019 Digital security, privacy, data protection and accountability in critical sectors

- *Prof. William Hynes*
- *William.hynes@futureanalytics.ie*
- *Future Analytics Consulting  Ltd., Dublin, Ireland.*

- Role: *Work Package Lead*

- Proposal activity: *SU-DS-05-2019: Digital security, privacy, data protection and accountability in critical sectors.*
  - *Sub Topic – (a) [2019]: Digital security, privacy and personal data protection in multimodal transport.*

# Digital security, privacy and personal data protection in multimodal transport

- *Secure access management for citizens to all types of vehicles.*
- *Seamless privacy aware solution to access across mass, shared and individual mobility, leading to added value to citizens while safeguarding data protection and privacy.*
- *Novel tailored solutions to reduce vulnerability.*
- *Assurance and protection against specific cyber-attacks.*
- *Standardization to allow the quick adoption.*

*FAC can deploy expertise gained from similar previous projects to help develop methods, tools, and evaluation criteria for the improvement.*

- *Reserach and analysis of extising practices, approached and tools.*
- *Wide stakeholder consultation regarding the effecitveness of existing research, methods, and related technologies.*
- *Brainstorming and analysis of the potential for combining best practice methods and approach.*
- *Development of pilot methods to measure the impact of new proposals and potential gaps – informed by stakeholder consultation and analysis.*

# Project participants

- Proposed coordinator: *NA*
- Partners / Other participants:
  Future Analytics Consulting – Work Package Lead
- Looking for partners with the following expertise/ technology/ application field:
  - EU wide academic researchers
  - Cyber security Experts
  - Transport owners/operators
  - Transport security specialists
  - Relevant departments from local and regional authorities
  - Representatives from key citizen groups

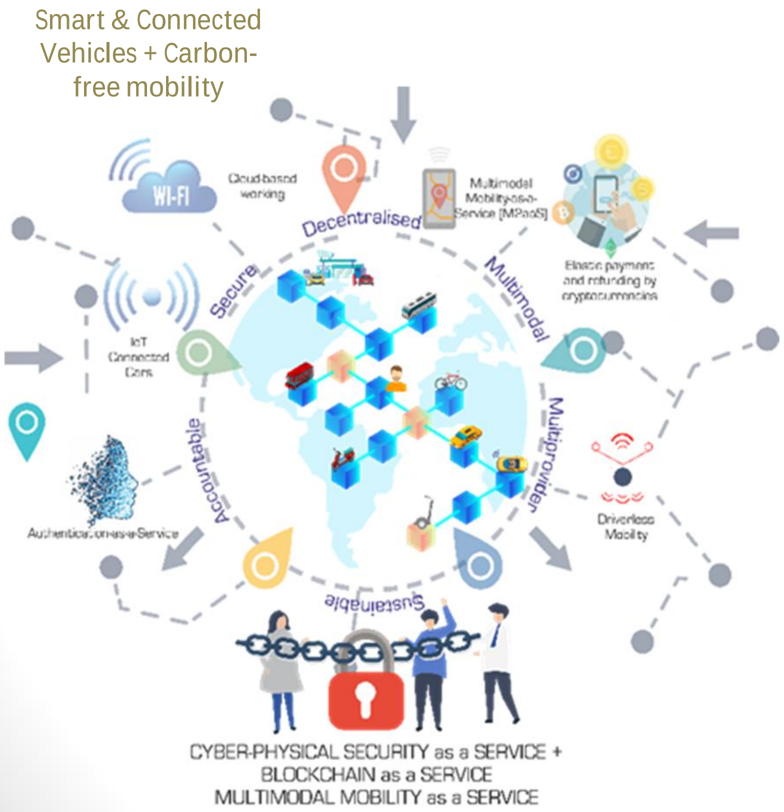
*Prof. William Hynes william.hynes@futureanalytics.ie*

# Cyber-physical Platform for Secure Internet of Mobility and Transportation ChainMove

- *Alper Kanak, PHD*
- *alper.kanak@ergtech.ch*
- *ERARGE & ERGTECH (ERGUNLER R&D Center)*
- Role: *S/T Provider and Concept Builder, Technical Coordinator*

- Proposal activity: *SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors (a) [2019]: Digital security, privacy and personal data protection in multimodal transport*

# ChainMove in brief


Smart & Connected Vehicles + Carbon-free mobility
WI-FI
Cloud-based working
Multimodal Mobility-as-a-Service (M2aaS)
Elastic payment and refunding by cryptocurrencies
Decentralised
Secure
Multimodal
IoT Connected Cars
Multiprovider
Accountable
Authentication-as-a-Service
Driverless Mobility
Sustainable
CYBER-PHYSICAL SECURITY as a SERVICE +
BLOCKCHAIN as a SERVICE
MULTIMODAL MOBILITY as a SERVICE

- From Motoring to Mobility
- Integrated Multimodal Mobility as a Service (M2aaS)
- Targeting urban land-transportation
- Security and Privacy Preservation is indispensible
- Data analytics to minimize risks and costs
- Decentralized data integrity and accountability
- Field trials in at least 3 EU cities

# Project participants

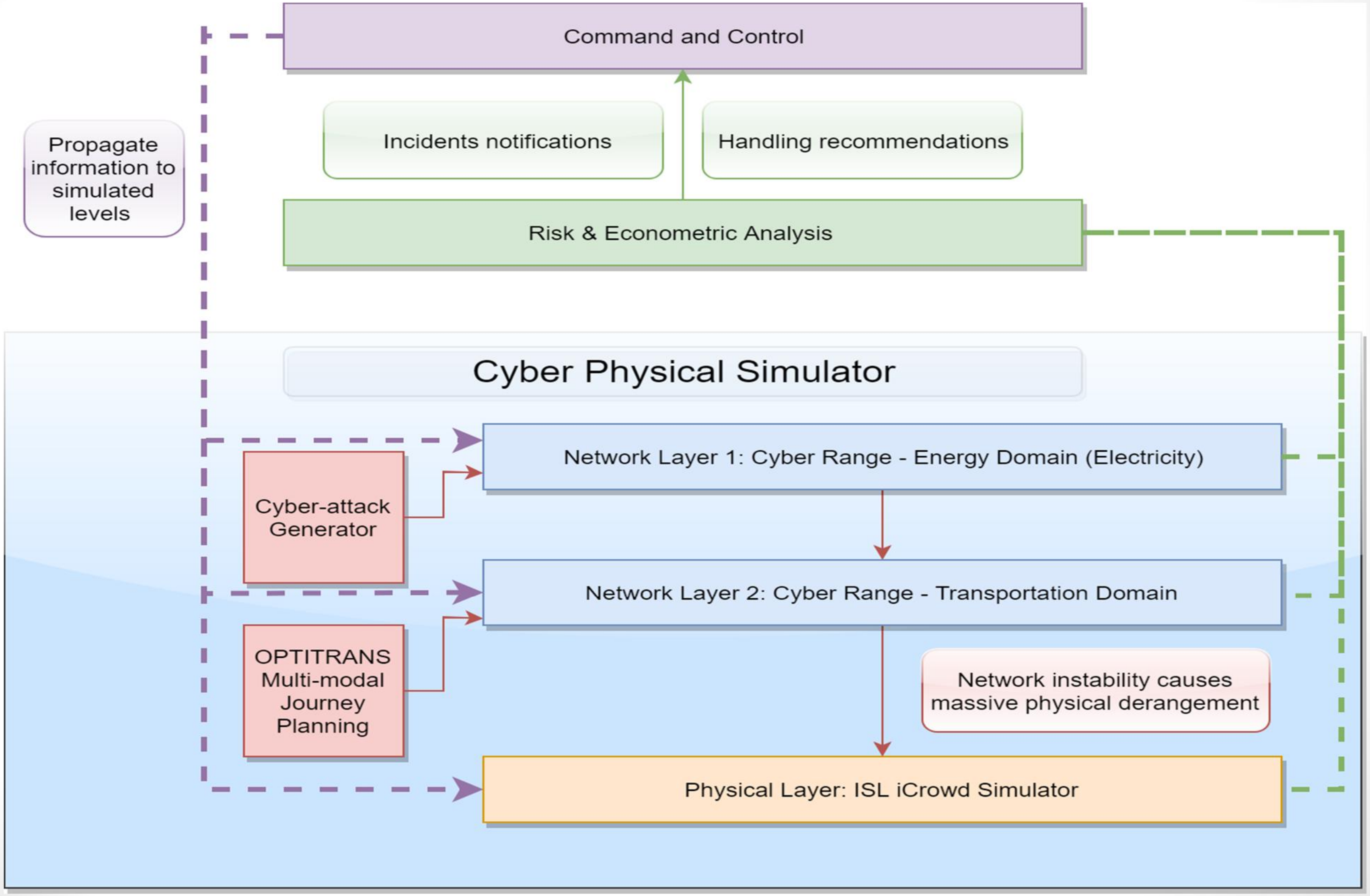
- Proposed coordinator:
  - *Administrative Coordinator: being sought*
  - *Technical Coordinator: ERARGE (IoT, CPS, chaotic analysis)*
- Partners / Other participants showing interest:
  - *A German Research Org.→ CPS, vulnerability analysis*
  - *A French Research Org.→ Cyber security, blockchain*
  - *An Austrian Res. Org.→ Blockchain analytics and threat intelligence*
  - *A big smart car manufacturer*
  - *A big manufacturer of connected public transportation vehicles*
  - *An Italian Insurance Company*
  - *A leading Spanish company for integration of transportation systems*
  - *3 municipalities or transportation autorities (İstanbul Metropolitan Municipality approved, etc)*
  - *A Romanian Company → SW integrator, mobile app developer, cloud provider*
  - *University of Tokyo (contributor) → Chaotic analysis and Chaotic Chips*
- Looking for partners with the following expertise/ technology/ application field:
  - *SME or big company having experience in blockchain enabled MaaS*
  - *Legal and ethics experts*
  - *Experts in standards*
  - *Socioeconomic and environmental analysis*
  - *End user cities with high impact*
  - *CERT or CSIRT*

# <An integrated approach to *Digital security, privacy and personal data protection in multimodal transport with the use of cyber-physical simulator*>

- *Stelios C. A. Thomopoulos*
- *scat@iit.demokritos.gr*
- *NCSR Demokritos*
- Role: *WP leader and S/T provider*
- Proposal activity: Digital security, privacy, data protection and accountability in critical sectors SU-DS05-2018-2019, *(a) [2019]: Digital security, privacy and personal data protection in multimodal transport*

Dr. Stelios C.A. Thomopoulos
Head of Integrated Systems Laboratory
Email: scat@iit.demokritos.gr
Phone number: (+30) 210 650 3155
Mobile: (+30) 6944 98669

# Proposal idea/content


Command and Control
Incidents notifications
Handling recommendations
Propagate information to simulated levels
Risk & Econometric Analysis
Cyber Physical Simulator
Network Layer 1: Cyber Range - Energy Domain (Electricity)
Cyber-attack Generator
Network Layer 2: Cyber Range - Transportation Domain
OPTITRANS Multi-modal Journey Planning
Network instability causes massive physical derangement
Physical Layer: ISL iCrowd Simulator

# Project participants

- Proposed Coordinator/WP Leader: *NCSRD*
- NCSRD's expertise on:
  - *Simulation Methods for modelling and validating cyberattackers' and cyberdefenders' behaviour.*
  - *Data Mining and Statistical Analysis Techniques for getting out related to cybercrime insights, from relevant datasets.*
  - *Theoretical and empirical economic analysis methods for econometric modelling of the factors affecting the economic conditions and behaviour of all the implicated, in the domains cybercrime.*
  - *Command and control/ Front-end development*
  - *Risk analysis*

- Looking for partners with the following expertise/ technology/ application field:
  - *End Users in the fields of transportation and energy (electricity utilities)*
  - *Cyber Ranges focusing on transportation and electricity domains*
  - *GDPR/Ethics Monitoring Experts*

# Secure and Trustworthy Healthcare Systems

- *Juan Arraiza*
- *jarraiza@vicomtech.org*
- *Vicomtech*
- Role: *Proposal coordinator (provisional)*

- Proposal activity: SU-DS05-2019 – subtopic (b)

# Healthcare Ecosystems Cyber Range

Develop a training oriented environment «Secure Healthcare Ecosystem Cyber Range» that can be used to test new vulnerabilities, measure risks and validate potential of cybersecurity controls in all actors of the healthcare sector avoiding compromise of real private data

- *Use the Cyber Range environment to:*
    - *create and maintain comprehensive vulnerability dataset*
    - *Create and maintain healthcare specific taxonomies and relationships*
    - *Domain adaptated risk control frameworks and tools (red team and blue team, focused in the healthcare ecosystem)*
    - *Develop and evaluate collaborative privacy-aware solutions in a sandbox environment*
    - *Exercise and test incident handling best/good practices*

# Project participants

- Proposed coordinator: *Open (Vicomtech could, but large/SME company preferable)*
- Partners / Other participants:
  - *A Cyber Security Centre (ES) – Public Entity* - CERT/CSIRT
  - *A Cyber Security company (ES) – SME – cyber security technology and service provider*
  - *Vicomtech (ES) – RTO – applied research on cyber security technologies; cyber security testbed (including access to cyber range)*
  - *A healthcare provider (ES) – operator of a healthcare service*

- Looking for partners with the following expertise/ technology/ application field:
  - *A Cyber Insurance company*
  - *CERTs/CSIRTs*
  - *Cyber Security companies*
  - *Healthcare operator*
  - *Pharmaceutical company*

# DOCTOR - Dynamic taxOnomy for seCurity assessmenT Of healthcaRe systems

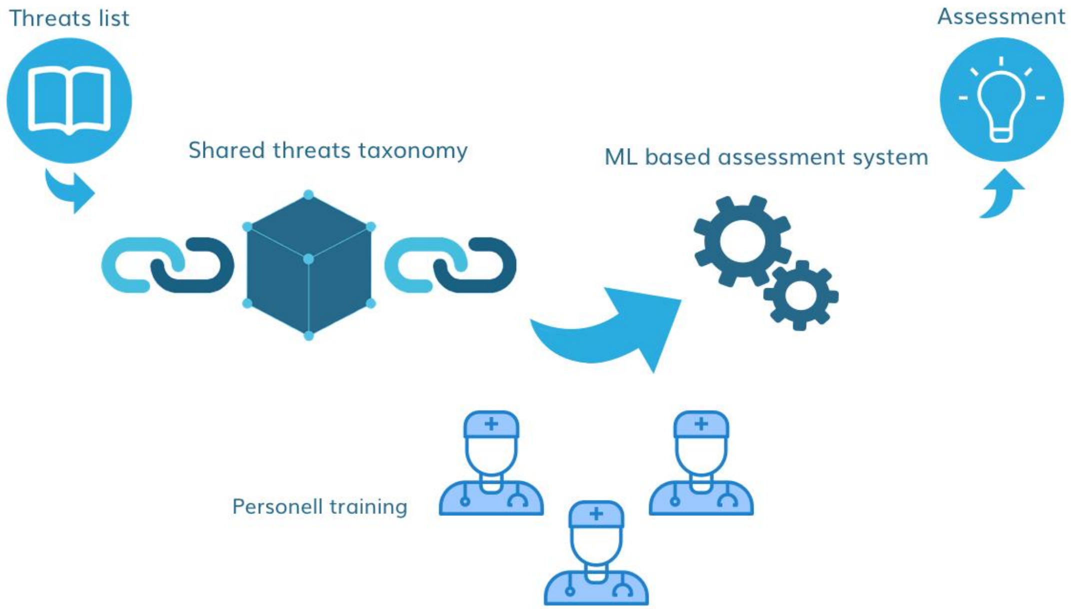
- *Graziano GIORGI*
- *Zanasi & Partners (Italian SME specialised in security, defence and intelligence)*

- Role: *Proposal coordinator*
- Proposal activity:
  - *SU-DS05-2019*
  - *Sub-topic B*

Zanasi & Partners

# DOCTOR overview

- *The DOCTOR project aims at:*
  - *Building a shared dynamic taxonomy of healthcare cybersecurity threats using blockchain*
  - *Developing a machine learning based system to identify system vulnerabilities and ongoing attacks*



# Project participants

- Proposed coordinator: *Zanasi & Partners*

- Partners / Other participants:
  - *IT and system integration*
    - *GFT (I)*
    - *IBM (IL)*
  - *Healthcare practitioners*
    - *Gemelli Polyclinic (I)*
    - *Debrè Hospital (tbc) (F)*
    - *Berlin Hospital (tbc) (D)*

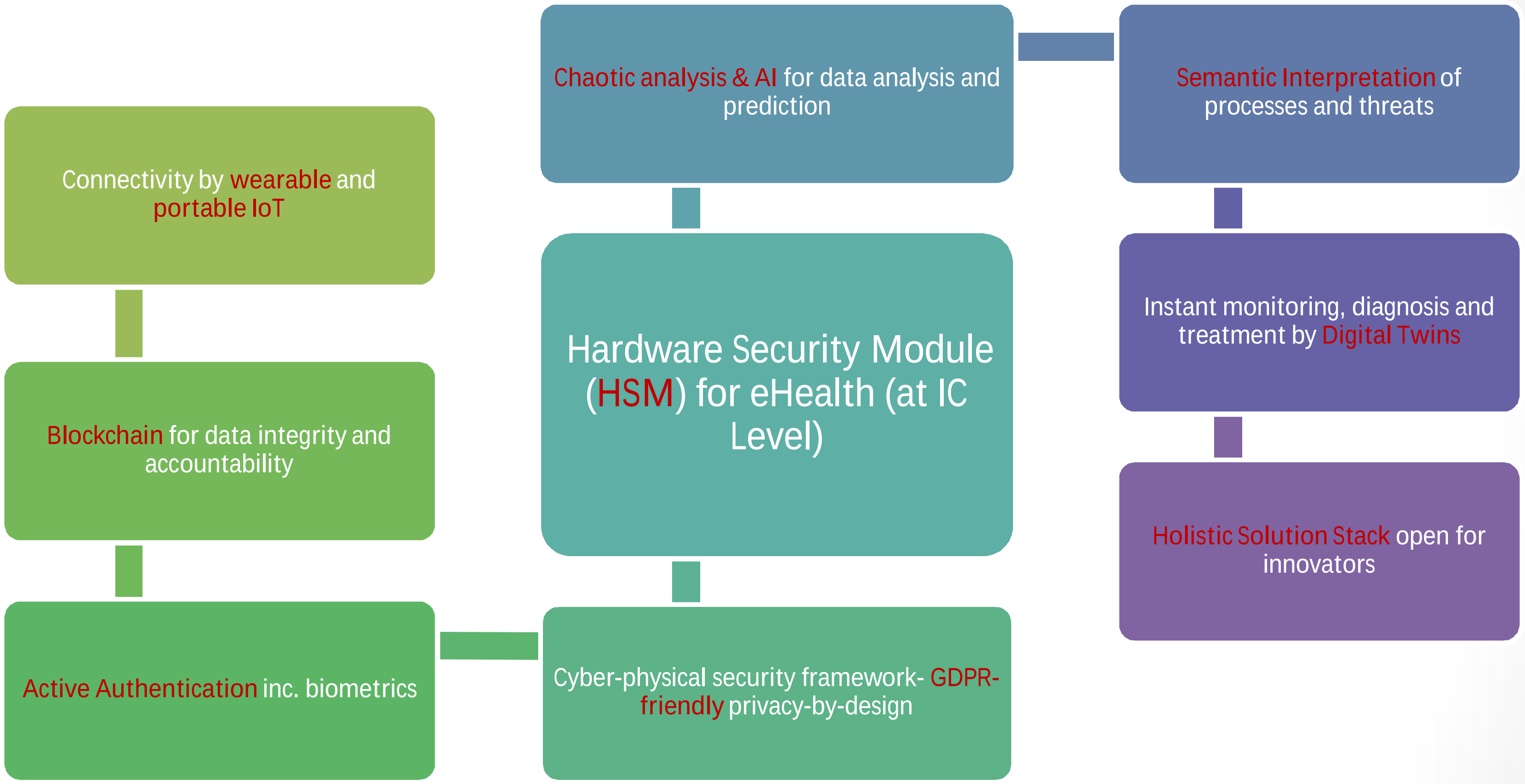
- Looking for:
  - *Possible coordinator*
  - *Blockchain technology experts*
  - *IoT experts*

# An Accountable, Secure & Semantic Cyber-Physical HealthChain

- *Alper Kanak, PHD*
- *alper.kanak@ergtech.ch*
- *ERARGE & ERGTECH (ERGUNLER R&D Center)*
- Role: *S/T Provider and Concept Builder*

- Proposal activity: *SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors (b) [2019]: Digital security, privacy and personal data protection in healthcare ecosystem*

# HealthChain, a project digitally chains



Connectivity by wearable and portable IoT

Blockchain for data integrity and accountability

Active Authentication inc. biometrics

Chaotic analysis & AI for data analysis and prediction

Hardware Security Module (HSM) for eHealth (at IC Level)

Cyber-physical security framework- GDPR-friendly privacy-by-design

Semantic Interpretation of processes and threats

Instant monitoring, diagnosis and treatment by Digital Twins

Holistic Solution Stack open for innovators

# Project participants

- Proposed coordinator:
  - *Administrative Coordinator: being sought*
  - *Technical Coordinator: ERARGE (IoT, CPS, chaotic analysis)*
- Partners / Other participants:
  - *A Swiss Unviersity → active authentication, machine learning*
  - *A German LE → CPS, IoT security*
  - *Turkish Ministry of Health → end user, strategy and politics*
  - *A Romanian Company → SW integrator, cloud provider*
  - *A French Chip design and Manufacturing Company → Wearable and Iot Devices, IC*
  - *A Spanish Company → System Integrator*
  - *A Leading UK/Ireland research centre*
  - *University of Tokyo (contributor) → Chaotic analysis and Chaotic Chips*
- Looking for partners with the following expertise/ technology/ application field:
  - *Biometric*
  - *Blockchain*
  - *legal and ethics experts*
  - *Socioeconomic analysis*
  - *End users with high impact*

# SPHERE

# Secure Pervasive Healthcare

- *Gavin McWilliams*
  *Director of Engineering*
- *g.mcwilliams@qub.ac.uk*
- *CSIT, Queen's University Belfast*
- Role: *Proposal coordinator or WP leader*

- Proposal activity: *Secure Societies,* ***SU-DS05-2019****,*
  Digital security, privacy, data protection and accountability in critical sectors
  ***b)*** *Digital security, privacy and personal data protection in healthcare ecosystem*

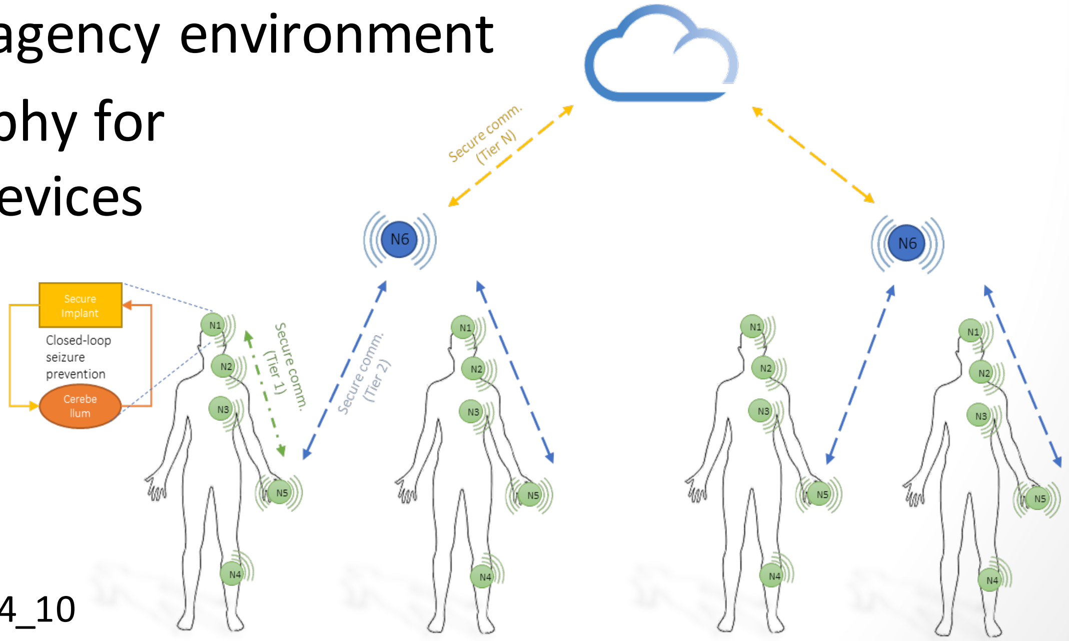
QUEEN'S UNIVERSITY BELFAST

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

The Queen's Anniversary Prizes
For Higher and Further Education
2015

# Privacy Preserving Health Analytics

- Secure computation on encrypted data, targeting the healthcare domain
- Optimised hardware designs of somewhat homomorphic encryption (SHE) and functional encryption (FE) schemes
- Privacy preserving medical record retrieval operating in a cross-border or multi-agency environment
- Lightweight cryptography for implantable medical devices



https://doi.org/10.1109/TC.2017.2677426
https://doi.org/10.1109/TC.2015.2498606
https://doi.org/10.1007/978-3-319-49890-4_10

# Project participants

- Proposed coordinator: QUEEN'S UNIVERSITY BELFAST | CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- Potential Partners:

Erasmus MC University Medical Center Rotterdam

USI Università della Svizzera italiana

UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh

CUH Ospidéal Ollscoile Chorcaí Cork University Hospital

SmartCardia

- Looking for partners with the following expertise/ technology/ application field:
  - *CERT/ CSIRT in Healthcare environment*
  - *Secure exchange of vulnerability data*
  - *Medical Records (EHR) Management Systems*

# Federated machine learning for digital security, privacy, data protection and accountability in healthcare ecosystem

- *Marcos Sacristán, marcos.sacristan@treetk.com*
  *Jaime Medina, jaime.medina@treetk.com*
- *Tree Technology - www.treetk.com (former Treelogic)*
  - *Spanish SME*
- Role: *Coordination*

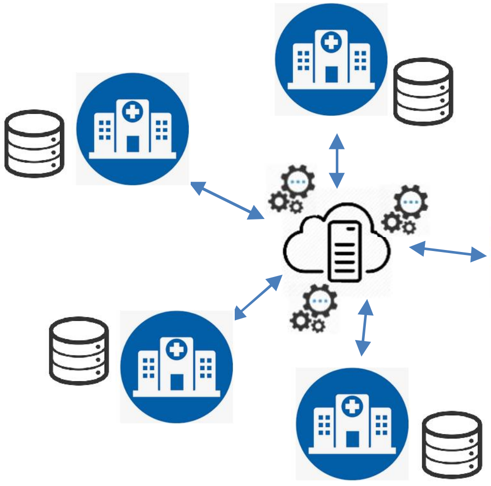
- Proposal activity: *SU-DS05-2019: Digital security, privacy, data protection and accountability in critical sectors - (b) Digital security, privacy and personal data protection in healthcare ecosystem*

# Proposal idea/content

- *Based on results from ongoing [MUSKETEER H2020 project](http://www.treetk.com/en/R&D_Musketeer.html):* *http://www.treetk.com/en/R&D_Musketeer.html*
- *Validated federated privacy-preserving machine learning platform on healthcare that is demonstrably:*
  - *safe enough (privacy-preserving in the face of legitimate and illegitimate –attempted- access and use)*
  - *interoperable, scalable and efficient enough to be deployed to a significant representation of the personal and private data in the healthcare sector.*

*Toolkit:*

- *Privacy preserving platform*
- *Personal data protection*
- *Cybersecurity*
- *Federated Machine Learning*
- *Healthcare-oriented*



*Personal data protection*

*Data do not leave health centre facilities*

*Privacy and scalability guaranteed by design*

*Data models are shared among health centres*

# Project participants

- Proposed coordinator: *TREE TECHNOLOGY (Open)*
- Partners / Other participants:
  - Experts in federated machine learning
  - Academics on privacy-preserving learning
  - *Healthcare centres (end-users)*

- Looking for partners with the following expertise:
  - *Data providers in healthcare sector*
  - *Other stakeholders in the healthcare ecosystem*
  - *CERT*/CSIRTS***
  - *Cybersecurity experts in healthcare sector*

**CERT, Computer Emergency Response Team*
***CSIRT ,Computer Security Incident Response Team*

Marcos Sacristán (TREE TECHNOLOGY) – marcos.sacristan@treetk.com

# MobID

- *Marc NORLAIN*
- *marc.norlain@ariadnext.com*
- ARIADNEXT
- Role: Proposal coordinator

- Proposal activity: SU-DS03-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
  - Sub-topic (a): protecting citizens' security, privacy and personal data

# Proposal idea/content

- MobID will develop a new platform that will allow easy and secured self-enrollment to provide a cost effective and secure mobile eID compliant with eIDAS regulation.
- It will combine groundbreaking technologies to allow self-enrollment through multiple identity proofs assessment beyond national identity schemes
- It will leverage the ubiquity of mobile devices and the fact that citizens are familiar with mobile interactions.
- By using privacy by design principles, it will provide citizens as well as public authorities and private actors with a unique, user-friendly, secured, interoperable solution and will thus promote trust and confidence in internet service and boost Digital Single Market.
- It will be tested by both public and private actors and integrated into eIDAS hubs.

marc.norlain@ariadnext.com | montaser.awal@ariadnext.com

# Project participants

- Proposed coordinator: ARIADNEXT
- Partners / Other participants:
    - AUDENCIA (FR) – HSS
    - CVC (ES) – Document assesment
    - IDIAP (CH) – Biometrics
    - INRIA (FR) – Privacy and data protection
    - OLAII (SLV) - End-User (tickets / cashless payments)
    - SCyTL (ES) - End-User (e-voting)
- Looking for partners with the following expertise/ technology/ application field:
    - *Applied Cryptography*
    - *End-users (banking industry, electronic signature, online gambling)*
    - *Governments willing to implement Mobile eID*

marc.norlain@ariadnext.com | montaser.awal@ariadnext.com