R&D IN CYBERSECURITY AT THE UPC

2023

Generalitat de Catalunya

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

CoFunded by the European Union

CONTENT

01

UPC

Knows the Universitat Politècnica de Catalunya (UPC) and discovers some of its figures.

02

CYBERSECURITY

What is cybersecurity? And why is it key in development?

03

RESEARCH AND INNOVATION

Description of the activity, research groups, centers and institutes that generate knowledge in the field of cybersecurity.

04

UPC EXCELLENCE R+D+I

Selection of the most impactful projects, articles, and doctoral theses related to cybersecurity at UPC

05

TRAINING

Bachelor's degrees, master's programs, and doctoral degrees offered at UPC in the field of cybersecurity.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

01 UPC

The Universitat Politècnica de Catalunya (UPC) is a public research university in the fields of engineering, architecture, sciences, and technology, with a strong presence and active involvement in the industrial hubs of the region. UPC contributes to Catalonia's innovation system through research projects, contracts, knowledge valorization, and technology commercialization to address the major challenges of society.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

RESEARCH AND INNOVATION ACTIVITY AT UPC 2022

227
National projects

162
International projects

1.011
R&D active projects

€78,1 m
In project revenues

€121,9 m
In contract revenues

2.526
Articles in scientific journals

331
Theses

14
Registered patents

13
New Technology-Based Companies

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

02

CYBERSECURITY

Cybersecurity encompasses the security of information systems, digital devices, and data networks. The term cybersecurity includes physical, logical, and management measures aimed at protecting digital assets, entities, and individuals. Nowadays, it is essential to be able to communicate while ensuring security, privacy, knowledge protection, authenticity, and auditability.

CYBERSECURITY AREAS

NETWORK SECURITY

In an increasingly interconnected world, **protecting the virtual dimension** of the infrastructure where all online activity takes place is one of the top priorities.

The field of network security focuses on safeguarding communication networks and the devices connected to them against cyber threats and attacks.

This includes the implementation of firewalls, **intrusion detection**, data encryption, and other security measures to prevent unauthorized access.

INFORMATION SECURITY

In the realm of networks, information refers to digital data that is transmitted and shared among interconnected devices. This information can range from text messages and emails to multimedia files such as images and videos**. Effective management of this information is essential to ensure effective communication.**

Protecting the information stored and transmitted through computer systems is fundamental. This involves data encryption, access management, the implementation of **security policies**, and other measures to ensure the confidentiality, integrity, and availability of information.

ARTIFICIAL INTELLIGENCE SECURITY

This technology is already present in almost every aspect of our lives. From virtual assistants that help us plan our day to **autonomous cars** promising a safer future on the roads, AI makes our lives easier. It enhances our healthcare, personalizes our learning experiences, and helps us make informed decisions in our finances.

As AI and machine learning play an increasingly important role in technology, security is required to protect the models, data, and AI-driven decisions against attacks.

CYBERSECURITY AREAS

SECURITY IN SUPPLY CHAIN

Digitization, automation, and the adoption of cloud-based supply chain management systems enable greater efficiency and visibility throughout the entire process. Furthermore, global **connectivity facilitates real-time collaboration** with suppliers, carriers, and customers worldwide, speeding up the delivery of products and services. In summary, technology and connectivity are fundamental pillars for an agile, efficient supply chain capable of adapting to the changing **demands of the global market.**

As more businesses adopt cloud services, **cloud security has become critical**. This includes protecting data and applications stored in public, private, or hybrid cloud environments.

CLOUD SECURITY

Cybersecurity in the cloud is essential in an increasingly digitized world. As organizations migrate their data and applications to public, private, or hybrid cloud environments, they face new security challenges. **Protecting confidential data, preventing cyber threats**, and ensuring business continuity are critical priorities. This involves the implementation of robust security measures, **such as data encryption**, multi-factor authentication, and continuous monitoring. Collaboration between cloud service providers and businesses is key to ensuring a secure cloud environment and safeguarding the confidentiality and integrity of digital assets.

As more companies adopt cloud services, **cloud security has become critical**. This includes protecting data and applications stored in public, private, or hybrid cloud environments.

Research and development (R&D) drive the creation of new cybersecurity technologies and tools, such as advanced threat detection systems, biometric authentication solutions, stronger encryption algorithms, and artificial intelligence techniques for threat identification.

Cybersecurity researchers conduct thorough analyses to identify vulnerabilities in existing systems and software. This research enables organizations to apply fixes and protect their systems against known threats. Additionally, cybersecurity simulations and exercises are conducted to assess the readiness of organizations and governments in the face of potential cyberattacks.

BASIC CONCEPTS (Termcat)

Firewall

“A firewall is software or hardware that manages and controls the communications of a local network with external networks to ensure security.”

Malware

"Software specifically designed to take control of a computer system, interfere with its normal operation, disrupt it, or cause damage."

Two-Factor authentication

"Verification of a user's identity based on a dual-key system, meaning it uses two different security elements to authenticate identity and log in."

Big Data

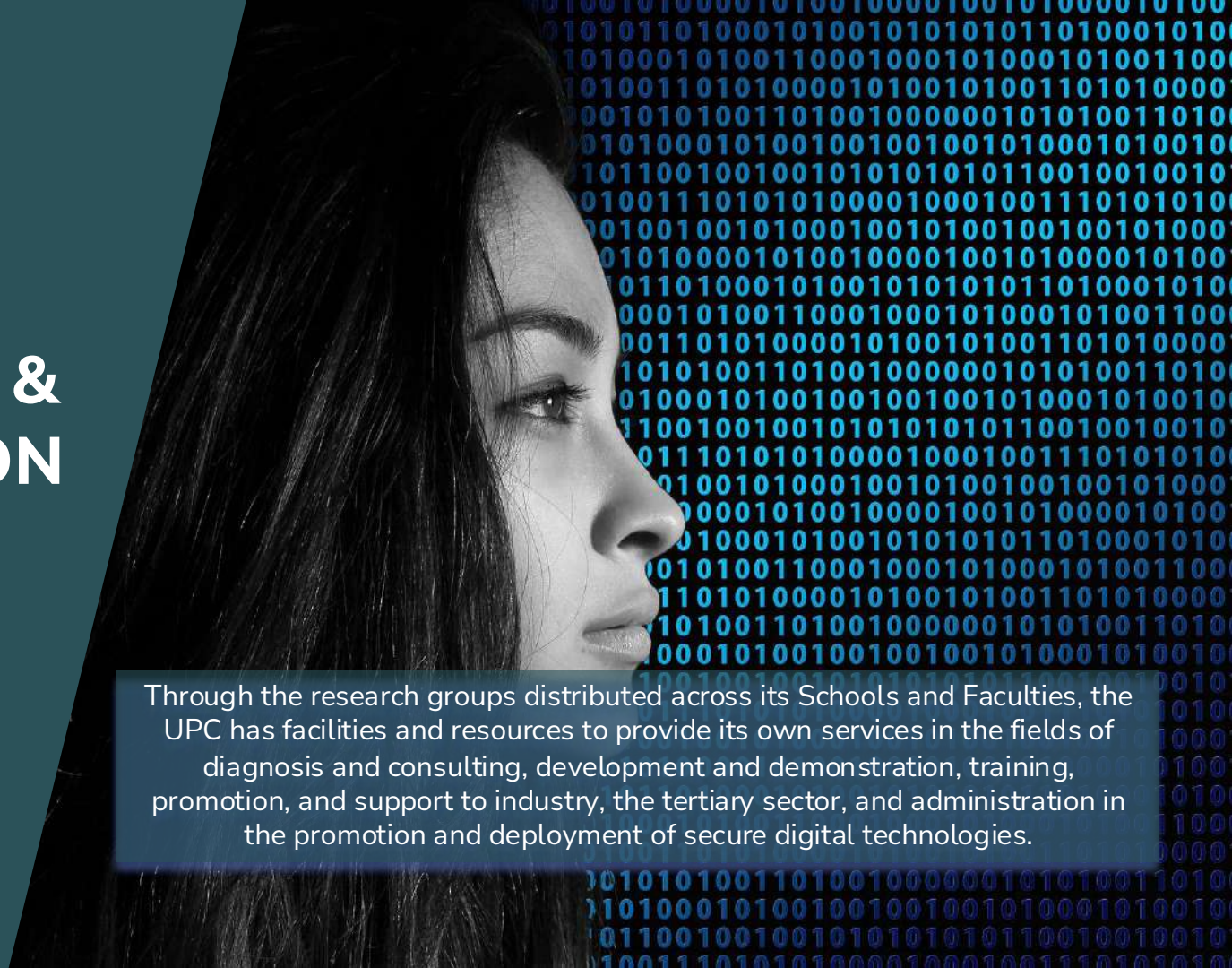
"Set of data that, due to its volume, nature, and the speed at which it must be processed, exceeds the capacity of typical computer systems."

Phishing

"Fraudulent practice involving the simulation of a false identity, often by impersonating a specific person or organization, whether through email, a phone call, or other means, with the aim of persuading potential victims to take an action that could lead to the theft of their personal data."

03

RESEARCH & INNOVATION



Through the research groups distributed across its Schools and Faculties, the UPC has facilities and resources to provide its own services in the fields of diagnosis and consulting, development and demonstration, training, promotion, and support to industry, the tertiary sector, and administration in the promotion and deployment of secure digital technologies.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

ACTIVITY EXAMPLES I

Softwarization of Internet network services and applications for 5G.

Design of next-generation networks, including routing, SDN, network management, security, etc.

Information management, with an emphasis on aspects related to information quality, exploration of data from various sources, and large volumes of data.

Scientific and technological development of remote data acquisition equipment and systems.

Development of information protection techniques, especially in the anonymization of databases to safeguard user privacy when this data is analyzed by third parties.

Audit and risk analysis of computer and industrial systems.

Response to incidents and forensic analysis of compromised computer systems.

ACTIVITY EXAMPLES II

Increasing the capacity of radio systems to handle large amounts of high-speed traffic to maximize system capacity and deliver quality of service.

Study of protocols that enable network self-configuration, including the study of ad hoc routing protocols, resource discovery, and autoconfiguration.

Ensuring cyber resilience in the supply chain of ICT systems in complex environments.

Mining, validation, correction, and fusion of heterogeneous data to support cognitive information.

Digital signal processing, electronic design of data acquisition systems, and automation of complex measurement systems based on the use of intelligent monitoring and control devices.

Optimization in the management of hardware and software resources, both by the operating system and by virtualized elements.

Design of fault-tolerant, resilient, and secure diagnosis and control systems.

UPC RESEARCH GROUPS AND LABORATORIES IN CYBERSECURITY

- BAMPLA - Design and Evaluation of Broadband Networks and Services.
- CBA - Broadband Communications Systems and Architectures Research Group
- CRAAX - Advanced Network Architectures Lab
- DAMA – Data Management Group
- IMP – Information Modeling and Processing
- ISG - Information Security Group
- InLAB FIB – Laboratory of Computer Projects
- MAK - Mathematics Applied to Cryptography
- MCIA - Motion Control and Industrial Applications Research Group
- SAC – Advanced Control Systems
- SISCOM – Smart Services for Information Systems and Communication Network
- WNG - Wireless Networks Group

UPC SPECIFIC RESEARCH CENTERS

CCABA – Advanced Broadband Communications Center

The CCABA aims to create research structures in response to the emergence of new technologies (5G, 6G, IoT, Network and Service Virtualization, Artificial Intelligence and Augmented Reality, Machine Learning, Smart Cities, etc.).

CS2AC – Supervision, Safety and Automatic Control

A multidisciplinary group of UPC professors and researchers from the CSIC dedicated to the broad field of automatic control and monitoring systems. The main objective of CER CS2AC-UPC is to contribute to the competitiveness of our companies and to scientific and technical knowledge through the development of advanced control systems and the design of optimal systems, as well as fault-tolerant control of complex systems.

SARTI - Technological Development Center for Remote Data Adquisition and Information Processing Systems

The group's objective is the scientific and technological development of remote acquisition systems and equipment, with a particular emphasis on virtual instrumentation and oceanography, including simulations and statistical analysis methods, through the use of advanced electronic design techniques.

IDEAI - Intelligent Data Science & Artificial Intelligence Research Center

IDEAI-UPC is a research center certified as a consolidated research group of recognized excellence by AGAUR (SGR-1532), composed of seven specialized research nuclei in various branches of AI, with more than 80 full-time researchers, 72 permanent senior researchers, and 150 doctoral and master's students.

LABORATORIES AND INSTITUTES

LABORATORIES

- **RDLAB – Research and Development Lab**

  The Research and Development Laboratory (/rdlab) focuses on enhancing research and technology transfer processes through IT support and services.

INSTITUTES

IRI – Institut de Robòtica i Informàtica Industrial

The Institute has three main objectives: promote fundamental research in Robotics and Applied Computer Science, collaborate with the community on industrial technological projects, and provide scientific education through postgraduate courses.

04

UPC EXCELLENCE PROJECTS

In this document, excellence projects are considered those in which:

- The scientific process is rigorous and meets high-quality standards.
- They are strategic and driving forces.
- They commit to social challenges and have a significant scientific and socioeconomic impact.
- They have an impact on the territory.
- They involve various participating entities from the quadruple helix, making the projects multidisciplinary.

The UPC Excellence Projects are funded by various programs, such as the State Plan or Horizon Europe.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UPC EXCELLENCE PROJECTS

MEDSURANCE - Advanced Security-for-safety Assurance for Medical Device IoT

Advancements in healthcare technology systems have given rise to complex socio-technical architectures that provide patient-centered services. However, along with clinical benefits, **security risks have also emerged**, which need to be managed.

The MEDSECURANCE project aims to develop new methodologies and technologies to ensure the effective and continuous **management of secure systems in the Internet of Medical Things (IoMT)**. Its focus includes understanding IoMT threats, considering system interdependencies, information exchange, and regulatory implications. **It will provide scalable solutions for secure system management that enhance cybersecurity decision-making and automate cybersecurity assurance**, working in collaboration with medical industry partners and healthcare stakeholders.

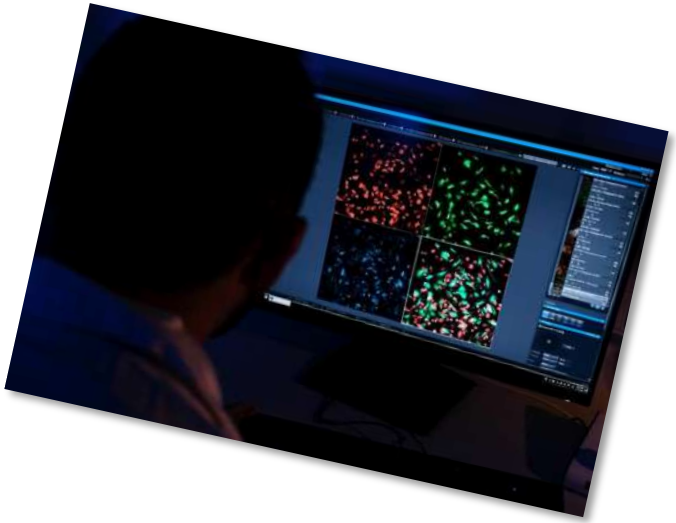


Image provided by Toni Santiso

UPC Research Group Involved: IMP- Information Modeling and Processing

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UPC EXCELLENCE PROJECTS

FISHY - A coordinated framework for cyber resilient supply chain systems over complex ICT infrastructures

The FISHY project aims to develop a platform that ensures cyber resilience in the supply chain of ICT systems in complex environments. This platform will enable secure orchestration of complex ICT systems from IoT to cloud infrastructure and networks, **managing risks, vulnerabilities, and security metrics**. Using intent-based interfaces and technologies such as data analytics, distributed ledgers, and artificial intelligence will be essential. Furthermore, the platform will be **designed to adapt in real-time and respond to cyberattacks, especially in the IoT domain**. This project includes use cases in sectors such as agriculture, manufacturing, and transportation, with the goal of demonstrating a proof of concept for the FISHY platform and establishing strategies for widespread adoption and dissemination.

UPC Research Group Involved: CRAAX

UPC EXCELLENCE PROJECTS

i3-MARKET - Intelligent, Interoperable, Integrative and deployable open source MARKETplace with trusted and secure software tools for incentivising the industry data economy

The i3-MARKET project addresses the growing demand for an innovative European Single Data Market on market platforms, demonstrating through industrial implementations that data economy growth is possible. The i3-MARKET proposal provides technologies for collaboration and federation of existing and future market platforms, **with a special focus on industrial data and sensitive business assets of SMEs and large industrial corporations.**

It is known that despite various research and innovation efforts in Big Data management, data personalization, and security, there is no widely accepted, reliable, and secure data market. **i3-MARKET will address this by developing missing technologies and solutions for a reliable, interoperable, and decentralized infrastructure**, called the i3-MARKET Software Framework or also known as the i3-MARKET Backplane, enabling federation through interoperability of existing and emerging data spaces and markets.

UPC Research Group Involved: ISG - Information Security Group

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UPC EXCELLENCE PROJECTS

COMPROMISE - Enhancing Communication Protocols with Machine Learning while Protecting Sensitive Data. Data privacy for communication networks and dynamic databases

The COMPROMISE project addresses the challenge of protecting privacy in a highly connected digital world. It focuses on improving privacy in network protocols and **preventing privacy attacks**. The project aims to balance the utility of technology with the protection of personal data, using expertise in security, privacy, communication protocols, and machine learning. Additionally, it is applied to wireless networks and routing protocols. **A practical case is MobilitApp**, an application that uses sensor data to enhance public transportation services.

UPC Research Group Involved: SISCOM

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UPC EXCELLENCE PROJECTS

RISEBLOCK - Privacy and security in public blockchains and their application to data marketplaces

The current data markets are closed and controlled by a few, limiting competition. Public Blockchains offer transparency and trust **based on smart contracts but raise privacy challenges.** Zero-Knowledge Proofs (ZKPs) can address these issues. This project focuses on creating data markets based on Public Blockchains and **investigating the security of Public Blockchains in general**. Data management in these Blockchains is also addressed, as well as how to control data redistribution. The goal is to promote a competitive and secure data economy where all stakeholders can participate freely under fair rules.

UPC Research Group Involved: ISG - Information Security Group

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UPC EXCELLENCE PROJECTS

IRIS - Artificial Intelligence threat Reporting and Incident response System

Advancements in Artificial Intelligence (AI) and the Internet of Things (IoT) have exponentially grown in recent years, **raising concerns about cybersecurity**. The IRIS project, funded by the European Union, will address the challenges of IoT and AI-driven ICT systems through a collaborative approach centered on Computer Emergency Response Teams (CERTs/CSIRTs).

Specifically, the project will provide CERTs/CSIRTs with a set of state-of-the-art incident response tools to assess, detect, respond to, and share threat and vulnerability information for IoT and AI-driven ICT systems. The project will establish the first dedicated online training and cyber exercises to prepare CERTs/CSIRTs for collaboratively **protecting critical infrastructures and systems against cross-border AI and IoT threats**. Pilot demonstrations will be conducted in Helsinki, Tallinn, and Barcelona.

UPC Research Group Involved: IMP – Information Modeling and Processing

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UPC EXCELLENCE PROJECTS

Research and investigation of tools and malware in cyberattacks on corporate infrastructures

The doctoral project will focus on the creation of tools, the definition of procedures during cybersecurity incident response, **and the analysis of malware software used by attackers**. This response will involve researching and analyzing the techniques and tactics used by cybercriminals, allowing for the definition of prevention and action measures against these threats.

The tools for analysis, response resolution, and implementation of protection measures may involve the use of various technologies, which could include open-source software projects, dedicated paid programs, various types of hardware, implementation of tools with artificial intelligence, etc**. The analysis prior to the implementation of protection measures will involve the study of malicious software**, both statically (reversing) and dynamically.

UPC Research Group Involved: ISG - Information Security Group

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

SOME PUBLICATIONS I

Ganguly, A.; S. Abadal; Thakkar, I.; Enright, N.; Riedel, M.; Babaie, M.; Balasubramonian, R.; Sebastian, A.; Pasricha, S.; Taskin, B. (2022) .Interconnects for DNA, Quantum, In-Memory, and Optical Computing: Insights from a panel discussion. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9714013
The article discusses the emergence of new computing paradigms, such as DNA, quantum, optical, and in-memory computing, driven by technological advancements. It also discusses the role of interconnections and the integration of technologies through chiplet-based architectures.

Leyva-Pupo, I., Cervello-Pastor, C., Anagnostopoulos, C., & Pezaros, D. P. (2022). Dynamic UPF placement and chaining reconfiguration in 5G networks. Computer Networks, 215, 109200. https://doi.org/10.1016/j.comnet.2022.109200
The article highlights the importance of Network Function Virtualization (NFV) and Multi-Access Edge Computing (MEC) in the development of 5G networks. It proposes solutions to optimize the placement and sequencing of virtual network functions, ensuring efficiency and quality of service in MEC environments.

Pujol-Perich, D., Suárez-Varela, J., Cabellos-Aparicio, A., & Barlet-Ros, P. (2022). Unveiling the potential of graph neural networks for robust intrusion detection. Performance evaluation review, 49(4), 111-117. https://doi.org/10.1145/3543146.3543171
In recent years, there has been an increase in cyberattacks with severe economic and privacy damage, highlighting the need for accurate Network Intrusion Detection Systems (NIDS). The article proposes a Graph Neural Networks (GNN) model that, by considering the relationships between network connections, achieves exceptional robustness against adversarial attacks compared to conventional ML techniques.

SOME PUBLICATIONS II

Rodríguez, E., Otero, B., & Canal, R. (2023). A survey of machine and deep learning methods for privacy protection in the internet of Things. Sensors, 23(3), 1252. https://doi.org/10.3390/s23031252
The article examines Machine Learning and Deep Learning-based solutions to preserve privacy in the Internet of Things (IoT), considering current threats and attacks in environments such as smart cities and autonomous vehicles.

Rodríguez, E., Valls, P., Otero, B., Costa, J. J., Verdú, J., Pajuelo, M. A., & Canal, R. (2022). Transfer-Learning-Based Intrusion Detection Framework in IoT networks. Sensors, 22(15), 5621. https://doi.org/10.3390/s22155621
The article addresses the increasing cyberattacks on the Internet of Things (IoT) and proposes a solution based on Transfer Learning (TL) to effectively detect zero-day attacks in 5G IoT networks with a lack of labeled data. This approach outperforms other systems in attack detection, demonstrating the effectiveness of TL in IoT environments.

Sedar, R.; Kalalas, C.; Vazquez, F.; Alonso, L.; Alonso, J. (2023). A comprehensive survey of V2X cybersecurity mechanisms and future research paths. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/10026338
The article discusses recent advances in Vehicle-to-Everything (V2X) communication, with an emphasis on improvements in connectivity and autonomous driving in transportation.

05 TRAINNING

BACHELOR'S DEGREE - UPC

- Bachelor's Degree in Telecommunication Systems Engineering (EETAC)
- Bachelor's Degree in ICT Systems Engineering (EPSEM)
- Bachelor's Degree in Telecommunication Technologies and Services Engineering (ETSETB)
- Bachelor's Degree in Telecommunication Electronics Engineering (ETSETB)
- Bachelor's Degree in Geoinformation and Geomatics Engineering (EPSEB)

MASTERS - UPC

- Master's degree in Cybersecurity (ETSETB)
- Master's degree in Advanced Telecommunication Technologies (ETSETB) i (EETAC)

Ph.D. PROGRAMS

- Ph.D. in Computer Science
- Ph.D. in Artificial Intelligence

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Més màsters: https://www.upc.edu/ca/masters
Més programes de doctorat: https://doctorat.upc.edu/ca/programes/

UPC-SCHOOL

- Master in Cybersecurity Management
- Postgraduate Program in Cyberattack Detection and Response
- Postgraduate Program in Cybersecurity Planning and Management
- Microcredential in Cybersecurity for Our Cities

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Més graus: https://www.upc.edu/ca/graus/

RESEARCH AND INNOVATION SUPPORT SERVICE

https://rdi.upc.edu
@RDI_UPC

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH