

# 2025 Activity Report

RESEARCH CENTRE: Inria Centre at Université de Lorraine  
IN PARTNERSHIP WITH: Université de Lorraine, CNRS

---

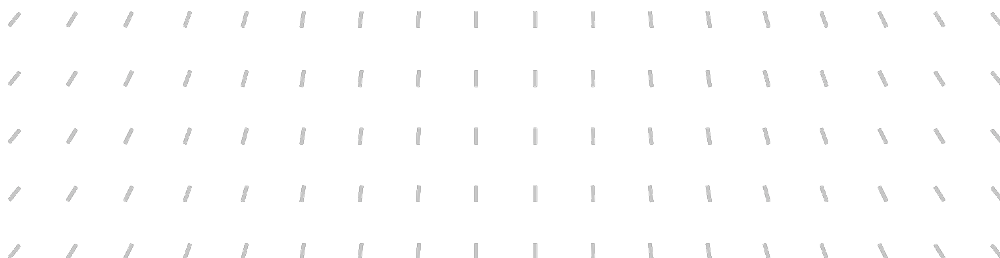
Project-Team

## RESIST

Resilience and elasticity for security and scalability of  
dynamic networked systems

---

*In collaboration with* Laboratoire lorrain de recherche en informatique et ses  
applications (LORIA)



## **Project-Team RESIST**

*Creation of the Project-Team: 2020 December 01*

Each year, Inria research teams publish an Activity Report presenting their work and results over the reporting period. These reports follow a common structure, with some optional sections depending on the specific team. They typically begin by outlining the overall objectives and research programme, including the main research themes, goals, and methodological approaches. They also describe the application domains targeted by the team, highlighting the scientific or societal contexts in which their work is situated. The reports then present the highlights of the year, covering major scientific achievements, software developments, or teaching contributions. When relevant, they include sections on software, platforms, and open data, detailing the tools developed and how they are shared. A substantial part is dedicated to new results, where scientific contributions are described in detail, often with subsections specifying participants and associated keywords. Finally, the Activity Report addresses funding, contracts, partnerships, and collaborations at various levels, from industrial agreements to international cooperations. It also covers dissemination and teaching activities, such as participation in scientific events, outreach, and supervision. The document concludes with a presentation of scientific production, including major publications and those produced during the year.

## Keywords

### Computer sciences and digital sciences

- A1.1.8. – Security of architectures
- A1.1.10. – Reconfigurable architectures
- A1.1.13. – Virtualization
- A1.2. – Networks
  - A1.2.1. – Dynamic reconfiguration
  - A1.2.2. – Supervision
  - A1.2.3. – Routing
  - A1.2.4. – QoS, performance evaluation
  - A1.2.6. – Sensor networks
  - A1.2.8. – Network security
- A1.3.3. – Blockchain
- A1.3.4. – Peer to peer
- A1.3.5. – Cloud
- A1.3.6. – Fog, Edge
- A1.5.2. – Communicating systems
- A2.3.5. – Cyber-physical systems
- A2.6. – Infrastructure software
- A3.2.2. – Knowledge extraction, cleaning
- A3.2.3. – Inference
- A3.3. – Data and knowledge analysis
- A4.1. – Threat analysis
- A4.4. – Security of equipment and software
- A4.9. – Security supervision
- A9. – Artificial intelligence
  - A9.2. – Machine learning
    - A9.2.1. – Supervised learning
    - A9.2.2. – Unsupervised learning
    - A9.2.3. – Reinforcement learning
  - A9.17. – Cybersecurity and AI

### Other research topics and application domains

- B5. – Industry of the future
- B6.3.2. – Network protocols
- B6.3.3. – Network Management
- B6.4. – Internet of things
- B6.5. – Information systems
- B6.6. – Embedded systems
- B7.2.1. – Smart vehicles
- B9.2.3. – Video games

## Contents

<b>Project-Team RESIST</b>	<b>1</b>
<b>1 Team members, visitors, external collaborators</b>	<b>5</b>
<b>2 Overall objectives</b>	<b>6</b>
2.1 Context . . . . .	6
2.2 Challenges . . . . .	7
<b>3 Research program</b>	<b>7</b>
3.1 Overview . . . . .	7
3.2 Monitoring . . . . .	8
3.3 Analytics . . . . .	8
3.4 Orchestration . . . . .	9
<b>4 Application domains</b>	<b>9</b>
4.1 Internet . . . . .	9
4.2 SDN and Data-Center Networks . . . . .	10
4.3 Fog and Cloud computing . . . . .	10
4.4 Cyber-Physical Systems . . . . .	10
<b>5 Highlights of the year</b>	<b>11</b>
5.1 Awards . . . . .	11
<b>6 Latest software developments, platforms, open data</b>	<b>11</b>
6.1 Latest software developments . . . . .	11
6.1.1 ROSCA . . . . .	11
6.1.2 llm-cvx . . . . .	11
6.1.3 C-CyberBattleSim . . . . .	12
6.2 New platforms . . . . .	12
6.3 Open data . . . . .	13
<b>7 New results</b>	<b>13</b>
7.1 Monitoring . . . . .	13
7.1.1 Security of IPFS DHT . . . . .	13
7.1.2 Optimizing the Transport of Low-latency and High-bitrate Traffic . . . . .	14
7.1.3 AI driven Monitoring in Cloud-Edge-IoT continuum . . . . .	14
7.2 Analytics . . . . .	15
7.2.1 Efficient Distribution of Security Filtering Rules in SDN . . . . .	15
7.2.2 Characterization and Troubleshooting of Cloud Gaming Applications on Mobile Networks . . . . .	15
7.2.3 Mitigating Synchronization Attacks on Distributed and Cooperative Microgrid Control Systems . . . . .	16
7.2.4 Cyber-Attack Paths Prediction . . . . .	16
7.2.5 Offensive and Defensive Cyber Security Capabilities of Large Language Models . . . . .	17
7.2.6 Security Alerts Correlation and Priorisation . . . . .	17
7.2.7 Assesment of Network Intrusion Dataset . . . . .	17
7.3 Orchestration . . . . .	18
7.3.1 Traffic Engineering for enhancing Quality of Service in 5G networks . . . . .	18
7.3.2 Security Configuration for Cloud Services . . . . .	18
7.3.3 Intelligent Configuration and Update for Future Networks . . . . .	19
<b>8 Bilateral contracts and grants with industry</b>	<b>20</b>
8.1 Bilateral grants with industry . . . . .	20

<b>9 Partnerships and cooperations</b>	<b>20</b>
9.1 International initiatives	20
9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program	20
9.1.2 Inria associate team not involved in an IIL or an international program	21
9.1.3 Visits of international scientists	21
9.1.4 Visits to international teams	22
9.2 National initiatives	23
9.2.1 ANR	23
9.2.2 PEPR	23
9.2.3 Inria joint Labs	26
9.3 Regional initiatives	26
<b>10 Dissemination</b>	<b>27</b>
10.1 Promoting scientific activities	27
10.1.1 Scientific events: organisation	27
10.1.2 Scientific events: selection	27
10.1.3 Journal	28
10.1.4 Invited talks	28
10.1.5 Leadership within the scientific community	29
10.1.6 Scientific expertise	29
10.1.7 Research administration	29
10.2 Teaching - Supervision - Juries - Educational and pedagogical outreach	29
10.2.1 Teaching	29
10.2.2 Supervision	30
10.2.3 Juries	31
10.2.4 Specific official responsibilities in science outreach structures	32
10.2.5 Participation in Live events	32
<b>11 Scientific production</b>	<b>33</b>
11.1 Major publications	33
11.2 Publications of the year	33

# 1 Team members, visitors, external collaborators

## Research Scientists

- Isabelle Chrisment [Team leader, INRIA, Professor Detachement, until Jun 2025, HDR]
- Nicolas Schnepf [INRIA, Researcher]

## Faculty Members

- Abdelkader Lahmadi [Team leader, UL, Professor, from Jul 2025, HDR]
- Laurent Andrey [UL, Associate Professor]
- Thierry Arrabal [UL, Associate Professor, from Sep 2025]
- Rémi Badonnel [UL, Professor, HDR]
- Thibault Cholez [UL, Associate Professor]
- Olivier Festor [UL, Professor, HDR]
- Abdelkader Lahmadi [UL, Associate Professor, until Jun 2025]

## Post-Doctoral Fellows

- Satou Kpoze [INRIA, Post-Doctoral Fellow, from Nov 2025]
- Runbo Su [UL, until Aug 2025]

## PhD Students

- Omar Anser [INRIA, until Sep 2025]
- Ahmad Atwi [INRIA]
- Enzo D'Andrea [UL, ATER]
- Mohamed Amine El Yagouby [UL]
- Mohammadreza Ghafari [UL]
- Katsuki Isobe [INRIA]
- Santiago Rios Guiral [UL, from May 2025]
- Jhon Sebastian Rojas Rodriguez [UL]
- Franco Terranova [UL]
- Gaelle Manuela Yonga Yonga [INRIA, from Dec 2025]
- Wafik Zahwa [UL, ATER, from Oct 2025]

## Technical Staff

- Remi Garcia [INRIA, Engineer]
- Matthews Jose [INRIA, Engineer, from Mar 2025]
- Matthews Jose [TELECOM NANCY, Engineer, until Feb 2025]
- Joel Ky [INRIA, Engineer, until Mar 2025]

## Interns and Apprentices

- Jorge Buzzio [UL, from Jun 2025]
- Thanh Thao Hoang Nguyen [UL, Intern, until May 2025]
- Satou Kpoze [INRIA, Intern, until Apr 2025]
- Nathan Lienard [INRIA, Intern, from Jun 2025 until Aug 2025]
- Raphael Michon [INRIA]
- Sana Rekbi [UL, from Jun 2025 until Aug 2025]
- Marcella Leticia Teixeira Scholze [INRIA, Intern, from Jun 2025 until Aug 2025]
- Aristide Urli-Canel [INRIA, Intern, from Jun 2025 until Aug 2025]

## Administrative Assistants

- Emmanuelle Deschamps [INRIA]
- Delphine Hubert [UL]
- Elsa Maroko [CNRS]
- Gallown Nizard [UL]
- Cecilia Olivier [INRIA]

## Visiting Scientist

- Sora Akagawa [UNIV OSAKA PREFECTURE, from Sep 2025 until Nov 2025]

## External Collaborator

- Jérôme François [Luxembourg University]

## 2 Overall objectives

### 2.1 Context

The increasing number of components (users, applications, services, devices) involved in today's Internet as well as their diversity make **the Internet a very dynamic environment**. Networks and cloud data centers have been becoming vital elements and an integral part of emerging **5G infrastructure**. Indeed, networks continue to play their role interconnecting devices and systems, and clouds are now the de facto technology for hosting services, and for deploying storage and compute resources, and even Network Functions (NFs).

While telecom operators have been historically providing Internet connectivity and managing the Internet infrastructure and services, they are now losing control to other stakeholders, particularly to Over-the-Top (OTT) content and service providers. Therefore, the delivery of Internet services has increased in complexity to mainly cope with the diversity and exponential growth of network traffic both at the core and at the edge. Intermediate players are multiplying and each of them has been proposing solutions to enhance service access performance.

In the Internet landscape, no single entity can claim a complete view of Internet topology and resources. Similarly, a single authority cannot control all interconnection networks and cloud data centers to effectively manage them and **provide reliable and secure services** to end users and devices at scale. The **lack of clear visibility into Internet operations** is exacerbated by the **increasing use of encryption solutions** which contributes to traffic opacity.

## 2.2 Challenges

In this context two main challenges stand out:

- **Scalability:** As mentioned above, the Internet ecosystem is continuously expanding in both size and heterogeneity. Scalability was already a challenge in the last decade but solutions mainly focused on scaling one dimension at a time, e.g. increasing the capacity of network links or that of compute resources in order to face peak demand, even if it is infrequent. Such **over-provisioning** however wastes significant resources and **cannot cope with future demand** at a reasonable cost. Scalability must be ensured across multiple dimensions and many orders of magnitude: more users, devices, contents and applications.
- **Security:** Security has gained a lot of importance in the last few years because the Internet has become a lucrative playground for attackers with large numbers of potential victims and numerous ways to reach them. Advanced Persistent Threats (APT) are the most sophisticated representatives of this evolution. Such **targeted attacks do not rely on generic scenarios**, usually described as a set of signatures. They are **complex by nature** and their investigation requires the **analysis of various sources of data**. At the same time, the generalization of encryption renders all deep packet inspection techniques obsolete and threat hunting becomes an even bigger challenge.

Additionally, an underground economy has been developed by cyber-criminals. Finally, because many applications are now provided as cloud-based services, physical isolation is also harder with potential attackers able to act directly in the field.

The highly dynamic nature of the Internet ecosystem, the requirement for higher and higher scalability, and the rising security threats have shown the **limitations of traditional approaches to address these challenges**. RESIST focuses on two complementary paradigms for achieving security and scalability:

- **Elasticity** refers to the ability of a system to **scale up and down on demand**. Elasticity of compute resources became more accessible with the advent of cloud computing. It has been recently leveraged in support of Network Function Virtualization (NFV) coupled with Software-Defined Networking (SDN). Understanding the dynamics of networked systems is critical in order to benefit from and efficiently orchestrate elasticity at all levels of the network, the system and the applications. On the one hand, elasticity facilitates scalability, as well as security by instantiating virtualized network security functions (e.g., firewall, IDS, DPI, etc.) on demand. On the other hand, it could increase the attack surface. This dilemma must be addressed. Moreover, issues inherent to elasticity such as the dynamic deployment and migration of resources bring new challenges in NFV environments since network functions are different from those of common cloud applications deployed in virtual machines and containers, e.g. in terms of network throughput.
- **Resilience** refers to the ability of a system to **adapt itself when facing challenging situations**. It is reasonable to assume that any system may face an attack for which protection mechanisms may fail. A comprehensive approach to resilience that considers not only the network and system resources but also the supported users and applications brings both benefits and challenges since users and applications can be very diverse, ephemeral and mobile. Applications are also deployed in dynamic environments like cloud platforms and are frequently reconfigured.

RESIST aspires to make **large-scale** networked systems **more secure and more resilient**, leveraging resource **elasticity** and assuming a highly dynamic environment.

## 3 Research program

### 3.1 Overview

The project aims at designing, implementing and validating novel models, algorithms and tools to **make networked systems elastic and resilient so as to enhance their scalability and security**, assuming users, applications and devices whose volume and heterogeneity will continue to increase.

Softwarization of networks and data analytics are key enablers for designing intelligent methods to orchestrate – i.e. configure in a synchronized and distributed manner – both network and system resources.

Intelligent orchestration leverages indeed data analytics for decision-making. Input data reflecting the past and current states of the system can be used to extract relevant knowledge including future states. To generate knowledge and validate orchestration decisions, a running system has to be monitored. Monitoring will also be steered and dynamically reconfigured through orchestration. Accordingly, the RESIST project is structured into three main complementary research axes detailed hereafter, namely **Monitoring**, **Analytics** and **Orchestration**.

### 3.2 Monitoring

The evolving nature of the Internet ecosystem and its continuous growth in size and heterogeneity call for a better understanding of its characteristics, limitations, and dynamics, both locally and globally so as to improve application and protocol design, detect and correct anomalous behaviors, and guarantee performance.

To face these scalability issues, **appropriate monitoring models, methods and algorithms are required for data collection, analysis and sharing** from which knowledge about Internet traffic and usage can be extracted. Measuring and collecting traces necessitate user-centered and data-driven paradigms to cover the wide scope of heterogeneous user activities and perceptions. In this perspective, we propose monitoring algorithms and architectures for large scale environments involving mobile and Internet of Things (IoT) devices.

RESIST also assesses **the impact of the Internet infrastructure evolution integrating network softwarization on monitoring**, for example the need for dedicated measurement methodologies. We take into account not only the technological specifics of such paradigms for their monitoring but also the ability to use them for collecting, storing and processing monitoring data in an accurate and cost-effective manner.

Crowd-sourcing and third-party involvement are gaining in popularity, paving the way for massively distributed and collaborative monitoring. We thus investigate opportunistic mobile crowdsensing in order to collect user activity logs along with contextual information (social, demographic, professional) to effectively measure end-users' **Quality of Experience**. However, collaborative monitoring raises serious concerns regarding trust and sensitive data sharing (open data). Data anonymization and sanitization need to be carefully addressed.

Finally, methodological aspects are also important for ensuring **trustworthy and reproducible experiments**, and raise many challenges regarding testbed design, experiment description and orchestration, along with automated or assisted provenance data collection.

### 3.3 Analytics

A large volume of data is processed as part of the operations and management of networked systems. These include traditional monitoring data generated by network components and components' configuration data, but also data generated by dedicated network and system probes.

**Understanding and predicting security incidents or system ability to scale** requires the elaboration of novel **data analytics techniques** capable to cope with large volumes of data generated from various sources, in various formats, possibly incomplete, non-fully described or even encrypted.

We use machine learning techniques (e.g. Topological Data Analysis or multilayer perceptrons) and leverage our domain knowledge to fine-tune them. For instance, machine learning on network data requires the definition of new distance metrics capable to capture the properties of network configurations, packets and flows similarly to edge detection in image processing. RESIST contributes to developing and making publicly available an **analytics framework dedicated to networked systems** to support Intelligence-Defined Networked Systems.

Specifically, the goal of the RESIST analytics framework is to facilitate the extraction of knowledge useful for **detecting, classifying or predicting security or scalability issues**. The extracted knowledge is then leveraged for orchestration purposes to achieve system elasticity and guarantee its resilience. Indeed, predicting when, where and how issues will occur is very helpful in deciding the provisioning of resources at the right time and place. Resource provisioning can be done either reactively to solve the issues or proactively to prepare the networked system for absorbing the incident (resiliency) in a timely manner thanks to its elasticity.

While the current trend is towards centralization where the collected data is exported to the cloud for processing, we seek to extend this model by also developing and evaluating novel approaches in which **data**

**analytics is seamlessly embedded within the monitored systems.** This combination of big data analytics with network softwarization enablers (SDN, NFV) can enhance the scalability of the monitoring and analytics infrastructure.

### 3.4 Orchestration

The ongoing transformations in the Internet ecosystem including network softwarization and cloudification bring new management challenges in terms of service and resource orchestration. Indeed, the growing sophistication of Internet applications and the complexity of services deployed to support them require novel models, architectures and algorithms for their automated **configuration** and **provisioning**. Network applications are more and more instantiated through the **composition of services, including virtualized hardware and software resources**, that are offered by **multiple providers** and are subject to changes and updates over time. In this dynamic context, efficient orchestration becomes fundamental for ensuring performance, resilience and security of such applications. We are investigating the chaining of different functions for supporting the security protection of smart devices, based on the networking behavior of their applications.

From a resilience viewpoint, this orchestration at the network level allows the dynamic **reconfiguration of resources** to absorb the effects of congestions, such as link-flooding behaviors. The goal is to drastically reduce the effects of these congestions by imposing dynamic policies on all traffic where the network will adapt itself until it reaches a stable state. We also explore mechanisms for **detecting and remediating potential dysfunctions** within a virtualized network. Corrective operations can be performed through dynamically composed VNFs (Virtualized Network Functions) based on available resources, their dependencies (horizontal and vertical), and target service constraints. We also conduct research on verification methods for automatically assessing and validating the composed chains.

From a security viewpoint, this orchestration provides **prevention mechanisms** that capture adversaries' intentions early and **enforces security policies** in advance through the available resources, to be able to proactively mitigate their attacks. We mainly rely on the results obtained in our research activity on security analytics to build such policies, and the orchestration part focuses on the required algorithms and methods for their automation.

## 4 Application domains

### 4.1 Internet

Among the different network types, the Internet is the one to link them all and is consequently our most prominent subject, not to mention its prime importance in today's society. The Internet also exhibits its own challenges due to the scale and diversity of stakeholders, applications and network technologies in use.

From a security perspective, **monitoring and analysing Internet traffic is an important part of threat prevention and predictive security**. Indeed, large network telescopes like the one we use in **the High Security Laboratory** allow detecting world-wide campaigns of attacks which target a specific exploit in some applications. Moreover the monitoring of the Internet traffic at the **edge** is the best way to quickly detect distributed attacks like DDoS (Distributed Denial of Service) and to mitigate them before they become effective. However, the Internet traffic analysis is made much more complicated since the **massive shift towards encryption** that happened few years ago, which requires new traffic classification methods.

The performance and resilience of services running over the Internet is also a major topic of RESIST. In particular, it is very difficult to **diagnose the cause of a degradation of performance among the different actors and technologies** that are used to deliver a service over the Internet (access medium, ISP, CDN, web-browser, etc.). Networked systems deployed at Internet scale are also a natural research subject for RESIST. Indeed **decentralized systems** like P2P (Peer-to-Peer) networks or blockchains are known to be robust and scalable. However, their security and performance have to be carefully assessed because a single flaw in their design can endanger the whole system.

## 4.2 SDN and Data-Center Networks

As the SDN paradigm and its implementations bring new opportunities that can be leveraged in different contexts, in particular for security and performance, programmable networks are also part of the research scope of RESIST. This includes data-plane **programming models and hardware offloading** that enable very flexible programming at the network level. While OpenFlow was initially designed for academic research, SDN in general has then been adopted by industrial players, above all in **data-center networks**. It supports innovations to better share load and optimize resources among processes, in particular for virtualization platforms. Contributing to the development of these technologies is primordial for us as they are key elements for monitoring and enhancing the performance and security of future data-center networks.

When defining or extending SDN technologies, the strongest constraint is to guarantee a satisfactory level of performance, *i.e.* enabling high flexibility in programming with a **reduced footprint of network throughput**. However, as it may also break isolation principles between multiple tenants, security has to be carefully considered, either by adding safeguard mechanisms at run-time or through a priori verification and testing.

## 4.3 Fog and Cloud computing

Cloud computing has largely evolved in the last years including new networking capabilities as highlighted in the previous section towards the model of XaaS or **everything-as-a-service**. Moreover, cloud computing continues to be more distributed and aims at integrating more heterogeneous resources. One particular example is **fog computing** that consists of a massively distributed number of different resources, including low-performance ones. Large network operators have a great interest in fog computing because they already operate such an infrastructure (e.g. a national operator with regional clouds and setup boxes in end users' homes). Softwarization or virtualization of all functions and services will help them to be competitive by reducing their costs. In general, intelligent orchestration of massively distributed resources will be investigated in various application domains, including **federated cloud infrastructures, fog computing, 5G networks, IoT and big data infrastructures**.

The manageability of such largely distributed systems is a core topic with questions related to monitoring, security and orchestration of resources. Major changes and errors can have dramatic effects on a real system. This slows down innovation and adoption of new propositions or features. Hence, **controlled and reproducible experiments are vital**.

As shown by our past work, we are able to quickly adjust to experimental needs in most areas of distributed computing and networking, such as *High Performance Computing (HPC)*, *Big Data*, *Peer-to-peer systems*, *Grid computing*, etc. However, in the context of RESIST, **we will focus mainly on *Software-Defined Infrastructures***, gathering *cloud computing* for compute and storage resources, *software-defined networking* and *network function virtualization* for networking. Those infrastructures share many common features: need for performance, for scalability, for resilience, all implemented using flexible software components.

We plan to integrate our experimental platforms developed within the PEPR programs—namely Cloud, Future Networks, and Cybersecurity—with the SLICES initiative, thereby contributing to a large-scale, federated experimental infrastructure for computer science research.

## 4.4 Cyber-Physical Systems

Cyber-Physical Systems (CPSs) used to be well isolated and so designed accordingly. In the last decade, they have become **integrated within larger systems** and so accessible through the Internet. This is the case with **industrial systems**, like SCADA, that have been unfortunately exposed to major threats. Furthermore, the **Internet-of-Things (IoT)** has become a reality with numerous protocols, platforms and devices being developed and used to support the growing deployment of smart\* services: smart home, transport, health, city... and even rather usual rigid systems such as industry 4.0.

From an academic perspective, the IoT can be seen as an evolution of sensor networks. It thus inherits from the same problems regarding security and scalability, but with a higher order of magnitude both in terms of number of devices and their capabilities, which can be exploited by attackers. Research in this area has focused on developing dedicated protocols or operating systems to guarantee security and performance, RESIST aims to tackle identical problems but **assuming a more practical deployment of IoT systems**

**composed of heterogeneous and uncontrolled devices.** Indeed, this ecosystem is very rich and **cannot be controlled by a unique entity**, e.g. services are often developed by third parties, manufacturers of embedded devices are different from those providing connectivity.

As a result, managing an IoT system (monitoring, changing configuration, etc.) is very hard to achieve as most of the devices or applications cannot be directly controlled. For instance, many IoT providers rely on their own cloud services, with their own unknown **proprietary protocols** and most of the time through **encrypted channels**. Above all, the use of middle-boxes like gateways hides the IoT end-devices and applications. We will thus need to infer knowledge from **indirect and partial observations**. Likewise, control will be also indirect for example through filtering or altering communications.

## 5 Highlights of the year

### 5.1 Awards

We received the best paper award of the French networking community conference (CORES 2025) for our pioneering work [16], which delivers the first-ever experimental evaluation of the Low Latency, Low Loss, and Scalable Throughput (L4S) architecture under real cloud gaming (CG) traffic conditions.

## 6 Latest software developments, platforms, open data

### 6.1 Latest software developments

#### 6.1.1 ROSCA

**Name:** Robust and Scalable Correlation of Alerts

**Keywords:** Alert correlation, Intrusion Detection Systems (IDS), Anomaly detection

**Functional Description:** ROSCA is a transparent solution that can handle a large volume of security alerts to reduce analyst fatigue, delayed responses, and missed attacks. It is suited for in-house adaptation or re-implementation by Security Operations Centers (SOCs). It is grounded in the MITRE ATT&CK kill chain model, and automatically aggregates and correlates alerts based on their shared attributes, enabling the construction of contextualised attack cases. Each case is assigned a score reflecting its threat level, before being presented to analysts within a prioritised queue. Our method handles multi-stage attack patterns and supports rapid processing through a robust, noise-tolerant scoring mechanism designed for interpretability and operational integration. We validate the effectiveness of ROSCA on real-world alert data and compare it against the MATE framework, demonstrating superior prioritisation accuracy and more reliable identification of critical alerts.

**URL:** <https://gitlab.inria.fr/resist/watch-rosca-alert-prioritisation/>

**Publication:** [hal-05351162](https://hal.archives-ouvertes.fr/hal-05351162)

**Contact:** Remi Garcia

**Participants:** Remi Garcia, Abdelkader Lahmadi, Pierre-Francois Gimenez, an anonymous participant

#### 6.1.2 llm-cvx

**Keywords:** LLM, Cyber attack

**Functional Description:** This repository provides an implementation of the LLM-CVX Benchmarking Framework to evaluate 14 LLMs (listed in data/llms.json ([https://gitlab.inria.fr/resist/llm-cvx/-/blob/main/data/llms.json?ref\\_type=heads](https://gitlab.inria.fr/resist/llm-cvx/-/blob/main/data/llms.json?ref_type=heads))) on exploiting 36 CVEs (listed in data/cves.json). The evaluation uses two exploit tools: Metasploit and GitHub PoCs, along with correction-loop prompting strategies, as detailed in the paper linked below.

**Publication:** [hal-05349650/](https://hal.archives-ouvertes.fr/hal-05349650/)

**Contact:** Mohamed Amine El Yagouby

### 6.1.3 C-CyberBattleSim

**Name:** Continuous CyberBattleSim

**Keywords:** Reinforcement learning, Cyber attack, Embedding model

**Scientific Description:** This repository builds upon the CyberBattleSim framework by introducing a modular, multi-stage pipeline with the following core components:

1. Automated Scenario Generation: Leverages Shodan and the National Vulnerability Database (NVD) data to extract real-world service distributions and vulnerabilities. It uses this data to generate diverse synthetic scenarios via domain randomization based on configurable parameters.
2. Game Reformulation: Models the attack environment as a Partially Observable Markov Decision Process (POMDP), allowing more realistic and effective learning.
3. Embedding Model Learning: Uses a Graph AutoEncoder and Language Models to embed graph and vulnerability information into latent continuous spaces.
4. Invariant Agent Architecture: Defines observation and action spaces that are independent of specific graph topologies or vulnerability sets by leveraging the previously described latent representations. This framework supports the training of Deep Reinforcement Learning (DRL) algorithms using Stable-Baselines3 implementations, and enables direct comparison with the global and local space formulations introduced in prior work.

**Functional Description:** Continuous CyberBattleSim (C-CyberBattleSim) is an advanced extension of Microsoft's CyberBattleSim, a simulation tool designed for training and evaluating reinforcement learning (RL) agents in cyber-attack path prediction. C-CyberBattleSim enhances the original tool in three directions: (1) it expands the scenario generation pipeline by leveraging Cyber Threat Intelligence collected from Shodan's empirical distributions to create synthetic network scenarios that closely reflect real-world conditions, (2) it introduces an automated process for simulating the outcomes of real-world vulnerabilities by inferring potential effects directly from their metadata, and (3) it integrates an embedding model that combines graph neural networks and language models to represent network nodes and vulnerabilities in continuous vector spaces. This approach introduces continuous observation and action spaces for RL agents, enabling more scalable and generalizable learning.

**News of the Year:** Simulation tool released with the publication "Scalable and Generalizable RL Agents for Attack Path Discovery via Continuous Invariant Spaces".

**URL:** <https://github.com/terranoafr/C-CyberBattleSim>

**Contact:** Franco Terranova

**Participants:** Abdelkader Lahmadi, Isabelle Chrisment, Franco Terranova

**Partners:** Université de Lorraine, Loria

## 6.2 New platforms

### Electrical Microgrid Security Assessment Platform

**Participants:** Abdelkader Lahmadi (*contact*), Aurélie Kpoze.

During 2025, we maintained our electrical microgrid platform and its control part with SDN-based communication network. The platform comprises Distributed Generators (DGs), Open vSwitches (OVSs) installed on Raspberry Pi devices, and a POX controller. The platform allows us to validate and evaluate methods of mitigating Man-in-the-Middle (MitM) attacks by demonstrating the effectiveness of SDN and reinforcement learning approaches in limiting their impact on the microgrid [17].

## Programable Networks Cluster

**Participants:** Jérôme François, Frédéric Beck (*contact*), Matthews Jose.

We develop the PNC (Programmable Networks Cluster) platform to deploy experimentation with fully isolated network slices under user-defined topologies for advanced systems and networking research. The platform allows researchers to describe a target topology and automatically instantiate it as a VXLAN-based slice, where virtual machines are interconnected through programmable hardware and software data paths. Depending on the experiment, the platform allows to pass through heterogeneous resources to the VMs, including programmable switches, SmartNICs with DPDK support, FPGA-based accelerators, GPUs, and OpenFlow-capable devices, enabling realistic in-network processing and high-performance traffic handling. This flexible architecture supports a wide range of use cases such as software-defined networking, programmable data planes, in-network computation, traffic engineering, large-scale traffic generation, and security experiments requiring strict isolation (e.g., malware or DDoS studies). By combining automation, hardware acceleration, and topology isolation, the PNC platform enables both functional validation and realistic performance evaluation of experimental networked systems. In 2025, we finalized the implementation of the different logical components of this platform, which is now entering a pre-production phase where the current release will be tested in real conditions over the 2026 year. The platform is developed in the scope of the PEPR Cybersecurity Superviz project.

## 6.3 Open data

### Datasets and models for generalizable RL agents for attack path discovery

**Contributors:** Franco Terranova; Abdelkader Lahmadi; Isabelle Chrisment

**Description:** This dataset contains all data used to produce the results presented in [23]. It was generated using the *C-CyberBattleSim* framework, an extension of Microsoft CyberBattleSim, and includes scraped vulnerability and service data (NVD, Shodan), generated network scenarios, configurations, and experimental results. The repository provides full training, testing, and hyperparameter optimization outputs for the Graph Autoencoder (GAE), reinforcement learning agents, and the multi-label vulnerability classifier used in the study, enabling full reproducibility.

**Dataset PID:** [10.5281/zenodo.15689667](https://zenodo.org/record/15689667)

**Project link:** [C-CyberBattleSim on Github](#)

**Publications:** [23]

**Contact:** Franco Terranova

**Release contributions:** Data scraping, scenario generation, configuration files, model checkpoints, training/testing results, and hyperparameter optimization logs.

## 7 New results

### 7.1 Monitoring

#### 7.1.1 Security of IPFS DHT

**Participants:** Thibault Cholez (*contact*), Victor De Moura Netto (*LORELEY Team*), Claudia Ignat (*LORELEY Team*).

The InterPlanetary File System (IPFS) is a decentralized peer-to-peer (P2P) storage that relies on Kademlia, a Distributed Hash Table (DHT) structure commonly used in P2P systems for its proved scalability. However, DHTs are known to be vulnerable to Sybil attacks, in which a single entity controls multiple malicious nodes. Recent studies have shown that IPFS is affected by a passive content eclipse attack, leveraging Sybils, in which adversarial nodes hide received indexed information from other peers, making the content appear unavailable. Fortunately, the latest mitigation strategy coupling an attack detection based on statistical tests and a wider publication strategy upon detection was able to circumvent it.

In 2025, we made a new active Sybil attack, with malicious nodes responding with semantically correct but intentionally false data, exploiting both an optimized placement of Sybils to stay below the detection threshold and an early trigger of the content discovery termination in Kubo, the main IPFS implementation. Our attack achieves to completely eclipse content on the latest Kubo release. When evaluated against the most recent known mitigation, it successfully denies access to the target content in approximately 80% of lookup attempts. To address this vulnerability, we propose a new mitigation called SR-DHT-Store, which enables efficient, Sybil-resistant content publication without relying on attack detection but instead on a systematic and precise use of region-based queries, defined by a dynamically computed XOR distance to the target ID. SR-DHT-Store can be combined with other defense mechanisms, resulting in a defense strategy that completely mitigates both passive and active Sybil attacks at a lower overhead, while allowing an incremental deployment [30].

### 7.1.2 Optimizing the Transport of Low-latency and High-bitrate Traffic

**Participants:** Thibault Cholez (*contact*), Olivier Festor, Mohammadreza Ghafari.

The rapid advancement of immersive multimedia applications necessitates network technologies that can deliver both low-latency and high-bitrate traffic to ensure a seamless Quality of Experience (QoE). Among those applications, Cloud Gaming (CG) platforms have gained much popularity recently and are expected to become a significant part of Internet traffic in the upcoming years. However, the characteristics of their traffic are challenging for networks to transport and make it difficult to maintain a good quality of service (QoS) in degraded network conditions when congestion occurs. New network architectures such as Low Latency, Low Loss, and Scalable Throughput (L4S) or Big Packet Protocol (BPP) offer new technical means to avoid bufferbloat-induced latency thanks to the network support, but have not yet been assessed on real high-bitrate and low-latency applications. In 2025, we pursued our dissemination work on the first evaluation ever made of L4S transporting real CG traffic. In particular, we received the best paper award of the French networking community conference (CORES 2025 [16]) and we gave an invited talk at the Internet Congestion Control Research Group (ICCRG) meeting of the IETF.

Then, we conducted a new study [14] to evaluate BPP's Packet Wash mechanism in conjunction with Scalable Video Coding (SVC) for real-time applications like CG. The packet wash mechanism can discard on-the-fly higher-quality payload layers in network buffers during congestion events, preventing gameplay interruptions without requiring server-side negotiation or re-encoding. This instantaneous network-based reaction minimizes the effects of congestion compared to traditional bitrate adaptation methods. Experimental results for 2K game streaming demonstrate that the packet wash mechanism preserves visual quality with negligible degradation during sudden bandwidth drops.

In a follow up study [15], we proposed to leverage Region Of Interest (ROI) based SVC combined with Packet Wash to further improve the Quality of Experience (QoE) under network congestion. Comparative experiments for various coding strategies after applying packet wash show that ROI SVC can handle bandwidth drops more efficiently, up to 52% bitrate reduction, while still maintaining uninterrupted gameplay and satisfactory visual quality in the most critical regions of the game, according our QoE evaluation involving real users. These results indicate that packet wash with ROI SVC provides an effective solution for real-time interactive multimedia streaming, such as cloud gaming.

### 7.1.3 AI driven Monitoring in Cloud-Edge-IoT continuum

**Participants:** Abdelkader Lahmadi (*contact*), Ahmad Atwi.

Monitoring large-scale systems such as the Cloud-Edge-IoT continuum is challenging due to their distributed, heterogeneous, and evolving nature. Tracking all components—from cloud servers to IoT devices—demands intensive probe deployment and frequent data collection, causing network traffic, computation, and storage overhead. These challenges are intensified by the lack of prior knowledge about which metrics matter most, often leading to redundant monitoring.

In [10], we explored whether Large Language Models (LLMs) can uncover causal relationships between monitoring metrics using only their textual descriptions. We proposed a novel batch prompting strategy that allows LLMs to reason over multiple variables simultaneously, reducing query complexity while preserving interpretability. Our evaluation across several instruction-tuned LLMs shows stronger inter-model alignment than existing pairwise methods and reveals overlaps with causal graphs from traditional numerical algorithms. These results suggest that LLMs can support intelligent monitoring by identifying influential metrics and minimizing redundancy.

## 7.2 Analytics

### 7.2.1 Efficient Distribution of Security Filtering Rules in SDN

**Participants:** Abdelkader Lahmadi (*contact*), Wafik Zahwa, Michael Rusinowitch (*PESTO team*).

Software Defined Networks (SDN) heavily rely on diverse management rules (ACL, traffic control, etc.) to satisfy security and business requirements of their associated services. As these networks are increasing in size and complexity, their management rules configured in devices are becoming more complex. These rules are constantly growing in size and it is challenging to distribute them across network devices with limited capacities. Typically implemented in switches using Ternary Content-Addressable Memory (TCAM), ACLs placement faces challenges due to the limited capacity of TCAM memory.

As communication networks and hosted services expand, the growing complexity and volume of policies require scalable algorithms for effective rule placement. In [24], we developed a novel approach that combines graph embedding neural networks (GNN) with deep Q-learning (DQN) to automate optimized ACL distribution across network switches. Our method efficiently manages TCAM utilization while integrating operational constraints (bandwidth, ordering) and it was extensively evaluated on both synthetic and real-world topologies. Results show that it outperforms heuristic and Integer Linear Programming (ILP) based techniques, offering superior scalability, adaptability, and robustness for ACL rule placement. This work was done in collaboration with Inria PESTO team and NUMERYX Company.

### 7.2.2 Characterization and Troubleshooting of Cloud Gaming Applications on Mobile Networks

**Participants:** Abdelkader Lahmadi (*contact*), Joël Ky.

Detecting abnormal network events is an important activity of Internet Service Providers particularly when running critical applications (e.g., ultra low-latency applications in mobile wireless networks). Abnormal events can stress the infrastructure and lead to severe degradation of user experience. Machine Learning (ML) models have demonstrated their relevance in many tasks including Anomaly Detection (AD) and Root Cause Diagnosis (RCD).

However they still rely on expert defined rules or supervised ML models that require extensive labeled datasets. This dependence on manual labeling makes them costly, time-consuming, and impractical for real-world wireless networks diagnostics. To overcome these limitations, we developed RAID (Root cause Anomaly Identification and Diagnosis) [19], a two-stage ML framework that diagnoses Wi-Fi performance

issues using time series KPIs collected directly from the Wi-Fi access point, with Cloud VR serving as a use case. RAID combines contrastive learning-based anomaly detection with a lightweight classifier to categorize network impairments. We evaluate RAID, with a real-world Cloud VR use case, in a testbed using NVIDIA CloudXR and a Meta Quest 2, collecting Wi-Fi performance metrics on the access point, under controlled conditions. Results demonstrate that RAID outperforms existing RCD methods, achieving high accuracy even with minimal labeled data. Compared to conventional supervised and self-supervised time series models, RAID offers a scalable, real-time solution with a good trade-off between training efficiency and inference speed, making it well-suited for practical deployment in dynamic Wi-Fi network environments. This work was done in collaboration with the University of Waterloo and Orange Innovation. The major results of this research activity are developed in the PhD of Joel KY defended in 2025 [25].

### 7.2.3 Mitigating Synchronization Attacks on Distributed and Cooperative Microgrid Control Systems

**Participants:** Abdelkader Lahmadi (*contact*), Satou Aurélie Kpoze, Isabelle Chrisment.

Industrial Control Systems (ICSs) are widely used in various industries, enabling the control and monitoring of critical infrastructures such as microgrids. In these infrastructures, distributed and cooperative control systems are commonly employed to synchronize set points through information exchange over communication networks. However, these systems are increasingly vulnerable to various security threats, particularly those targeting synchronization data.

A critical challenge in these systems is the control network reconfiguration in response to synchronization attacks targeting communication links. In [17], we developed a Deep Reinforcement Learning (DRL)-based reconfiguration approach that autonomously adjusts the control network among DGs, considering the microgrid's stability constraints. The main idea is to enhance synchronization in our microgrid by connecting synchronized nodes to unsynchronized ones. Our objective is to construct a minimum spanning tree (MST) that enables the distributed control system to exchange synchronization information efficiently and in a timely manner, while avoiding compromised links and minimizing disruption to microgrid stability after reconfiguration. Our experimental results demonstrate that the DRL-based strategy outperforms a traditional greedy algorithm by achieving a more optimal reconfiguration of the control network.

### 7.2.4 Cyber-Attack Paths Prediction

**Participants:** Abdelkader Lahmadi (*contact*), Franco Terranova, Isabelle Chrisment.

Attack paths represent the sequences of network nodes compromised by attackers while exploiting their respective vulnerabilities. Current methods for predicting such attack paths largely depend on existing human expertise or established heuristics. These traditional methods are time-consuming and require highly skilled threat-hunting analysts to identify these attack paths and proactively apply security measures. However, the task becomes challenging when facing large-scale and highly vulnerable networks. Recently, Reinforcement Learning (RL) has gained traction for training agents in identifying these critical paths. However, current solutions typically train RL agents tailored to a specific environment—defined by a fixed network structure and vulnerability set—requiring costly retraining whenever either changes. This limitation arises from optimizing the agent to map between discrete input and output spaces, treating network nodes and vulnerabilities as atomic discrete elements.

In [23], we developed a novel method for constructing continuous and invariant input and output spaces for RL agents, enabling them to learn transferable policies that generalize across diverse network configurations and vulnerability sets. We also released Continuous CyberBattleSim (C-CyberBattleSim) [32], an enhanced version of Microsoft CyberBattleSim designed to train agents with the novel continuous spaces. The tool is further extended to integrate real-world vulnerability data and a new scenario generation pipeline to improve the realism of training and testing environments. Agents trained in continuous spaces are assessed in 800 scenarios with varying sizes and various allocations of 829 real-world vulnerabilities, demonstrating an

average improvement of 9.3x in scalability against agents trained in discrete spaces, as well as an average generalization score of 89% to more complex scenarios when trained in simpler scenarios. A final study evaluates whether continuous agents trained in simulation can adapt to real-world and emulated scans. On average, agents achieve 75% of the score they would have if trained directly on the scans, demonstrating effective knowledge transfer.

### 7.2.5 Offensive and Defensive Cyber Security Capabilities of Large Language Models

**Participants:** Abdelkader Lahmadi (*contact*), Mohamed Amine El Yagouby, Olivier Festor.

The increasing capabilities of Large Language Models (LLMs) in code generation and reasoning have raised concerns about their potential misuse, particularly for automating or assisting with vulnerability exploitation tasks. This concern highlights the need for a systematic evaluation of the offensive potential of LLMs. Existing methodologies in this context use synthetic vulnerabilities, rely on fixed prompting strategies and exploit tools in their evaluation, and do not consider efficiency.

In [12], we developed LLM-CVX, a novel benchmarking framework designed to systematically evaluate LLMs on real-world CVE exploitation tasks, with extensibility towards prompting strategies and exploit tools, and allowing LLMs to make multiple attempts to capture both effectiveness and efficiency. We implemented this framework to evaluate 14 state-of-the-art LLMs on exploiting 36 real CVEs using 2 exploit tools (Metasploit and GitHub PoC) and a correction loop that enables LLMs to correct their previous exploitation attempts. In this evaluation, we used a novel set of metrics that we developed in [11], to better capture the efficiency of these models, in terms of successive attempts, when handling binary outcome tasks. Experimental results reveal variation in the behavior of different LLMs, using both exploitation tools, with closed-source models generally outperforming open-source ones.

### 7.2.6 Security Alerts Correlation and Prioritisation

**Participants:** Abdelkader Lahmadi (*contact*), Rémi Garcia, Pierre-François Gimezez (*PIRAT Team, Inria Rennes*).

In large organisations and complex infrastructures, the overwhelming volume of security alerts often results in analyst fatigue, delayed responses, and missed attacks. Security Operations Centers (SOCs) typically rely on black-box commercial solutions, offering limited transparency into their alert classification mechanisms and lacking the flexibility for in-house adaptation or re-implementation. To address these limitations and improve situational awareness, in [13] we developed ROSCA, an efficient alert prioritisation method grounded in the MITRE ATT&CK kill chain model. The proposed approach automatically aggregates and correlates alerts based on their shared attributes, enabling the construction of contextualised cases. Each case is assigned a score reflecting its threat level, before being presented to analysts within a prioritised queue. Our method handles multi-stage attack patterns and supports rapid processing through a robust, noise-tolerant scoring mechanism designed for interpretability and operational integration. We validate the effectiveness of ROSCA on real-world alert data and compare it against the MATE framework, demonstrating superior prioritisation accuracy and more reliable identification of critical alerts. This work was done in collaboration with Inria PIRAT team and the SOC of the Hospices Civils de Lyon.

### 7.2.7 Assessment of Network Intrusion Dataset

**Participants:** Jérôme François (*contact*), Omar Anser, Isabelle Chrisment.

This work defines an assessment of test set used for evaluating machine learning-based network intrusion detection. It introduces three metrics to capture the specificity of the test set space in regard to the train

set space. The objective is to check if the test points range in regions of the space that will challenge the intrusion detector. Our approach, namely TATA, is model-agnostic and we also propose an augmentation technique to improve the quality of the dataset. TATA employs a reinforcement learning (RL) approach guided by the three aforementioned metrics, configuring a testbed that produces realistic data [9].

## 7.3 Orchestration

### 7.3.1 Traffic Engineering for enhancing Quality of Service in 5G networks

**Participants:** Abdelkader Lahmadi (*contact*), Santiago Rios-Guiral, Ye-Qiong Song (*SIMBIOT Team*).

Programmable networks have transformed network management, particularly within Traffic Engineering (TE), which aims to optimize data flow across the network. By offering flexibility and efficiency, programmable networks facilitate advanced traffic and resource management capabilities. Key technologies in this area, such as Software-Defined Networking (SDN) and Programmable Data Planes (PDPs), enable real-time, dynamic routing and network control. These frameworks further allow the integration of Artificial Intelligence (AI) mechanisms to automate and refine network management processes. Specifically, Reinforcement Learning (RL) is a promising approach for TE applications due to its adaptability to evolving network conditions.

In [6], we elaborated a survey with an in-depth review of TE solutions that leverage RL and programmable networks to improve network performance, including works from 2018 to 2025. The proposed survey includes a timely update on the state-of-the-art and presents a taxonomy that categorizes existing solutions based on RL principles and specific TE objectives. Our analysis highlights key findings and insights, contributing valuable knowledge for implementing TE mechanisms within programmable networks. This work was done in collaboration with the University of Antioquia (Colombia).

In [22], we considered the case study of an autonomous urban transportation system (Urbanloop system) utilizing pod vehicles on dedicated rail circuits and requiring stable, high-performance, and continuous communication. We mainly analyzed how communication QoS impacts this system safety and performance. Using the simulators Veins-Simu5G, we evaluated the effects of packet loss and latency under various communication and mobility scenarios, and the related impacts on safety distance and pod deployment density. Furthermore, we validated our simulation findings through preliminary real-world testing with the OAIBOX platform, built upon the OpenAirInterface framework, confirming the practical relevance of our results for future deployments.

### 7.3.2 Security Configuration for Cloud Services

**Participants:** Rémi Badonnel (*contact*), Nicolas Schnepf, Olivier Festor.

Cloud infrastructures provide new facilities to build elaborated added-value services by composing and configuring a large variety of computing resources, from virtualized hardware devices to software products. They are however further exposed to security attacks than traditional environments. Preventing vulnerabilities is an important requirement to ensure the security of cloud infrastructures and their services, where distributed and dynamically evolving execution environments may significantly increase the attack surface. Effective vulnerability management in such ecosystems is therefore essential to maintain secure and dependable service execution.

We pursued our efforts on vulnerability management by considering the issues related to the edge-cloud continuum, through our collaboration with University of Milano (Italy). The edge-cloud continuum reshapes how we conceptualize and implement computing across diverse environments. This continuum represents a seamless integration of edge computing, which brings computational resources closer to data sources, with traditional cloud computing frameworks, enabling a more distributed, responsive, and efficient computing landscape. We proposed a novel methodology that systematically evaluates the vulnerabilities of potential deployment targets within the edge-cloud continuum. In this manner, it aims to identify the most appropriate

deployment options for each service request, taking into consideration the specific security requirements and non-functional properties specified by the user. Furthermore, our methodology provides a framework for managing the migration of services in response to invalidated requirements, ensuring that security and performance integrity of services is maintained throughout their life-cycle. We evaluated the proposed approach through realistic scenarios, demonstrating its effectiveness in enhancing cloud service security while reducing migration overhead. This approach therefore not only contributes to enhance the security of the edge-cloud continuum with respect to vulnerabilities, but also optimizes the alignment between service requirements and the capabilities of the deployment infrastructures [27].

We also started to investigate vulnerability prevention for moving target defense approaches that tend to leverage artificial intelligence to protect cloud services. In particular, we considered the design of a moving target defense strategy that combines artificial intelligence with verification techniques. The proposed framework relies on two main components, namely a learning block using reinforcement learning algorithms to automate movement selection based on rewards, and a verifier block using configuration verification techniques to assess these movements. We formalized this approach mathematically, aiming to make movements unpredictable for attackers, while minimizing the risk of vulnerable configurations. We conducted extensive experiments with a proof-of-concept prototype, comparing our approach to a baseline strategy and using vulnerability descriptions from the official OVAL repository. Results show that our strategy significantly reduces exposure to severe attacks with minimal assessment time overhead. Additionally, we evaluated the predictability of movements by attackers and the associated costs in terms of service unavailability [20].

### 7.3.3 Intelligent Configuration and Update for Future Networks

**Participants:** Nicolas Schnepf (*contact*), Katsuki Isobe, Rémi Badonnel.

Effective management of configuration and software updates on network and security equipments like firewalls and intrusion detection systems is a significant challenge in network operations and management, particularly when considering specific performance and security requirements like ensuring that the traffic will always traverse a certain network function. This challenge is increased by the dynamics and heterogeneity of future networks that are ever more driven by artificial intelligence methods and techniques.

In the context of the PhD thesis of Katsuki Isobe, we investigated the extension of the Eagle algorithmic solution to address the case of dynamic security chains in 5G/B5G networks [31]. These efforts were performed in collaboration with TU Berlin, Aalborg University and the Inria DIANA team. The objective is to support the dynamic update of service chaining and their inherent constraints. We specified an automated solution for synthesizing update schedules automatically and with the smallest possible number of update batches—an aspect important for decreasing the overall duration of the complete network update. It supports both vulnerability and congestion awareness. We added service chaining constraints specifying that network flows must traverse several services given as a directed graph deployed into the overall network. We provided two algorithms relying on this approach, the first one computing the shortest possible update sequence, the second one greedily computing each update batch as the largest possible set of remaining nodes to update. We compared these two approaches, and demonstrated their practical applicability in the context of 5G networks, as well as on a large benchmark of ISP Internet topologies combined with different service chaining. An extensive empirical evaluation shows that our approach is tractable and scales to realistic service chaining and network sizes [21].

In the meantime, we proposed a testbed architecture for evaluating the performance of LLMs to generate and enrich probabilistic automata characterizing the network behaviour of end device applications. These behavioural automata can then serve as a support to build and configure chains of security functions, that are deployed in network infrastructures. The testbed architecture consists of three main pipelines. The first pipeline specifies a baseline method based on process mining to generate behavioural automata. The second pipeline corresponds to the generation of automata based on LLM techniques. The third pipeline combines the two previous ones. It first generates automata using process mining, and then augments them using LLM techniques. Based on the prototyping of this testbed architecture, we have performed extensive series of experiments to evaluate the performances of LLM techniques with respect to the generation and enrichment of automata, and also to quantify their level of explainability in that context.

This work has been achieved in collaboration with Aristide Urli student at TELECOM Nancy, Université de Lorraine.

## 8 Bilateral contracts and grants with industry

### 8.1 Bilateral grants with industry

#### Numeryx Technologies (Paris, France)

**Participants:** Abdelkader Lahmadi (*contact*), Wafik Zahwa, Michael Rusinowitch (*PESTO team*).

- Wafik Zahwa, CIFRE PhD Student, is supervised by Abdelkader Lahmadi, Michael Rusinowitch (Inria PESTO team) and Mondher Ayadi (NUMERYX) on *Building Self-Driven Network Functions* [24]. Since October 2022.

#### Orange Innovation (Lannion, France)

**Participants:** Abdelkader Lahmadi (*contact*), Joël Ky.

- Joël Ky, CIFRE PhD Student, is supervised by Abdelkader Lahmadi, Raouf Boutaba (University of Waterloo) and Bertrand Mathieu (Orange Innovation) on *Automatic Characterization, Classification and Troubleshooting of Cloud Gaming Applications* [18, 19, 25]. PhD defended in April 2025.

#### Hospices Civils de Lyon, France)

**Participants:** Abdelkader Lahmadi (*contact*), Rémi Garcia, Isabelle Chrisment, Pierre-François Gimenez (*PIRAT team*).

- Rémi Garcia, Research Engineer, is supervised by Abdelkader Lahmadi, Isabelle Chrisment and Pierre-François Gimenez (Inria PIRAT Team, Rennes) on *False Positive Reduction in Intrusion Detection Systems for Hospital Environments* [13]. Since November 2024.

## 9 Partnerships and cooperations

### 9.1 International initiatives

#### 9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

NSSICS

**Title:** Network Softwarization for Secure Industrial Control Systems

**Duration:** 2024 to 2026

**Coordinator:** Jules Deliga (jules.degila@imsp-uac.org)

**Partners:** University of Abomey Calavi (Benin)

**Inria contact:** Abdelkader Lahmadi

**Summary:** In this associated team project with the University of Abomey Calavi (Benin), we are addressing the problems of securing industrial control systems using Machine Learning (ML) techniques and software-defined networking (SDN). The work focuses on the development of new techniques for detecting complex attacks, the automated generation of security policies and the orchestration of these policies for their effective deployment. These new techniques must also respect the operational constraints of these critical systems.

This collaboration led to the following publication: [17].

### 9.1.2 Inria associate team not involved in an IIL or an international program

#### DECEPTIA

**Title:** Deception Technologies for Honeypots with Intelligence and Adaptability

**Duration:** 2025 to 2027

**Coordinator:** Hans Dieter Schotten (schotten@dfki.uni-kl.de)

**Partners:** Inria RESIST and PIRAT research groups, Osaka Metropolitan University (OMU, Japan), University of Tokyo (UTokyo, Japan) and the German Research Center for Artificial Intelligence (DFKI Kaiserslautern, Germany)

**Inria contact:** Isabelle Chrismet

**Summary:** In this associate team, we address the global and local cybersecurity issues and define the following three research questions: (i) What are the characteristics of new anomalous traffic observed in large-scale honeypots deployed across multiple geolocations and services? (ii) How can we make honeypots adapt on-the-fly to the attacker's behavior and also evolve interaction between them? (iii) How can we develop an effective phishing detection system that not only accurately identifies phishing attacks, but also educates and explains the risks to end-users in a way that increases their awareness and resilience to future phishing attempts? To solve these research questions, we deploy honeypots related to various locations (e.g., Japan, France and Germany) and various services (e.g., research institutes, cloud, home, edge), and conduct experiments and analysis of anomalous traffic.

This collaboration led to the following publication: [8].

### 9.1.3 Visits of international scientists

#### Sora Nakagawa

**Status** PhD Student

**Institution of origin:** Osaka Metropolitan University

**Country:** Japan

**Dates:** from September 17 to November 16

**Context of the visit:** we worked on latency assurance for mobile devices in edge networks.

**Mobility program/type of mobility:** research stay

#### Filip Katulic

**Status** Researcher

**Institution of origin:** University of Zagreb

**Country:** Croatia

**Dates:** from November 17 to November 22

**Context of the visit:** we worked on exploiting generative artificial intelligence for supporting cyber-range platforms.

**Mobility program/type of mobility:** research stay

**Ivan Kovacevic**

**Status** Researcher

**Institution of origin:** University of Zagreb

**Country:** Croatia

**Dates:** from November 17 to November 22

**Context of the visit:** we worked on exploiting generative artificial intelligence for supporting cyber-range platforms.

**Mobility program/type of mobility:** research stay

**Dora Pavelic**

**Status** PhD Student

**Institution of origin:** University of Zagreb

**Country:** Croatia

**Dates:** from November 17 to November 22

**Context of the visit:** we worked on exploiting generative artificial intelligence for supporting cyber-range platforms.

**Mobility program/type of mobility:** research stay

#### 9.1.4 Visits to international teams

##### Research stays abroad

**Franco Terranova**

**Visited institution:** Universitat Politècnica de Catalunya (UPC)

**Country:** Spain

**Dates:** October 2025 to March 2026

**Context of the visit:** Franco Terranova, PhD student, has been awarded a LUE-DrEAM mobility grant from the University of Lorraine. Within this framework, he is conducting a research visit with the research team of Prof. Albert Cabellos-Aparicio at the Universitat Politècnica de Catalunya (UPC). During this stay, Franco is closely collaborating with Prof. Cabellos-Aparicio in the context of his PhD research, with a particular focus on the generalization of Reinforcement Learning techniques for networking tasks.

**Mobility program/type of mobility:** research stay

## 9.2 National initiatives

### 9.2.1 ANR

#### ANR COMMITS

**Participants:** Abdelkader Lahmadi (*contact*).

**Title:** COnverged coMMunication, control and scheduling Infrastructure for multi pods-based Transport Systems

**Coordinator:** Université de Lorraine (Abdelkader Lahmadi)

**Duration:** 2024 to 2028

**Partners:** Urbanloop SME, CNAM, CRAN

**Local contact:** Abdelkader Lahmadi

**Summary:** The main goal of the project is to develop a converged communication, control and scheduling infrastructure to build a cyber-physical system for managing the **Urbanloop** transport network at a large scale. The main challenge is to control the entire transport network while respecting safety, security and timing constraints. COMMITS will develop its own control and scheduling system as well as the low-latency communication architecture on which the system relies in order to automate an on-demand and rail-based transport system.

The RESIST team is coordinating this project and is mainly involved in the development and the evaluation of the management of the communication system based on 5G to guarantee the scalability, the security and the QoS of the Urbanloop transport network when deployed with thousands of capsules. Our contributions in this project are published in [22, 6].

### 9.2.2 PEPR

#### PEPR CyberSecurity / SuperviZ

**Participants:** Abdelkader Lahmadi (*contact*), Jérôme François, Frédéric Beck (*SED*).

**Acronym:** SuperviZ

**Title:** Supervision and orchestration of cybersecurity

**Coordinator:** Inria (Ludovic Mé)- Télécom SudParis (Hervé Debar)

**Duration:** 2022 to 2028

**Partners:** CentraleSupélec, EURECOM, Institut Mines-Télécom, Institut Polytechnique de Grenoble, Université de Rennes 1, Université de Lorraine, CEA, CNRS

**Local contact:** Abdelkader Lahmadi

**Summary:** SuperviZ is one of the projects of PEPR on cybersecurity under the axis *security of systems* and under the domain *security of systems, networks and software* [28]. It aims at improving methods in detection, response and mitigation of cyber attacks. Because it is impossible to ensure that a system is 100% secure, supervision of security aims at improving preventive techniques and mitigate the threats when those techniques failed to provide a sufficient level of security. This project considers the following challenges: increase of the volume and heterogeneity of devices to be managed, complexity of the interconnection of different systems grouped into large-scale critical infrastructure (system

of systems), sophistication of attacks becoming more and more stealthy, massive attacks targeting a significant number of devices within a short-term attack campaign.

The RESIST team is involved in the following topics of research: reinforcement learning for automated risk assessment, robust and explainable automated machine learning pipeline, automated mitigation of cyber-threats, generalization of behavioral detection techniques, creation of a SDN-capable platform for network experiment. Our contributions in this project are published in [23, 9].

#### PEPR Future Networks / NF-HiSec

**Participants:** Isabelle Chrisment (*contact*), Rémi Badonnel, Nicolas Schnepf.

**Title:** End-to-end security for the network of the future

**Coordinator:** IMT (Hervé Debar)

**Duration:** 2023 to 2027

**Partners:** IMT, CEA, INRIA, LORIA, CNRS

**Local contact:** Isabelle Chrisment, Rémi Badonnel

**Summary:** The NF-HiSec project designs new methods and tools to secure the networks of the future. More specifically it covers five major objectives. The first objective concerns the protection of these networks, through the specification and deployment of end-to-end security policies. The second objective aims to detect and manage attacks in these complex environments. The third objective focuses on the protection of personal data in the case of lawful interception. The fourth objective aims to model the operation of the security mechanisms of these networks, so as to ensure that the security services provided correspond to the needs of the applications which request them. The fifth objective is to formalize the link between hardware and software layers on the one hand, and security properties, to ensure the integration of cyber mechanisms in all layers of the network.

The RESIST team is working on automating and formally verifying the building and off-loading of chains of security functions at the edge level in the context of networks of the future. Our contributions in this project are published in [21] and [31].

#### PEPR Future Networks / NF-NAI

**Participants:** Thibault Cholez (*contact*), Olivier Festor.

**Title:** Networks Architecture and Infrastructure and Networks, Cloud, and Sensing Convergence

**Coordinator:** IMT (Jean-Louis Rougier)

**Duration:** 2023 to 2027

**Partners:** IMT, CEA, Eurecom, INRIA, CNRS

**Local contact:** Thibault Cholez, Olivier Festor

**Summary:** Beyond traditional objectives, including advances in throughput, execution speed, latency, or object connection density, the outcomes of the NF-NAI project will enable the effective integration of multiple new technologies, including technologies for the physical layer (e.g. reconfigurable intelligent surfaces), transition to 3D systems (e.g. NTN – non-terrestrial networks) and architectural principles (e.g. slicing and dynamic end-to-end orchestration). The project will facilitate the emergence of new applications and services by reaching the objective of transparency – towards uses – in terms of

performance, robustness and security. The project will also design interfaces offering a rich level of capabilities and personalization to the service plane and to application developers, over the whole chain, from connected mini-objects to large data centres through multi-access edge computing (MEC).

The RESIST team is interested in improving network support for low-latency high-bitrate applications by proposing either new Active Queue Management algorithms working in conjunction with Congestion Control Algorithms, or by improving scheduling decisions of the base station to better take into account the QoS requirements of new immersive multimedia applications [14, 15].

#### PEPR Cloud / TRUSTINCloudS

**Participants:** Isabelle Chrisment (*contact*), Rémi Badonnel (*contact*), Thibault Cholez (*contact*), Nicolas Schnepf, Olivier Festor.

**Title:** Cybersecurity of cloud infrastructures

**Coordinator:** CEA (Aymen Boudguiga & Antoine Choffrut)

**Duration:** 2023 to 2030

**Partners:** AMU, IMT, UL, EURECOM, UT3, CEA, INRIA

**Local contact:** Isabelle Chrisment, Rémi Badonnel, Thibault Cholez

**Summary:** The TRUSTINCloudS project will design solutions for the major cybersecurity challenges specific to Cloud environments. The work carried out in this project aims at adapting traditional security mechanisms (e.g. PEPR Cyber) to the characteristics of the Cloud in order to address the specific threats of the different types of Clouds (IaaS, PaaS,...). The main objective of TRUSTINCloudS is to study and develop new methodologies to strengthen Cloud security and implement them in platforms in order to build a sovereign and trusted Cloud. It must also raise awareness of the possibilities and limitations of these methodologies. The project is organized in such a way as to work on the one hand on the security of the infrastructures, and on the other hand on the security of the data (in the broad sense) that these infrastructures host. When relevant, prototypes will be implemented within the shared infrastructure provided by the SILECS project of the PEPR Cloud.

The RESIST team is investigating two different topics. The first is related to the security management of cloud infrastructures, in link with the activities developed in the SPIREC project (see paragraph 9.2.2 below) also part of the PEPR Cloud. The second axis is done in collaboration with the Inria LORELEY team and aims to improve the security and performance of fully distributed P2P systems relying on a DHT, from which the InterPlanetary File System (IPFS) is a modern representative.

Our contributions in this project are published in [27] and [20].

#### PEPR Cloud / SPIREC

**Participants:** Isabelle Chrisment (*contact*), Abdelkader Lahmadi (*contact*).

**Title:** Multi-level supervision and prediction for geo-distributed, heterogeneous infrastructures in the Cloud/Edge/IoT continuum

**Coordinator:** IMT (Mario Südholt)

**Duration:** 2023 to 2030

**Partners:** IMT, CEA, CNRS, INRIA, UVSQ, UL

**Local contact:** Isabelle Chrisment, Abdelkader Lahmadi

**Summary:** The Cloud-Edge-IoT continuum (CEI) is characterized by highly heterogeneous infrastructures as well as applications and services that are built using different multi-layer software stacks. The monitoring of infrastructures and applications, anomaly detection of service and application executions as well as the prediction of resources usage are fundamental services for the management of the CEI, just like for the Cloud. The SPIREC project will meet the challenges of supervising services of the continuum, detecting their execution anomalies and predicting their resource usage. The project aims to define methods and techniques, notably using distributed machine learning, to enable its efficient management, provide means to secure them and, more generally, ensure a variety of quality of service properties. The partners will also develop software components and tools in order to integrate these functionalities in existing infrastructures and applications, in particular SLICES, industrial systems and future software ecosystems.

The RESIST team is planning to investigate methods and techniques for monitoring hardware and software resources in Cloud/Fog/IoT infrastructures. The team is also interested in studying AI-based approaches to improve multi-level anomaly detection and to facilitate the placement of supervision probes and the analysis of large volumes of logs.

Our contributions in this project are published in [10].

### 9.2.3 Inria joint Labs

#### Inria-Orange Joint Lab

**Participants:** Jérôme François (*contact*), Olivier Festor, Matthews Jose, Abdelkader Lahmadi, Joël Roman Ky, Raouf Boutaba, Nicolas Schnepf.

**Title:** Inria - Orange Joint Laboratory

**Duration:** 2015 to 2025

**Summary:** The challenges addressed by the Inria-Orange joint laboratory relate to the massively distributed infrastructure and fog/edge computing virtualization. In particular the management of these infrastructures with the use of AI-based techniques and the lifecycle of deployed applications will be considered including different perspectives: performance, energy, security... The work carried in the PhD of Joël Roman Ky [18, 19, 25] has contributed to this joint lab.

## 9.3 Regional initiatives

### AMI CMA: CyMoVE project

**Participants:** Abdelkader Lahmadi (*contact*), Ye-Qiong (*SIMBIOT team*), Marine Minier (*CARAMBA team*).

**Title:** CYMOVE: Develop training modules, innovative approaches, and promote careers for the mobility of tomorrow

**Coordinator:** Université de Haute Alsace (UHA)

**Duration:** 2025 to 2029

**Partners:** UHA, Communauté de communes de Mulhouse (M2A), Pôle Véhicule du Futur (PVF), Chambre des Métiers d'Alsace (CMA), Numéum, Lycée Loritz de Nancy, Lycée Gustave Eiffel de Talange, Holo3, Université de Lorraine, Université de Reims Champagne Ardenne (URCA)

**Local contact:** Abdelkader Lahmadi

**Summary:** The automotive industry is facing major challenges due to societal, regulatory, and technological changes. The 2021 Climate and Resilience law mandates a transition to electric vehicles by 2035. The increasing connectivity of vehicles heightens cybersecurity challenges, with risks of cyberattacks targeting embedded systems and networks. Companies must also contend with a shortage of skilled labor and the need to modernize production. Recent studies and reports recommend tailored training programs at various levels to address these challenges. CyMoVe offers progressive, modular, and complementary training programs covering all levels and learning modalities, ranging from awareness to technical expertise, from Bac -3 to Bac +5. These programs include cybersecurity, energy management, and electric vehicle maintenance, providing a holistic approach to addressing vulnerabilities. In the Grand Est region, the project aims to train learners at the relevant levels using the modules developed within the CyMoVe project.

RESIST team is involved in developing lightweight security approaches for embedded networking protocols in connected cars including intrusion detection techniques and the benchmarking of lightweight cryptography in collaboration with Inria CARAMBA team.

## 10 Dissemination

**Participants:** Rémi Badonnel, Thibault Cholez, Isabelle Chrisment, Olivier Festor, Abdelkader Lahmadi, Jérôme François, Nicolas Schnepf, Omar Anser, Franco Terranova, Mohamed Amine El Yagouby, Jhon Sebastian Rojas Rodriguez.

### 10.1 Promoting scientific activities

#### 10.1.1 Scientific events: organisation

##### Member of the organizing committees

- Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), travel grant co-chair, IEEE/IFIP Network Operations and Management Symposium (NOMS 2026), travel grant co-chair.
- Olivier Festor: IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), Distinguished Experts Panels Co-Chair.

#### 10.1.2 Scientific events: selection

##### Member of the conference program committees

- Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP International Conference on Network and Service Management (CNSM 2025), IEEE Global Communications Conference (Globecom 2025), Cyber Security in Networking Conference (CSNet 2025), IEEE International Workshop on Education, Training and Awareness in Cybersecurity (ETACS 2025), IEEE/IFIP Network Operations and Management Symposium (NOMS 2026), Experience Track of IEEE/IFIP Network Operations and Management Symposium (NOMS 2026).
- Thibault Cholez: Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2025), IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP Network Operations and Management Symposium (NOMS 2026), IEEE Conference on Network Softwarization (NetSoft 2025), IEEE International Workshop on Distributed In-Network Computing Technologies (D-Netcomp 2025).
- Isabelle Chrisment: IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2025), International Workshop on Traffic Measurements for Cybersecurity (WTMC 2025).

- Abdelkader Lahmadi: IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP International Conference on Network and Service Management (CNSM 2025), IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2025), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2025), IEEE Global Communications Conference (Globecom 2025), IEEE Conference on Standards for Communications (CSCN 2025).

### 10.1.3 Journal

#### Member of the editorial boards

- Rémi Badonnel: Editor-in-Chief for Springer Journal of Network and System Management (JNSM) since January 2023, Associate Editor for IEEE Transactions on Network and Service Management (TNSM), Associate Editor for IEEE Transactions on Cloud Computing, Associate Editor for Wiley International Journal of Network Management (IJNM).
- Thibault Cholez: Associate Editor for Springer Journal of Network and System Management (JNSM).
- Abdelkader Lahmadi: Associate Editor for IEEE Transactions on Network and Service Management (TNSM).

#### Reviewer - reviewing activities

- Rémi Badonnel: IEEE Transactions on Network and Service Management (TNSM), IEEE Transactions on Cloud Computing (TCC), Springer Journal of Network and System Management (JNSM), Wiley International Journal of Network Management (IJNM).
- Thibault Cholez: IEEE Transactions on Network and Service Management (TNSM), ACM Transactions on Internet Technology, Springer Journal of Network and System Management (JNSM).
- Abdelkader Lahmadi: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM), IEEE Transactions on Information Forensics and Security, IEEE/ACM Transactions on Networking (ToN), IEEE Transactions on Mobile Computing, ACM Transactions on Privacy and Security, IEEE Vehicular Technology Magazine, IEEE Transactions on Big Data, ACM Computing Surveys, IEEE Transactions on Artificial Intelligence.

### 10.1.4 Invited talks

- Thibault Cholez
  - Talk on "Improving Cloud Gaming traffic QoS: a comparison between class-based queuing policy and L4S" in The Internet Congestion Control Research Group (ICCRG), Internet Engineering Task Force (IETF) 122, March 2025
- Abdelkader Lahmadi
  - Talk on "Security Monitoring and Policy Enforcement in Networked Systems" in RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2025
  - Talk on "Artificial Intelligence for Cyber Security: from LLM-Powered Offensive Capabilities to AI-Driven Attack Path Prediction" in the conference CESAR 2025 by DGA, Rennes in November 2025
  - Talk on "Cybersecurity Research and Innovation" during the inauguration event of the regional Cyber Security Hub, Metz in October 2025
- Remi Badonnel
  - Talk on "Cybersecurity for the Future World" in the Association for the Advancement of Management Event, March 2025

- Talk on "Cybersecurity and Networking" in the Rendez-Vous Informatique of the Programme National de Formation (PNF), April 2025
- Talk on "Cybersecurity Skills and Training Programs" in the Thales Cyber Luxembourg Event, June 2025
- Omar Anser and Franco Terranova delivered a hands-on tutorial on "Meta-Learning for Reinforcement Learning: Enabling Agents to Generalize to Unseen Scenarios" at the: [25th European Agent Systems Summer School \(EASSS 2025\)](#)

### 10.1.5 Leadership within the scientific community

- Rémi Badonnel is chair of the IFIP (International Federation for Information Processing) WG6.6 (Working Group 6.6) dedicated to the management of networks and distributed systems, and is member of the SSLR Working Group (Security of Systems, Software and Networks) of the CNRS GDR on Cybersecurity.
- Olivier Festor is member of the NISC Board. NISC stands for NOMS IM steering committee. The board coordinates the organization, management and evolution of the major conferences in the Network and Service Management scientific community and interacts with the associated Scientific and Professional organizations.

### 10.1.6 Scientific expertise

- Isabelle Chrisment is the regional scientific coordinator for the Alliage project in the context of the CPER Grand-Est (2021-2027). She served as a member of the evaluation committee for the ASTRID 2025 call for proposals launched by the French National Research Agency (ANR) and the Defense Innovation Agency (AID).
- Abdelkader Lahmadi served as a member of the ANR committee CE39 (sécurité globale, résilience et gestion de crise, cybersécurité) in 2025. He served as an expert for the European Research Executive Agency (REA) in the call HORIZON-JU-SNS-2025-01.
- Rémi Badonnel is, together with Marine Minier, in charge of the coordination of research, teaching and innovation activities on cybersecurity at the University of Lorraine.

### 10.1.7 Research administration

- Isabelle Chrisment was Deputy Scientific Director at Inria in charge of the national scientific domain "Networks, Systems and Services, Distributed Computing" until June 2025. Since July 1, 2025, she is the Director of the Inria Center at Université de Lorraine and the Inria Branch in Strasbourg.
- Abdelkader Lahmadi is the responsible of the research department "Networks, Systems and Services" at LORIA since October 2025.
- Rémi Badonnel is a member of the COMIPERS at Inria Nancy Grand Est, and of the Commission de la Mention Informatique (CMI) at University of Lorraine.

## 10.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

### 10.2.1 Teaching

#### Teaching responsibilities

- Rémi Badonnel is heading the Internet Systems and Security specialization of the 2<sup>nd</sup> and 3<sup>rd</sup> years at the TELECOM Nancy engineering school, and is responsible for the pedagogical coordination of the cybersecurity platform of this school (including two professional cyber-ranges). He is also in charge of the pedagogical coordination of a new training curriculum on cybersecurity by apprenticeship (one year as a student, two years as apprentice), which has been recently accredited by the CTI.

- Thibault Cholez is in charge of the diplomas in apprenticeship at TELECOM Nancy engineering school.
- Olivier Festor is the Director of *Lorraine INP* which groups all eleven engineering schools of University of Lorraine and one undergraduate programme (classe préparatoire aux grandes écoles).
- Abdelkader Lahmadi was heading the Engineering of Digital Systems (ISN) degree at ENSEM engineering school until June 2025.

### Teaching courses

- Thierry Arrabal : 105 hours - L3 - Linux system, algorithmics, Web development and data base, Cybersecurity - TELECOM Nancy, Université de Lorraine
- Rémi Badonnel: 242 hours - L3, M1, M2 - Networks, Systems and Services, Software Design and Programming, Cloud Computing, Network and Cybersecurity Management - TELECOM Nancy, Université de Lorraine
- Thibault Cholez: 250 hours - L3, M1, M2 - Computer Networks, Network Services Administration, Mobile applications and Internet of Things, Git, Linux Commands and Tools - TELECOM Nancy, Université de Lorraine
- Olivier Festor: 192 hours - L3, M1, M2 - Advanced algorithmics and problem solving, Advanced data structures, Competitive programming, Databases and data management, Assembly language, Network security, network management, Software testing Devops and SCRUM, Project Management - TELECOM Nancy, Université de Lorraine
- Jérôme François: 70 hours - M1, M2 - Network security, network management, big data - TELECOM Nancy, Université de Lorraine
- Abdelkader Lahmadi: 280 hours - BUT1, L3, M1, M2 - Sensor Networks, Distributed Systems and Algorithms, Algorithms and Advanced Programming, Security of Cyber Physical Systems - ENSEM Engineering School, Université de Lorraine and IUT Nancy-Charlemagne, Université de Lorraine

### E-learning

- MOOC *Supervision de Réseaux et Services*, FUN Project, Université de Lorraine, Ingénieur, formation initiale et continue, Thibault Cholez, Rémi Badonnel, Laurent Andrey, Olivier Festor, Abdelkader Lahmadi, Jérôme François. The content of the MOOC has been opened to other academic curricula through the FUN CAMPUS platform. Two local sessions have also been organized in 2025 at TELECOM Nancy for students and apprentices.
- MOOC *Sécurité des Réseaux Informatiques (Session 5)*, FUN Project, led by IMT (SudParis and Saint Étienne), with contributions from Inria and Université of Lorraine. In addition to the national session (from October to November 2025), one local session has been organized in 2025 at TELECOM Nancy for students.
- MOOC *Becoming a Cybersecurity Consultant*, Concordia Project, Rémi Badonnel, Thibault Cholez and Lama Sleem. The course contents were on open access on the Coursera MOOC platform in 2025.

### 10.2.2 Supervision

#### PhD in progress

- Omar Anser, *Automation of Attack Mitigations in 5G Environments*, since December 2021, supervised by Isabelle Chrisment and Jérôme François.
- Franco Terranova, *Reinforcement Learning-Based Approaches for Automated Security Analysis of Networked Systems*, since October 2023, supervised by Isabelle Chrisment and Abdelkader Lahmadi.

- Mohamed Amine El Yagouby, *Modeling and Detection of AI-Assisted Cyberattacks*, since November 2024, supervised by Olivier Festor and Abdelkader Lahmadi, in joint supervision with the University International of Rabat (Morocco).
- Ahmad Atwi, *Adaptive and Optimal Placement of Monitoring Probes Based on Reinforcement Learning*, since December 2025, supervised by Abdelkader Lahmadi.
- Santiago Rios, *Models and Algorithms for the Orchestration System of an On-Demand Rail Transport Network*, since March 2025, supervised by Abdelkader Lahmadi and Ye-Qiong Song (SIMBIOT)
- Jhon Sebastian Rojas Rodriguez, *Reinforcement Learning for Anomaly Detection and Root Cause Analysis in the Computing Continuum*, since November 2024, supervised by Abdelkader Lahmadi.
- Wafik Zahwa, *Construction of network functions based on machine learning*, since Octobre 2022, supervised by Michael Rusinowitch and Abdelkader Lahmadi.
- Katsuki Isobe, *Security Orchestration at the Edge for Future Networks*, since October 2024 (pre-thesis from June to September 2024), supervised by Rémi Badonnel and Nicolas Schnepf.
- Gaelle Yonga, *Moving-target Defense Driven by Artificial Intelligence for Cloud Composite Services*, since December 2025, supervised by Rémi Badonnel and Thierry Arrabal.
- Victor Henrique De Moura Netto, *Improving security and performance of IPFS's DHT*, supervised by Thibault Cholez and Claudiat Ignat (LORELEY).
- Mohammadreza Ghafari, *Improving network support for low-latency high-bitrate applications*, supervised by Thibault Cholez and Olivier Festor.

#### Defended PhD

- Enzo d'Andréa, *Reusable and Adaptable Machine Learning for Network Security*, defended on 1st December 2025, supervised by Olivier festor and Jérôme François.
- Joël Roman Ky, *Anomaly Detection and Root Cause Diagnosis for Low-Latency Applications in Time-Varying Capacity Networks*, defended on 29th April 2025, supervised by Isabelle Chrisment, Raouf Boutaba (University of Waterloo, Canada), Abdelkader Lahmadi, Bertrand Mathieu (Orange Inovation, France).

#### 10.2.3 Juries

Team members participated in the following PhD defense committees:

- Marius Letourneau, PhD in Computer Science from Université de Technologie de Troyes en Sciences pour l'Ingénieur. Title: *Impacts et détectabilité des menaces ciblant les services réseaux basse latence: le cas de l'architecture L4S*, July 2025 - (Abdelkader Lahmadi as reviewer and Isabelle Chrisment as examiner).
- Nischal Aryal, PhD in Computer Science from Institut Polytechnique de Paris (Telecom SudParis). Title: *Blockchain-based Collaboration framework for B5G and 6G Cellular Networks*, September 2025 - (Abdelkader Lahmadi as reviewer).
- Sara Chennoufi, PhD in Computer Science from Institut Polytechnique de Paris (Telecom SudParis). Title: *Privacy-Preserving and Robust Attack-Knowledge Sharing in Heterogeneous 5G Networks via Federated Prototype-Based Intrusion Detection*, December 2025 - (Abdelkader Lahmadi as reviewer).
- Hélène Orsini, PhD in Computer Science from CentraleSupélec (France). Title: *Weakly-Supervised Learning for Botnet Traffic Analysis and Adversarial Robustness Assessment*, March 2025 - (Isabelle Chrisment as reviewer).
- Fatemeh Stodt, PhD in Computer Science from Université de Strasbourg (France). Title: *Building a Secure and Scalable Distributed Network using Blockchain and Zero Trust for IIoT*, July 2025 - (Isabelle Chrisment as president).

- Ildi Alla, PhD in Computer Science from Université de Lille (France). Title: *Monitoring for Detection and Localization of Cyber Attacks in Wireless Networks*, September 2025 - (Isabelle Chrisment as examiner).
- Ruslan Bondaruc, PhD in Computer Science from University of Milan (Italy). Title: *An Assurance-Driven Service Composition for Data-Intensive Pipelines in Cloud-Edge Continuum*, November 2025 - (Thibault Cholez as reviewer).
- Walid Megherbi, PhD in Computer Science from Lyon University (France). Title: *Anomaly Detection in Graph Streams*, April 2025 - (Rémi Badonnel as reviewer).
- Yangjie Xu, PhD in Computer Science from Luxembourg University (Luxembourg). Title: *Quantum Machine Learning: Diverse perspectives on Application Scenarios*, April 2025 - (Rémi Badonnel as reviewer).
- Tan Nhat Linh Le, PhD in Computer Science from Paris Saclay University (France). Title: *A Novel AI-based Intrusion Detection System for 3GPP 5G-IoT traffic*, December 2025 - (Rémi Badonnel as examiner).
- Grace Tessa Masse, PhD in Computer Science from Avignon University (France). Title: *Cyberdeception and Resilience in Federated Learning Systems*, December 2025 - (Rémi Badonnel as reviewer).
- Rachid Guedjali, PhD in Computer Science from University of Lorraine (France). Title: *Dynamics of validator selection and behavior in byzantine fault tolerant blockchain systems*, December 2025 - (Rémi Badonnel as president).

Team members participated in the following Habilitation Degree committees:

- Daphné Tuncer, HDR in Computer Science from Conservatoire National des Arts et Métiers (France). Title: *On the Complexity of Managing Communication and Information System Infrastructures*, May 2025 - (Isabelle Chrisment as reviewer and Olivier Festor as examiner).
- Mališa Vučinić, HDR in Computer Science from Université PSL (France). Title: *Lightweight Solutions for a Secure Internet of Things*, October 2025 - (Isabelle Chrisment as reviewer).

#### 10.2.4 Specific official responsibilities in science outreach structures

- Rémi Badonnel coordinated in 2025 the organization of two Capture The Flag events on cybersecurity which took place at TELECOM Nancy, the Engineering school of Computer Science of University of Lorraine, which targets Bachelor-level and Master-level students in Cybersecurity, with the objective of finding the maximum number of vulnerabilities on a specific system hosted over a cyber-range platform.
- Rémi Badonnel coordinated in 2025 the local organization of REMPLAR 2025 at TELECOM Nancy. REMPLAR is the largest national cyber crisis management exercise managed by ANSSI (the French National Cybersecurity Agency). This exercise mobilized a total of 5000 professionals from nearly 1000 organizations at the national level, including private companies, local authorities, prefectures, and regional Computer Security Incident Response Teams (CSIRTs).
- Rémi Badonnel participated to the organization of the Cyber Humanum Est event, which corresponds to a 5-days cyber wargame exercise dedicated to cyber crisis management, bringing together more than 100 participants, and organized under the aegis of the Cyber Defense Command (COMCYBER) of the Ministry of Armed Forces, and of Lorraine INP, the Collegium of Engineering Schools of the University of Lorraine.

#### 10.2.5 Participation in Live events

This year Franco Terranova, Mohamed Amine El Yagouby and Jhon Sebastian Rojas Rodriguez, three RESISTTeam PhD students participated to the national day "Fête de la Science" (Science in Fest): *Quand l'IA anticipe les hackers (When IA anticipates hackers)*

## 11 Scientific production

### 11.1 Major publications

- [1] P. Graff, X. Marchal, T. Cholez, B. Mathieu, S. Tuffin and O. Festor. ‘Improving Cloud Gaming traffic QoS: a comparison between class-based queuing policy and L4S’. In: *2024 8th Network Traffic Measurement and Analysis Conference (TMA)*. Network Traffic Measurement and Analysis Conference (TMA 2024). Dresden, Germany: IEEE, 22nd May 2024, p. 10. DOI: [10.23919/TMA62044.2024.10558920](https://doi.org/10.23919/TMA62044.2024.10558920). URL: <https://inria.hal.science/hal-04594817>.
- [2] M. Jose, K. Lazri, J. François and O. Festor. ‘Stateful InREC: Stateful In-network REal Number Computation with Recursive Functions’. In: *IEEE Transactions on Network and Service Management* (10th Aug. 2022), pp. 1–1. DOI: [10.1109/TNSM.2022.3198008](https://doi.org/10.1109/TNSM.2022.3198008). URL: <https://inria.hal.science/hal-03794876>.
- [3] A. Laraba, J. François, S. Rahman Chowdhury, I. Chrisment and R. Boutaba. ‘Mitigating TCP Protocol Misuse With Programmable Data Planes’. In: *IEEE Transactions on Network and Service Management* 18.1 (Mar. 2021), pp. 760–774. DOI: [10.1109/TNSM.2021.3054528](https://doi.org/10.1109/TNSM.2021.3054528). URL: <https://inria.hal.science/hal-03480222>.
- [4] N. Schnepf, R. Badonnel, A. Lahmadi and S. Merz. ‘Automated Orchestration of Security Chains Driven by Process Learning’. In: *Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning*. Wiley, 12th Oct. 2021. DOI: [10.1002/9781119675525.ch12](https://doi.org/10.1002/9781119675525.ch12). URL: <https://inria.hal.science/hal-03518390>.
- [5] F. Terranova, A. Lahmadi and I. Chrisment. ‘Leveraging Deep Reinforcement Learning for Cyber-Attack Paths Prediction: Formulation, Generalization, and Evaluation’. In: *The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024)*. Padua, Italy, 30th Sept. 2024, pp. 1–16. DOI: [10.1145/3678890.3678902](https://doi.org/10.1145/3678890.3678902). URL: <https://hal.science/hal-04662428>.

### 11.2 Publications of the year

#### International journals

- [6] S. Ríos-Guiral, A. Lahmadi, J. F. Botero and S. A. Gutiérrez. ‘Leveraging Reinforcement Learning for Traffic Engineering in Programmable Networks: A Survey’. In: *Communications Surveys and Tutorials, IEEE Communications Society* (2025), pp. 1–1. DOI: [10.1109/comst.2025.3632870](https://doi.org/10.1109/comst.2025.3632870). URL: <https://inria.hal.science/hal-05398965> (cit. on pp. 18, 23).

#### Invited conferences

- [7] F. Terranova, S. Rekbi, A. Lahmadi and I. Chrisment. ‘Multi-Taxonomy Vulnerability Classification with Hierarchically Finetuned Language Models’. In: *DIMVA 2026 - Conference on Detection of Intrusions and Malware and Vulnerability Assessment*. Chania, Crete, Greece, 1st July 2026. URL: <https://hal.science/hal-05500820>.

#### International peer-reviewed conferences

- [8] T. Angeli, F. Beck, D. Kondo, I. Chrisment, H. Tode and H. Schotten. ‘Demo: SweetsPot: A Distributed HoneyPot Federation Platform’. In: *Local Computer Networks (LCN)*. Sydney, Australia, 14th Oct. 2025. URL: <https://inria.hal.science/hal-05381945> (cit. on p. 21).
- [9] O. Anser, J. François, I. Chrisment and D. Kondo. ‘TATA: Benchmark NIDS Test Sets Assessment and Targeted Augmentation’. In: *ESORICS 2025 - 30th European Symposium on Research in Computer Security*. Toulouse, France, 22nd Sept. 2025. URL: <https://hal.science/hal-05148383> (cit. on pp. 18, 24).
- [10] A. Atwi and A. Lahmadi. ‘LLM-Driven Causal Discovery for Monitoring Metrics in Computing Continuum Systems: A Comparative Study’. In: *LCN 2025 - IEEE 50th Conference on Local Computer Networks*. Sydney, Australia: IEEE, 14th Oct. 2025, pp. 1–8. DOI: [10.1109/LCN65610.2025.11146314](https://doi.org/10.1109/LCN65610.2025.11146314). URL: <https://hal.science/hal-05343924> (cit. on pp. 15, 26).

- [11] M. A. El Yagoubi, A. Lahmadi, M. Zakroum, O. Festor and M. Ghogho. ‘Evaluating LLMs Efficiency Using Successive Attempts on Binary-Outcome Tasks’. In: *Actes de CORIA-TALN-RJCRI-RECITAL 2025. Actes de l’atelier Évaluation des modèles génératifs (LLM) et challenge 2025 (EvalLLM)*. CORIA-TALN-RJCRI-RECITAL 2025. Marseille, France, 30th June 2025, pp. 120–126. URL: <https://hal.science/hal-05213688> (cit. on p. 17).
- [12] M. A. El Yagoubi, A. Lahmadi, M. Zakroum, O. Festor and M. Ghogho. ‘LLM-CVX: A Benchmarking Framework for Assessing the Offensive Potential of LLMs in Exploiting CVEs’. In: *AISeC 2025 - 18 th ACM Workshop on Artificial Intelligence and Security*. Taipei, Taiwan, 13th Oct. 2025. DOI: [10.1145/3733799.3762978](https://doi.org/10.1145/3733799.3762978). URL: <https://inria.hal.science/hal-05349650> (cit. on p. 17).
- [13] R. Garcia, A. Lahmadi, P.-F. Gimenez and C. Sala. ‘ROSCA: Robust and Scalable Security Alert Correlation and Prioritisation using the MITRE ATT&CK Framework’. In: *WATCH 2025 - First International Workshop on Analytics, Telemetry, and Cybersecurity for HPCC (High Performance Computing and Communications)*. Taipei, Taiwan, 2025. DOI: [10.1145/3733826.3762680](https://doi.org/10.1145/3733826.3762680). URL: <https://inria.hal.science/hal-05351162> (cit. on pp. 17, 20).
- [14] M. Ghafari, T. Cholez and O. Festor. ‘Evaluation of Packet Wash for Low-Latency High-Bitrate Game Streaming’. In: *EMS 2025 - 3rd Workshop on Emerging Multimedia Systems*. Coimbra, Portugal: ACM, 8th Sept. 2025, pp. 7–12. DOI: [10.1145/3746441.3748228](https://doi.org/10.1145/3746441.3748228). URL: <https://inria.hal.science/hal-05375897> (cit. on pp. 14, 25).
- [15] M. Ghafari, T. Cholez and O. Festor. ‘QoE Evaluation of BPP Packet Wash Using ROI-based Scalable Video Coding’. In: *ISM 2025 - 27th IEEE International Symposium on Multimedia*. Naples, Italy: IEEE, 8th Dec. 2025, pp. 1–8. URL: <https://inria.hal.science/hal-05424680> (cit. on pp. 14, 25).
- [16] P. Graff, X. Marchal, T. Cholez, S. Tuffin, B. Mathieu and O. Festor. ‘Amélioration de la QoS du trafic de Cloud-Gaming : une comparaison entre HTB et LAS’. In: *CORES 2025 - 10èmes Rencontres Francophones sur la Conception de Protocoles, l’Évaluation de Performances et l’Expérimentation des Réseaux de Communication*. CORES 2025 - 10èmes Rencontres Francophones sur la Conception de Protocoles, l’Évaluation de Performances et l’Expérimentation des Réseaux de Communication. Saint Valery-sur-Somme, France, 2nd June 2025. URL: <https://hal.science/hal-05031655> (cit. on pp. 11, 14).
- [17] A. Kpoze, A. Lahmadi, M. Ma, I. Chrisment, J. Degila and A. Ahouandjinou. ‘Reconfiguration of Distributed Cooperative Microgrid Control Systems via Deep Reinforcement Learning to Mitigate Synchronization Attacks’. In: *SmartGridComm 2025 - IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*. 2025 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). North York, Canada: IEEE, 21st Oct. 2025, pp. 1–7. DOI: [10.1109/SmartGridComm65349.2025.11204592](https://doi.org/10.1109/SmartGridComm65349.2025.11204592). URL: <https://hal.science/hal-05349594> (cit. on pp. 12, 16, 21).
- [18] J. R. Ky, B. Mathieu, A. Lahmadi and R. Boutaba. ‘CATS: Contrastive learning for Anomaly detection in Time Series’. In: *2024 IEEE International Conference on Big Data (Big Data)*. Washington DC, United States: IEEE, 16th Jan. 2025. DOI: [10.1109/BigData62323.2024.10825476](https://doi.org/10.1109/BigData62323.2024.10825476). URL: <https://hal.science/hal-04881349> (cit. on pp. 20, 26).
- [19] J. R. Ky, B. Mathieu, A. Lahmadi, M. Wang, N. Marrot and R. Boutaba. ‘RAID: Root cause Anomaly Identification and Diagnosis’. In: *ECML PKDD 2025 - European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases*. Vol. 16020. Lecture Notes in Computer Science. Porto (Portugal), Portugal: Springer Berlin Heidelberg, 4th Oct. 2026, pp. 438–455. DOI: [10.1007/978-3-662-72243-5\\_25](https://doi.org/10.1007/978-3-662-72243-5_25). URL: <https://hal.science/hal-05219367> (cit. on pp. 15, 20, 26).
- [20] M. Oulaaffart, R. Badonnel, N. Schnepf and C. Bianco. ‘Enhancing Artificial Intelligence with Verification Techniques to Support Automated Moving Target Defense in Cloud Composite Services’. In: *2025 IEEE 11th International Conference on Network Softwarization (NetSoft)*. Budapest, France: IEEE, 23rd June 2025. DOI: [10.1109/NetSoft64993.2025.11080533](https://doi.org/10.1109/NetSoft64993.2025.11080533). URL: <https://hal.science/hal-05185090> (cit. on pp. 19, 25).

- [21] N. Schnepf, R. Badonnel, D. Saucez, S. Schmid and J. Srba. ‘Eagle: Vulnerability and Congestion Aware Software Update Synthesis in Softwarized Networks with a 5G Network Case Study’. In: *IEEE Xplore. NOMS 2025 - IEEE Network Operations and Management Symposium. NOMS 2025-2025 IEEE Network Operations and Management Symposium*. Hawaii, United States: IEEE, 12th May 2025, pp. 1–9. DOI: [10.1109/NOMS57970.2025.11073658](https://doi.org/10.1109/NOMS57970.2025.11073658). URL: <https://hal.science/hal-05185079> (cit. on pp. 19, 24).
- [22] R. Su, A. Lahmadi, Y.-Q. Song and J.-P. Mangeot. ‘Assessing 5G Connectivity for Urbanloop: a Pod-based Autonomous Railway Transport System’. In: *2025 IEEE 102nd Vehicular Technology Conference*. Chengdu, China, 2025. URL: <https://hal.science/hal-05157729> (cit. on pp. 18, 23).
- [23] F. Terranova, A. Lahmadi and I. Chrisment. ‘Scalable and Generalizable RL Agents for Attack Path Discovery via Continuous Invariant Spaces’. In: *2025 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*. Gold Coast, Australia, 19th Oct. 2025, pp. 440–457. DOI: [10.1109/RAID67961.2025.00029](https://doi.org/10.1109/RAID67961.2025.00029). URL: <https://hal.science/hal-05182437> (cit. on pp. 13, 16, 24).
- [24] W. Zahwa, A. Lahmadi, M. Rusinowitch and M. Ayadi. ‘Deep Reinforcement Learning for In-Network Placement of ACL Rules Under Constraints’. In: *IEEE Explore. CNSM 2025 - 21st International Conference on Network and Service Management*. Bologne, Italy, 27th Oct. 2025. URL: <https://inria.hal.science/hal-05327868> (cit. on pp. 15, 20).

#### Doctoral dissertations and habilitation theses

- [25] J. R. Ky. ‘Anomaly Detection and Root Cause Diagnosis for Low-Latency Applications in Time-Varying Capacity Networks’. Université de Lorraine, 29th Apr. 2025. URL: <https://theses.hal.science/tel-05077121> (cit. on pp. 16, 20, 26).
- [26] A. Lahmadi. ‘Contributions to the Monitoring and Security of Networked Systems’. Université de Lorraine (UL), 4th Mar. 2025. URL: <https://hal.univ-lorraine.fr/tel-04984019>.

#### Reports & preprints

- [27] R. Bondaruc, N. Schnepf, R. Badonnel, C. A. Ardagna and M. Anisetti. *Towards Secure Service Deployment in Cloud-Edge Continuum*. 22nd Jan. 2025. URL: <https://inria.hal.science/hal-04907033> (cit. on pp. 19, 25).
- [28] H. Debar, L. Mé, J. Leneutre, V. Nicomette, J. François, C. Gouy-Pailler, G. Blanc and S. Mocanu. *Superviz project mid-term progress report*. Télécom SudParis (Institut Mines-Télécom); Inria, Oct. 2025. URL: <https://hal.science/hal-05444442> (cit. on p. 23).
- [29] H. Debar, L. Mé, J. Leneutre, V. Nicomette, J. François, C. Gouy-Pailler, G. Blanc and S. Mocanu. *SuperviZ supervision et orchestration de la sécurité Rapport d’avancement à mi-projet*. Télécom SudParis (Institut Mines-Télécom); Inria, Oct. 2025, pp. 1–56. URL: <https://hal.science/hal-05315778>.
- [30] V. H. de Moura Netto, T. Cholez and C.-L. Ignat. *Active Sybil Attack and Efficient Defense Strategy in IPFS DHT*. 2nd May 2025. URL: <https://inria.hal.science/hal-05424411> (cit. on p. 14).
- [31] N. Schnepf, R. Badonnel, D. Saucez, J. Sbara and S. Schmid. *Towards Vulnerability and Congestion Aware Software Update Synthesis for Softwarized Networks*. 22nd Jan. 2025. URL: <https://inria.hal.science/hal-04906917> (cit. on pp. 19, 24).

**Software**

- [32] [SW] F. Terranova, A. Lahmadi and I. Chrisment, *Continuous CyberBattleSim* version 1.0.0, 15th July 2025. LIC: <https://spdx.org/licenses/MIT>. HAL: [hal-05194047](https://hal.inria.fr/hal-05194047), URL: <https://inria.hal.science/hal-05194047>, VCS: <https://github.com/terranoafr/C-CyberBattleSim>, SWHID: [swh:1:dir:0b32c22ea0771c26604e38728ab090df6469c4aa;origin=https://github.com/terranoafr/C-CyberBattleSim;visit=swh:1:snp:bc5aa14f7d947bec6111c51264e58ec506eedac;anchor=swh:1:rev:7374c32b6711bb0e9b6d5fcd94d4eacc034c07cb](https://sw.hub.com/terranoafr/C-CyberBattleSim;visit=swh:1:snp:bc5aa14f7d947bec6111c51264e58ec506eedac;anchor=swh:1:rev:7374c32b6711bb0e9b6d5fcd94d4eacc034c07cb) (cit. on p. 16).