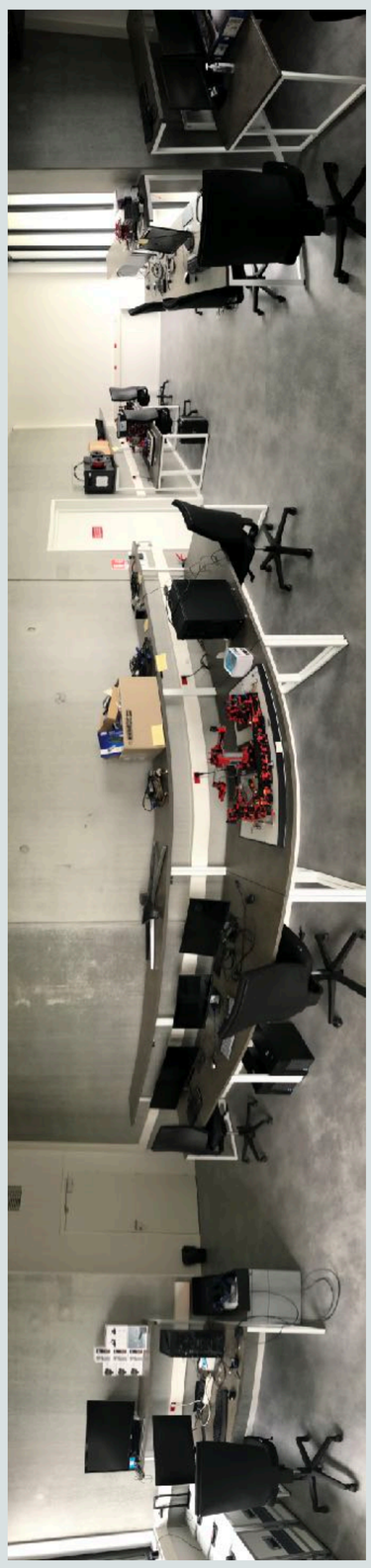
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIRE
CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/



We are hiring!

PostDoc (1 year/ full time 35h/w)
Cybersecurity for critical mobile Infrastructures

We are looking for an outstanding candidate to strengthen our research team. We offer challenging research in a rich environment with excellent research perspectives. This position is to be filled as soon as possible. Prolongation after one year might be possible if desired.

Context - the domain you will be working in

The Digital Transformation results in all kinds of infrastructures becoming software-controlled, networked, and remote-manageable. While this brings many opportunities, cybersecurity is its biggest challenge.
A central critical infrastructure affected by the Digital Transformation is transportation of humans and goods. Formerly isolated trains or buses become part of a connected mobility. Remote monitoring and over-the-air updates become reality. This requires strong security measures to be installed.

Scope - the topics you will be working on

The goal of this PostDoc is establishing and *heading the connected mobility cybersecurity research* line at the chair Cyber CNI in close collaboration with the chairholder and the industry partner. This includes setting up pilots for prototyping and evaluating the research, as well as regular interaction with the chair's PhDs, and other staff.

You will specify and implement at least one pilot for a connected vehicle that can receive over the air updates. You will identify security challenges and develop and test mitigations. The use of AI and human-machine-interfaces, e.g. in SOCs, will be central to your work. Distributed ledgers and other mechanisms can become important. Overall, you will be able to shape this new research axis together with the local experts.

Scenarios: Autonomous train, railways, signaling and stations will be important scenarios.

Keywords: Authentication, Authorization, Remote attestation, Access control, Software life-cycle, SOC, Threat Management, Risk Management, Safety vs. Security, Collaboration, AI, a plus would be knowledge in human-machine-interfaces, visualization, 3D visualization, Immersive Interfaces

Requirements - what you should bring

Solid and proven research skills. Curiosity and motivation to work in a dynamic research environment.

Knowledge: Knowledge in some or all of the following cybersecurity topics (please refer to these in your cover letter): SOC, threat intelligence, risk management, human-in-the-loop, 3D immersive interfaces, Update management, Security, Safety, Privacy, distributed approaches, AI, collaborative approaches

Languages: English (ability to read and write research papers in English), French (ability to communicate at least basically in French; courses can be taken to improve French)

Expectations - what you can expect to happen

If selected, you will have the chance to develop this research line together with the chairholder, the industry partners, and the researchers at IMT Atlantique. It is expected that part of the research gets submitted for publishing internationally. Collaboration with different PhD candidates is expected. Participation in teaching, especially MOOC creation will be possible, if wanted.

CHAIR OF
CYBER CNI
Critical National Infrastructures

Application process

Application deadline: 30.8.2021, 3pm CEST

Please send an email with one (1) PDF including:
- a motivational letter, covering the points "requirements" and your experience
- your CV
- your certificates (esp. PhD)
- a research statement (containing your research methodologies and possible research directions you would be interested to develop including scientific literature references)
- contact addresses (mail and phone) of 1-3 people we can contact to inquire information about you and at least two reference letters

to **recruit-postdoc-2021-1@cybercni.fr**.

This poster was made at the chaire Cyber CNI | https://cyber-cni.fr/ | Our monthly cybersecurity speaker series https://talk.cybercni.fr/ | Our science blog https://future-iot.org/

Institut Mines-Télécom
IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom
TELECOM Paris
TELECOM SudParis
AIRBUS AMOSSYS BNP PARIBAS La banque d'un monde qui change
EDF NOKIA Bell Labs SNCF PÔLE D'EXCELLENCE CYBER
Union européenne Région Bretagne

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIRE
CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/

Your future hosting environment: Excellence in Cybersecurity research and education in France

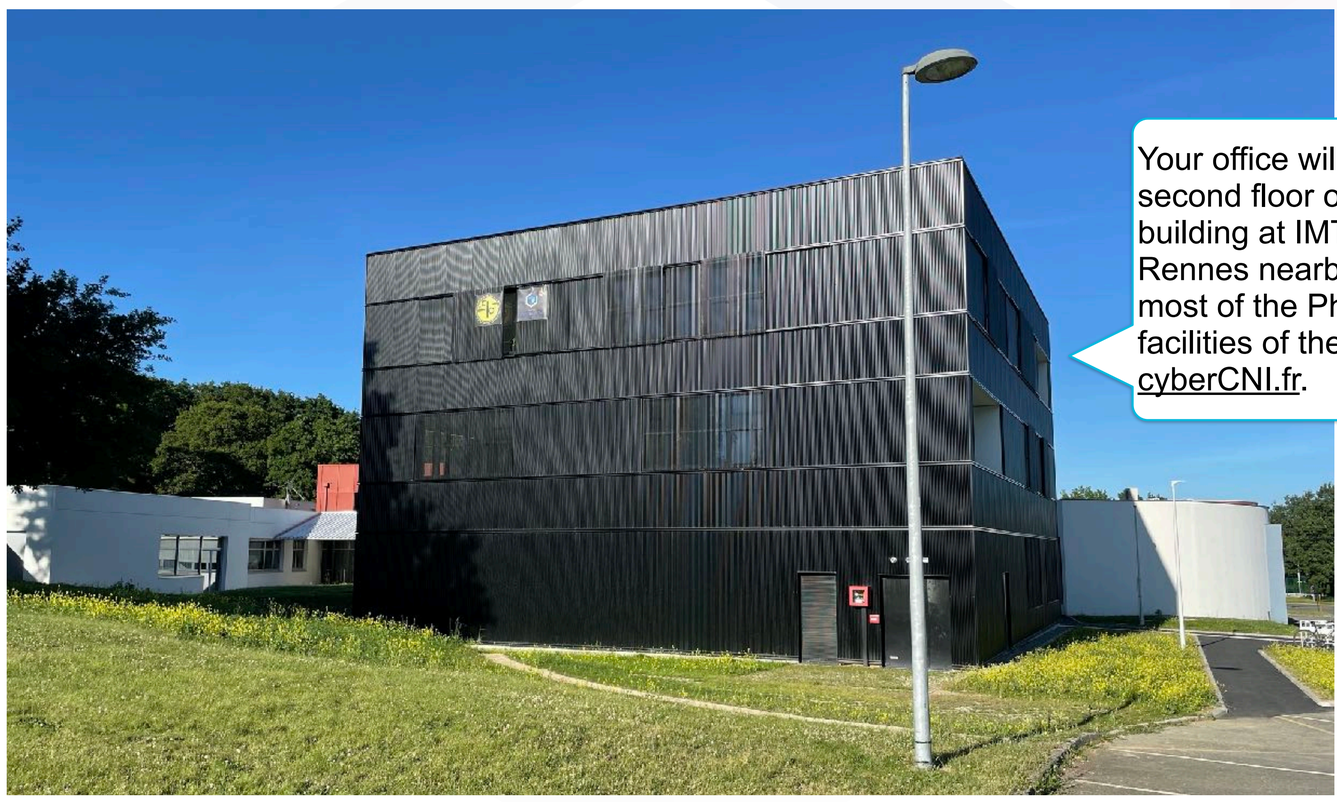
The hosting environment

The offered position is within one of France's finest addresses for research at a chair that is well-known for its excellence in cybersecurity.

The position is located within the technical university IMT Atlantique at the Rennes campus within the SRCD department at the chair Cyber CNI. Relocation to Rennes is required.

IMT: The Institut Mines Télécom (IMT) is France's biggest association of technical universities. IMT is a public institution dedicated to higher education and research for innovation.
It is a key player in the fusion of science, engineering and digital technology, and takes its schools' skills into the major fields of transformation in digital technology, industry, energy and the environment as well as their impact on the industry of the future, cities, health, and autonomy. For more info: https://www.imt.fr/en/imt/presentation-of-imt/

IMT Atlantique: Internationally recognized, IMT Atlantique's research positions it as one of the world's Top 400 Technological Universities. This research, conducted in the fields of digital sciences, engineering sciences, physics and management, fosters the conditions for inter-disciplinary research that is a source of innovation in response to the major challenges facing companies and society. For more info: https://www.imt-atlantique.fr/en/research-innovation



Your office will be located at the second floor of the newest building at IMT Atlantique Rennes nearby the chairholder, most of the PhDs and the lab facilities of the chaire cyberCNI.fr.

IRISA is today one of the largest French research laboratory (more than 850 people) in the field of computer science and information technologies.
Structured into seven scientific departments, the laboratory is a research center of excellence with scientific priorities such as bioinformatics, systems security, new software architectures, virtual reality, big data analysis and artificial intelligence.

Chair Cyber CNI: Cybersecurity for Critical Networked Infrastructures (Cyber CNI) is an industrial research chair. The Cyber CNI Chair at IMT Atlantique is devoted to research, innovation, and teaching in the field of the cybersecurity of critical infrastructures, including industrial processes, financial systems, building automation, energy networks, water treatment plants, transportation.

The chair covers the full stack from sensors and actuators and their signals over industrial control systems, distributed services at the edge or cloud, to user interfaces with collaborative Mixed Reality, and security policies.

The chair currently hosts 6+3 (three are getting recruited) PhD students, 1+3 PostDocs, 11 Professors, 1+1 engineers, and 2 internship students. The chair runs a large testbed that enables applied research together with the industry partners. The industry partners of the second funding round are Airbus, Amossys, BNP Paribas, EDF, Nokia Bell Labs, and SNCF.

Brittany is the cybersecurity region number 1 in France. The chair Cyber CNI is strongly embedded in the cybersecurity ecosystem through its partnerships with the Pôle d'Excellence Cyber (PEC) and the Brittany Region. The chair provides a unique environment for cybersecurity research with lots of development possibilities. For more info : https://cybercni.fr

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

SNCF