ERASMUS+ PROJECT

Deliverable 2.1

Survey of the EU best practices, framework and strategic documentation on 5G and beyond network security

Abstract. This document presents a comprehensive survey of the European Union's best practices, frameworks, and strategic documentation related to the security of 5G and beyond networks. It analyzes key initiatives, policies, and study programmes developed to address the complex cybersecurity challenges posed by advanced network architectures. The survey highlights cutting-edge practices in areas such as 5G network security, AI in cybersecurity, quantum cryptography and regulatory compliance. By examining EU-funded projects, industry standards, and research outputs, the document provides actionable insights and recommendations for developing novel learning courses for enhancing the resilience and security of next-generation communication networks.

Funded from the European Union's Erasmus+ Capacity Building in the field of Higher Education Programme under Grant Agreement No 101179818

Document properties

Document number	D2.1
Document title	Survey of the EU best practices, framework and strategic documentation on 5G and beyond network security
Document responsible	Rui Luis Aguiar (UoA)
Document editor	Roman Odarchenko (KAI), Maksim Iavich (CU)
Editorial team	Maryna Yevdokymenko (NURE), Emil Faure (ChDTU)
Target dissemination level	PU
Status of the document	Published
Version	1.0

Document history

Revision	Date	Issued by	Description
0.1	November 15, 2024	UoA	Initial ToC
0.2	November 22, 2024	KAI	Updated ToC, section 1
0.3	November 29, 2024	CU	Updated ToC, section 2
0.4	December 6, 2024	KAI, NURE	Update of sections 1, 2
0.5	December 8, 2024	ChSTU	Section 3, section 4
0.6	December 24, 2024	CU	Ready for review
0.7	December 26, 2024	UoA	Reviewed
0.8	December 27, 2024	KAI	Reviewed
0.9	December 28, 2024	CU, KAI	Updated after review
1.0	December 30, 2024	UoA, KAI, CU	Final version

Disclaimer

Executive Summary

This document provides a detailed survey of the European Union's best practices, frameworks, and strategic documentation regarding the security of 5G and beyond networks. With the rapid adoption of 5G technologies and the impending transition to 6G, ensuring the security and resilience of digital infrastructure has become paramount. The survey covers EU-funded R&D projects, regulatory analyses, academic study programs, and cutting-edge research laboratories.

Key findings include:

- the EU's strategic approach to 5G and 6G development, emphasizing innovation and regulatory alignment;
- the role of quantum technologies and AI/ML in shaping the security landscape for advanced networks;
- insights from prominent EU R&D projects and their contributions to securing 5G infrastructures;
- existing academic programs and laboratory setups that address 5G security challenges.

The document concludes with actionable recommendations for leveraging EU insights to enhance the security, scalability, and innovation of 5G and beyond networks globally.

List of authors

Company	Name	Contribution
UoA	Rui Luis Aguiar, Vitor Cunha	Introduction, Conclusions, Executive Summary
KAI	Roman Odarchenko, Alla Pinchuk	Introduction, Conclusions, Executive Summary, Section 1, Section 3.2, Section 4.1
CU	Maksim Iavich, Sergei Simonovi	Introduction, Section 2, Section 3.3, Section 4.2
ATSU	David Gegechkori	Section 2
BSU	Lela Turmanidze	Section 2
NURE	Maryna Yevdokymenko, Oleksandr Lemeshko, Oleksandra Yeremenko	Section 3.1, Section 4.3
ChSTU	Artem Lavdanskyi, Emil Faure	Section 4.2

Table of Contents

DOCUMENT PROPERTIES 2
DOCUMENT HISTORY 2
DISCLAIMER 2
EXECUTIVE SUMMARY 3
LIST OF AUTHORS 4
TABLE OF CONTENTS 5
INTRODUCTION 6
1. EU R&D PROJECTS 7
2. EU REGULATIONS ANALYSIS 15
2.1. THE EUROPEAN UNION'S APPROACH TO 5G: A STRATEGIC VISION FOR DIGITAL TRANSFORMATION 15
2.2. THE EMERGING LANDSCAPE OF 6G: THE EUROPEAN UNION'S PROSPECTIVE REGULATORY FRAMEWORK 16
2.3. QUANTUM TECHNOLOGIES IN THE EUROPEAN UNION: A COMPREHENSIVE EXPLORATION OF INNOVATION AND REGULATION 17
2.4. EU AI ACT: FIRST REGULATION ON ARTIFICIAL INTELLIGENCE 18
2.5. SUMMARY OF NIST IR 8547: TRANSITION TO POST-QUANTUM CRYPTOGRAPHY STANDARDS 20
REFERENCES 22
3. EXISTING STUDY PROGRAMMES AND COURSES ANALYSIS 23
3.1. AI/ML TECHNOLOGIES FOR SECURITY OF 5G AND BEYOND NETWORKS 23
3.2. CYBERSECURITY IN 5G AND BEYOND 34
3.3. POST-QUANTUM AND QUANTUM CRYPTOGRAPHY 45
3.4. DEVSECOPS 49
4. R&D LABORATORIES 54
4.1. 5G SECURITY LABORATORIES 54
4.2. QUANTUM R&D LABS 57
4.3. AI/ML R&D LAB 62
CONCLUSIONS 65

Introduction

The advent of 5G and the research into 6G technologies represent significant milestones in global digital transformation. These advanced network architectures promise unprecedented connectivity, speed, and reliability, enabling applications ranging from smart cities to autonomous systems. However, their complexity also introduces new vulnerabilities and security challenges. Addressing these challenges requires robust frameworks, innovative research, and collaborative regulatory efforts.

This document explores the European Union's approach to securing 5G and beyond networks through:

- analysis of EU-funded R&D projects that contribute to network security innovations;
- examination of EU regulations and strategic initiatives, including AI/ML applications, quantum technologies, and post-quantum cryptography;
- review of academic programs and study courses designed to train professionals in 5G security;
- overview of R&D laboratories at the forefront of 5G and beyond security.

The insights presented aim to serve as a resource for developing the new educational courses, adopting EU best practices in 5G and beyond security.

1. EU R&D projects

The following analysis is designed to support the SECURE project by identifying transferable insights, methodologies, and frameworks from EU-funded cybersecurity projects. By understanding how these projects addressed challenges similar to those SECURE aims to tackle, we can leverage proven strategies, avoid redundant efforts, and accelerate the creation of Research and Education Hubs (R&EHubs) in Georgia and Ukraine. This approach ensures the alignment of SECURE's objectives with established best practices in the field of cybersecurity, ultimately fostering a resilient and collaborative ecosystem.

Table 1 – EU R&D projects analysis

Project Title	Project Link	Years	Project Overview	Consortium
CyberSec4Europe	https://cybersec4europe.eu/	2019-2022	A flagship initiative to develop a pan-European cybersecurity framework addressing research, training, and operational needs. The project emphasizes collaboration between academia, industry, and public institutions to create a resilient digital ecosystem.	Fraunhofer, Thales, KU Leuven, and others
SPARTA	https://www.sparta.eu/	2019-2022	Focuses on specialized programs to tackle pressing cybersecurity challenges through research and innovation. SPARTA integrates multidisciplinary expertise to address security gaps in critical sectors like healthcare, finance, and transportation.	CEA, INRIA, Airbus, and other leading partners
ECHO	https://echonetwork.eu/	2019-2022	Builds a federated network of cybersecurity centers to advance EU capabilities in managing emerging threats. ECHO emphasizes cross-sectoral collaboration, fostering innovation, and enhancing operational security practices.	NATO CCDCOE, NTNU, Atos, and more

FORESIGHT	https://foresight-h2020.eu/	2019-2022	Develops advanced simulation platforms to enhance cybersecurity training for aviation, naval, and power grid environments. The project incorporates AI-driven tools and real-world scenarios to prepare professionals for complex cyber threats.	Sheffield Hallam University, University of Peloponnese, Minds & Sparks GmbH
THREAT-ARREST	https://www.threat-arrest.eu/	2019-2021	Offers a comprehensive virtualized training environment to simulate and counteract sophisticated cyberattacks. It targets organizations in critical domains such as energy, healthcare, and shipping.	Sphynx Technology Solutions AG, University of Brighton, and others
GEIGER	https://project.cyber-geiger.eu/	2020-2023	Aims to boost cybersecurity resilience among SMEs by providing tailored risk assessment tools, training resources, and an interactive cybersecurity knowledge hub.	FHNW, IBM Research, COGITANDA, and others
PROTECTIVE	https://protective-h2020.eu/	2017-2020	Develops tools for real-time situational awareness and threat intelligence sharing, enabling CSIRTs and SMEs to improve their cybersecurity posture. The project focuses on proactive prevention and response to cyber threats.	Irish Telecom, University of Patras, CESNET
CYBER-MAR	https://www.cyber-mar.eu/	2019-2023	Focuses on maritime cybersecurity by creating innovative tools and simulation platforms for safeguarding critical maritime operations against cyber threats.	CERTH, DANAOS, Lloyd's Register, and others
CONCORDIA	https://www.concordia-h2020.eu/	2019-2023	Aims to establish a European cybersecurity competence network by fostering cooperation among academia, industry, and public authorities to develop sustainable cybersecurity strategies.	LMU Munich, University of Twente, and others

GUARD	guard-project.eu	2019-2022	Introduces an IoT-specific cybersecurity framework to detect, respond to, and mitigate threats in dynamic environments. The project integrates blockchain technology for enhanced transparency and trust.	VTT, Engineering Ingegneria Informatica, and others
FutureTPM	**futuretpm.eu**	2018-2021	Explores quantum-resistant cryptographic algorithms for secure TPM implementations, addressing emerging threats in the quantum era.	University of Surrey, Infineon Technologies, and others
CyberSec4SMEs	https://cybersec4europe.eu/	2019-2022	Focuses on equipping SMEs with tailored cybersecurity solutions, including cost-effective tools, training programs, and collaborative networks to enhance resilience.	Research institutes and SME associations
SAFECARE	https://www.safe-care.org/	2018-2021	Secures healthcare systems by integrating advanced cybersecurity measures for physical and digital infrastructure, ensuring patient safety and data integrity.	Philips Healthcare, INRIA, and other partners
CYBER-TRUST	Official Website	2019-2022	Provides innovative solutions for IoT security using blockchain and advanced authentication mechanisms to mitigate risks in connected environments.	University of Piraeus, Hyperion Systems Engineering, and others
InterConnect	Official Website	2019-2022	Promotes cybersecurity in energy management systems, focusing on smart grids and IoT-enabled devices to ensure secure data exchange.	Energy and cybersecurity organizations
CERTCOOP	https://www.certcoop.gr/	2016-2019	Enhances collaboration among EU CERTs to address cross-border cybersecurity challenges through shared knowledge and tools.	CERT teams across the EU

CyberSecWomen	https://www.wicys.org/	2020-2023	Promotes gender diversity in cybersecurity by offering specialized training, mentorship programs, and career support for women in the field.	Academic institutions and diversity advocacy groups
CYRAIL	https://cyrail.eu/	2016-2019	Addresses cybersecurity challenges in railway systems by developing comprehensive security frameworks for transportation networks.	Transport security experts
SANCUS	https://sancus-project.eu/	2020-2023	Employs AI to enhance supply chain cybersecurity, focusing on anomaly detection, threat mitigation, and operational continuity.	AI and cybersecurity research groups
AI4Cyber	https://ai4cyber.eu/	2020-2023	Investigates the application of artificial intelligence in cybersecurity, aiming to automate threat detection and response for enhanced defense capabilities.	AI and cybersecurity consortia
Cybersecurity Education Initiative	https://cysed.org/	2020-2023	Facilitates cybersecurity awareness in educational institutions, equipping students and educators with the necessary skills to navigate digital risks.	Schools and university networks
CyberSecAcademy	https://www.cybersecurity-academy.com/	2020-2023	Develops standardized cybersecurity curricula for universities across Europe, promoting harmonized education and training.	Academic and professional training organizations
IoTAC	https://iotac.eu/	2020-2023	Enhances the security of IoT devices by employing advanced encryption, anomaly detection, and system hardening techniques.	IoT and cybersecurity firms
COLIBRI	https://illicitflows.eu/projects/colibri/	2020-2023	Focuses on improving cybersecurity in connected and autonomous vehicles through innovative security mechanisms.	Automotive and cybersecurity researchers

CYBER-AWARE	https://becyberaware.eu/	2019-2022	Enhances cybersecurity awareness in local governments, providing tailored solutions for improving digital resilience.	Government agencies and academic institutions
REWIRE	https://rewireproject.eu/	2020-2023	Provides re-skilling opportunities for professionals to enter the cybersecurity field, addressing workforce shortages in the sector.	Vocational training organizations
CyberSecResilience	https://www.impetus-project.eu/	2020-2023	Develops educational programs and tools to improve societal resilience against cyber threats, focusing on training and public awareness.	Public-private partnerships
Digital Awareness Network	https://www.digitalawarenessuk.com/	2020-2023	Builds networks to promote cybersecurity awareness in workplaces and schools, fostering a culture of proactive digital safety.	SMEs, schools, and training networks
HECTOR	https://www.hector-project.com/	2020-2023	Enhances cybersecurity in smart grids and critical infrastructure by developing advanced monitoring and threat detection systems.	Energy and cybersecurity organizations

Each of the above projects deserves attention and clearly makes a significant contribution to the development of highly qualified human potential. Table 2 summarizes the results of the analysis of the above projects in the context of the possibility of reusing their experience for the SECURE project.

Table 2 – Possibility of using project results

Project title	Relevance	Transferable elements
CyberSec4Europe	This project focuses on creating a pan-European cybersecurity framework, emphasizing collaboration among academia, industry, and public sectors.	○ Frameworks for capacity-building in cybersecurity research and training. ○ Knowledge-sharing platforms can inspire the proposed R&EHub network in SECURE. ○ Best practices in collaboration between institutions for unified

		digital resilience.
SPARTA	SPARTA emphasizes multidisciplinary innovation, addressing cybersecurity challenges in critical sectors.	- Specialized programs for different sectors (e.g., healthcare, finance) provide a model for tailoring SECURE's educational courses. - Innovation-driven methodologies can guide the development of labs in the R&EHubs.
ECHO	This project builds federated networks for operational security. Its cross-sectoral approach aligns closely with SECURE's goals.	- Federated network models can support cross-connection of SECURE's labs and stakeholders. - Strategies for operational resilience in critical infrastructure.
FORESIGHT	This project creates simulation platforms for training cybersecurity professionals.	- Realistic simulation platforms for 5G and beyond networks could be adapted for SECURE's labs. - Training methodologies targeting real-world scenarios enhance practical skills development.
THREAT-ARREST	Focuses on virtualized environments for cybersecurity training.	○ Virtualized environments are directly applicable to SECURE's training labs. ○ Real-time simulation techniques for attack detection and mitigation align with the objectives of the SECURE project's training modules.
GEIGER	GEIGER strengthens cybersecurity resilience for SMEs.	- Cyber risk assessment tools and tailored training programs could

		inspire content for SECURE's upskilling courses. - Outreach methods targeting SMEs and local communities offer scalable solutions for engaging non-urban areas.
PROTECTIVE	The project emphasizes real-time situational awareness and threat intelligence.	- Threat intelligence sharing frameworks could inform SECURE's cross-lab coordination. - Tools for real-time monitoring of critical infrastructures could enhance SECURE's practical labs.
CONCORDIA	Develops a cybersecurity competence network similar to the collaborative objectives of SECURE.	- Models for pan-European collaboration could inform SECURE's partnership strategies. - Research hubs in CONCORDIA can serve as benchmarks for R&EHub development.
SAFECARE	This project secures healthcare systems, aligning with SECURE's focus on critical infrastructure.	Methodologies for integrating cybersecurity in healthcare could serve as templates for SECURE's educational content.
AI4Cyber	Investigates AI's role in cybersecurity.	AI-driven solutions for threat detection and response can be integrated into SECURE's lab experiments and modules.

Thus, the next conclusion can be made.

Reusable elements:

- Simulation and virtualized training environments (FORESIGHT, THREAT-ARREST).
- Federated network models for lab interconnectivity (ECHO, CyberSec4Europe).
- Best practices in cross-sector collaboration (SPARTA, CONCORDIA).

Real-time threat intelligence sharing frameworks (PROTECTIVE).

Best practices to adopt:

- Multidisciplinary approaches to addressing cybersecurity (SPARTA, CyberSec4Europe).
- Inclusive training programs targeting diverse audiences, including SMEs and underrepresented groups (GEIGER, CyberSecWomen).
- AI integration for enhanced cybersecurity operations (AI4Cyber).

Potential for cross-integration:

- SECURE's R&EHubs could utilize the collaborative frameworks and platforms developed in CONCORDIA and SPARTA.
- Educational modules can adopt methodologies from projects like CyberSecAcademy and Digital Security Learning Initiative.

2. EU regulations analysis

2.1. The European Union's approach to 5G: a strategic vision for digital transformation

The emergence of 5G generation represents a pivotal second in virtual infrastructure, and the European Union has located itself at the vanguard of this technological revolution. Since 2016, the EU has advanced a complete and strategic method to 5G deployment, pushed through an imaginative and prescient of technological leadership, financial competitiveness, and strong safety.

At the middle of the EU`s 5G method is a multifaceted motion plan that transcends mere technological implementation. The number one goal has been to set up Europe as a worldwide chief in next-era telecommunications infrastructure. This ambition is rooted in a holistic method that cautiously balances technological innovation with vital concerns of safety, financial development, and societal impact.

Spectrum control has been an essential issue of the EU's 5G method. Recognizing the significance of harmonized community infrastructure, the EU has coordinated spectrum allocation throughout member states, specializing in key frequency bands that optimize 5G performance. This coordinated method guarantees regular community excellent and allows cross-border connectivity, a vital gain withinside the interconnected European landscape.

Security has emerged as a paramount situation withinside the 5G deployment method. In January 2020, the EU brought a complete cybersecurity toolbox that addresses capacity dangers related to 5G networks. This proactive degree consists of guidelines for limiting high-danger vendors, diversifying device suppliers, and imposing rigorous safety assessments. The method displays a nuanced expertise of the geopolitical complexities surrounding telecommunications infrastructure. The EU's commitment extends beyond regulatory frameworks. Substantial investments through programs like Horizon 2020 and Horizon Europe have supported research, infrastructure development, and innovation. These initiatives encourage public-private partnerships and position European companies at the cutting edge of 5G technology.

Implementation has been strategic and phased. Most EU countries launched initial 5G networks between 2019 and 2021, with ambitious targets for comprehensive urban coverage by 2025. The strategy also emphasizes addressing connectivity challenges in rural and remote areas, ensuring that the benefits of 5G technology are not limited to metropolitan regions.

The regulatory method entails a couple of stakeholders, consisting of the European Commission, BEREC, and country wide regulatory authorities. This collaborative version guarantees a coordinated but bendy implementation which could adapt to numerous country wide contexts at the same time as preserving universal European standards.

Challenges continue to be significant. The EU maintains to navigate complicated problems consisting of handling geopolitical tensions round community equipment, making sure regular implementation throughout member states, and addressing capacity worries associated with fitness and environmental impacts. The ongoing funding in studies and infrastructure demonstrates a long-time period dedication to technological sovereignty and virtual leadership.

What distinguishes the EU`s method is its complete vision. Rather than viewing 5G as simply a technological upgrade, the method conceptualizes it as a crucial infrastructure for virtual transformation. It represents a cautious stability among selling innovation, making sure protection, and helping monetary competitiveness.

As 5G maintains to evolve, the European Union stays devoted to its strategic vision. The movement plan isn't pretty much deploying a brand-new community technology, however

approximately shaping the virtual destiny of a whole continent. By prioritizing coordinated development, stringent protection measures, and non-stop innovation, the EU is positioning itself as an international chief withinside the subsequent technology of virtual communication.

2.2. The emerging landscape of 6G: the European Union's prospective regulatory framework

As the world of telecommunications continues to evolve, the European Union is already laying the groundwork for 6G networks, building upon the experiences and insights gained from 5G deployment. While 6G is still in its early conceptual and research stages, the EU is taking a proactive and strategic approach to its potential development and regulation.

To appreciate the EU's approach to 6G, it's essential to understand that regulatory frameworks are being developed simultaneously with technological research. Unlike previous generations of mobile networks, 6G is being conceptualized not just as a communication technology, but as an integral part of a broader digital ecosystem encompassing artificial intelligence, edge computing, and advanced sensing technologies.

6G standardization is expected to start around 2025 with early study phases. It will follow the global 6G vision. The need for 6G global standards and interoperability is important for our industries. It calls for engagement with all regions, in particular Asia and the US. Research and innovation initiatives relating to 6G have emerged around the world, with the first products and infrastructures expected towards the end of this decade. Europe has the potential to become a leading global provider of 6G if we target investment accordingly. It is crucial to maintain Europe’s sovereignty and market positions in 6G and advanced 5G through partnership with European industry. It is also essential to work with like-minded countries to ensure that the development and deployment of 6G technology align with shared principles and values.

The regulatory framework for 6G networks is built on several fundamental pillars:

1. Cybersecurity and Network Integrity Security stands as the paramount concern in the EU's 6G strategy. Drawing lessons from the challenges encountered during 5G deployment, the regulatory approach emphasizes embedded security protocols from the initial design stages, comprehensive risk assessment methodologies, advanced encryption and authentication mechanisms and rigorous guidelines for hardware and software development.
2. Research and Innovation Significant investments are being channeled into research through programs like Horizon Europe. The focus extends beyond traditional telecommunications, encompassing:
    - Artificial Intelligence integration
    - Quantum communication technologies
    - Energy-efficient network architectures
    - Advanced sensing and distributed computing networks
3. Spectrum Management A critical component of the regulatory framework involves sophisticated spectrum allocation strategies such as identification of optimal frequency ranges, development of harmonized spectrum usage guidelines, creation of flexible allocation mechanisms and support for diverse technological applications

While commercial 6G networks are not expected until approximately 2030, the groundwork is being meticulously laid. The current approach involves:

- Continuous research and development
- Incremental technological advancements
- Adaptable regulatory mechanisms

- Ongoing stakeholder engagement

The European Union's approach to 6G network regulation represents a holistic and forward-thinking strategy that extends far beyond traditional telecommunications policy. By integrating technological innovation, robust security measures, ethical considerations, and economic development, the EU is positioning itself as a key architect of future global communication technologies.

This comprehensive regulatory framework reflects a nuanced understanding that 6G is not merely a technological upgrade, but a transformative infrastructure that will reshape how societies interact with digital technologies. The EU's strategy demonstrates a commitment to responsible innovation, technological sovereignty, and global leadership in the telecommunications landscape.

As the world anticipates the next generation of mobile networks, the European Union stands prepared to guide the development of 6G with a balanced, strategic, and visionary approach.

2.3. Quantum technologies in the European Union: a comprehensive exploration of innovation and regulation

The realm of quantum technologies represents a frontier of scientific and technological innovation that promises to revolutionize multiple sectors of human endeavor. The European Union has emerged as a pivotal player in this transformative landscape, developing a comprehensive and strategic approach that seeks to position Europe at the forefront of quantum technological development.

Quantum technologies harness the unique and often counterintuitive principles of quantum mechanics, offering capabilities that far exceed traditional computational and sensing technologies. Unlike classical technologies that operate on binary principles, quantum systems can exist in multiple states simultaneously, process complex information in ways previously unimaginable, and create fundamentally new approaches to communication, computation, and measurement.

The European Union's approach to quantum technologies is characterized by a holistic and forward-thinking strategy. Rather than viewing quantum technologies as mere technological upgrades, the EU conceptualizes them as transformative infrastructures with profound implications for economic competitiveness, scientific research, and societal development.

This strategic vision is anchored in several core principles. First, there is a deep commitment to technological sovereignty. The EU recognizes that leadership in quantum technologies is not just about scientific achievement, but about maintaining economic independence and strategic technological capabilities. By investing heavily in research, infrastructure, and human capital, the European Union aims to create an indigenous quantum ecosystem that can compete on the global stage.

The regulatory approach to quantum technologies is sophisticated and nuanced. Unlike traditional technology regulations, the EU is developing frameworks that are adaptive and forward-looking. These regulations are not simply about controlling technological development, but about creating an environment that fosters responsible innovation. The governance model involves multiple stakeholders, including research institutions, private corporations, academic centers, and governmental bodies. This collaborative approach ensures that quantum technology development is multidimensional, considering not just technological feasibility, but also ethical implications, economic potential, and societal impact.

Quantum technologies encompass several critical domains. Quantum computing represents perhaps the most transformative area, promising computational capabilities that could solve

complex problems currently beyond human or classical computational capacities. From climate modeling to pharmaceutical research, quantum computers could unlock new frontiers of scientific understanding. Quantum communication technologies offer unprecedented levels of security and data transmission capabilities. By leveraging quantum mechanical principles like entanglement, these technologies could create communication networks that are theoretically impossible to intercept or hack, representing a quantum leap in cybersecurity. Quantum sensing technologies provide measurement capabilities of extraordinary precision. These could revolutionize fields ranging from medical diagnostics to environmental monitoring, offering insights and detection capabilities far beyond current technological limitations.

The European Union is not merely developing quantum technologies; it is strategically positioning them as a cornerstone of future economic competitiveness. Substantial financial resources are being channeled through programs like Horizon Europe, with the explicit goal of creating a robust quantum technology ecosystem. This investment strategy goes beyond direct research funding. It includes support for quantum technology startups, development of specialized educational programs, and creation of collaborative research infrastructures that can attract global talent and investment.

The path to quantum technological leadership is not without significant challenges. The complexity of quantum systems, the extraordinary technical skills required, and the massive research and development costs are substantial obstacles. Moreover, there are profound ethical considerations surrounding the deployment of technologies with such transformative potential. The EU is addressing these challenges through a comprehensive approach that emphasizes responsible innovation. This means not just developing technological capabilities, but carefully considering their societal implications, potential risks, and ethical deployment strategies.

While maintaining a focus on technological sovereignty, the European Union also recognizes the importance of international collaboration. Quantum technologies are inherently global, and no single nation or region can develop them in isolation. The EU is actively participating in international standard-setting, collaborative research initiatives, and knowledge-sharing platforms. This approach positions Europe not as a isolationist technological power, but as a collaborative leader committed to advancing human knowledge and technological capabilities.

The European Union's approach to quantum technologies represents a sophisticated fusion of scientific ambition, economic strategy, and responsible governance. By developing a comprehensive ecosystem that supports research, innovation, and ethical deployment, the EU is not just preparing for the future of technology—it is actively shaping that future. As quantum technologies continue to evolve, the European Union stands prepared to be a global leader, driving forward a technological revolution that promises to reshape our understanding of computation, communication, and scientific possibility.

2.4. EU AI Act: first regulation on artificial intelligence

As part of its digital strategy, the EU wants to regulate artificial intelligence (AI) to ensure better conditions for the development and use of this innovative technology. AI can create many benefits, such as better healthcare; safer and cleaner transport; more efficient manufacturing; and cheaper and more sustainable energy. In April 2021, the European Commission proposed the first EU regulatory framework for AI. It says that AI systems that can be used in different applications are analyzed and classified according to the risk they pose to users. The different risk levels will mean more or less regulation. AI applications influence what information you see online by predicting what content is engaging to you, capture and

analyses data from faces to enforce laws or personalize advertisements, and are used to diagnose and treat cancer. In other words**,** AI affects many parts of your life**.**

The journey towards the AI Act is rooted in a deep understanding of artificial intelligence's transformative potential and its equally significant risks. Unlike previous technological regulations that often reactive, the European Union has crafted a proactive framework that anticipates the complex implications of AI technologies on human society, individual rights, and fundamental values.

At the core of the AI Act lies a sophisticated risk-based classification system that recognizes the fundamental truth that not all artificial intelligence technologies are created equal. This approach demonstrates a sophisticated understanding of technological complexity, acknowledging that AI systems can range from relatively benign tools to potentially harmful technologies that could fundamentally undermine human autonomy and societal structures. The regulation categorizes AI systems into distinct risk levels, providing a targeted approach to governance. Unacceptable risk AI systems—those that pose direct threats to human rights and fundamental values—face the most stringent restrictions. These include invasive social scoring mechanisms, manipulative systems targeting vulnerable populations, and technologies that could systematically undermine individual human agency. High-risk AI applications receive equally careful scrutiny. For these systems, the Act mandates comprehensive risk management protocols, rigorous testing procedures, and ongoing monitoring mechanisms. This approach ensures that potentially powerful technologies are developed and deployed with careful consideration of their broader societal implications.

Beyond its technical specifications, the AI Act represents a profound ethical statement. It embodies a vision of technological development that prioritizes human values over unchecked technological progress. The regulation challenges the tech industry to view innovation not merely as a technical achievement, but as a fundamental social responsibility. This ethical approach is revolutionary. It suggests that technological capabilities should not be the sole metric of success, but must be balanced against their potential impact on human dignity, individual rights, and societal well-being.

The significance of the AI Act extends far beyond the borders of the European Union. By establishing a comprehensive regulatory framework, the EU is effectively creating a global standard for AI governance. Many international technology companies are likely to adopt these regulations as a baseline for their global operations, similar to how the General Data Protection Regulation (GDPR) became a worldwide benchmark for data protection.

A remarkable aspect of the AI Act is its attempt to balance strict regulation with technological innovation. The framework includes provisions to support AI research and development, create experimental regulatory sandboxes, and maintain Europe's global technological competitiveness. This approach recognizes that effective regulation is not about stifling innovation, but about guiding it towards more responsible and ethical trajectories.

The Act is not merely a theoretical document but a practical regulatory mechanism with robust enforcement capabilities. It introduces significant financial penalties for non-compliance, potential market exclusion for systems that fail to meet standards, and mandatory transparency requirements. Independent audit processes will ensure ongoing compliance and adaptation. No groundbreaking regulation is without its challenges. Critics argue that the AI Act might be too restrictive, potentially slowing technological innovation. The rapid evolution of AI technologies means that any regulatory framework risks becoming quickly outdated. However, the EU has built flexibility into the Act, allowing for continuous adaptation and refinement. The AI Act represents more than a regulatory document—it is a vision for how humanity can engage with transformative technologies. It suggests that technological progress

is not an unstoppable force to which society must passively adapt, but a process that can be consciously guided and shaped by human values and ethical considerations.

As artificial intelligence continues to reshape our world, the European Union's AI Act stands as a beacon of thoughtful, principled technological governance. It challenges us to reimagine the relationship between technological innovation and human society, offering a model of regulation that is nuanced, forward-thinking, and fundamentally committed to protecting human dignity. The world will be watching closely as this unprecedented regulatory experiment unfolds, potentially reshaping global approaches to artificial intelligence development. The EU has taken a bold step towards ensuring that technological progress serves humanity's best interests, rather than undermining them.

2.5. Summary of NIST IR 8547: transition to post-quantum cryptography standards

The document outlines the transition from classical cryptographic algorithms to post-quantum cryptography (PQC) standards, addressing the migration from algorithms vulnerable to quantum computing attacks. This transition is critical for ensuring the security of systems in the era of quantum computers. Here's a structured summary of the key concepts and guidelines outlined in the document.

1. Cryptographic Algorithm Approval Status

The document starts by explaining the approval status of cryptographic algorithms used in various security standards, providing clear terminology:

- **Acceptable**: Algorithms and key lengths that are approved for use according to specific standards.
- **Deprecated**: Algorithms that can still be used but come with known security risks. Organizations need to evaluate these risks and decide if continued use is acceptable.
- **Disallowed**: Algorithms that are no longer permitted for use in security-critical applications.
- **Legacy Use**: Algorithms that can only be used for processing already encrypted data (e.g., decrypting ciphertext or verifying digital signatures) but are not appropriate for securing new data.

2. Security Strengths and Post-Quantum Security Categories

The document provides an overview of how security strength is evaluated, both for classical and post-quantum cryptographic algorithms. Security strength refers to the amount of computational effort required to break an algorithm, typically measured in terms of bit-length security. The document highlights a challenge in estimating the security strengths of post-quantum algorithms due to uncertainties in predicting the capabilities of quantum computers.

For post-quantum cryptography, security is categorized into five broad categories, ranging from basic key search attacks on block ciphers to more complex attacks. These categories define the security levels based on quantum threats and classical computing attacks. Key examples include:

- **Category 1**: Key search on a block cipher with a 128-bit key (e.g., AES-128)
- **Category 2**: Collision search on a 256-bit hash function (e.g., SHA-256)
- **Category 5**: Key search on a 256-bit block cipher (e.g., AES-256)

3. Digital Signature Algorithms

NIST acknowledges the vulnerability of current digital signature algorithms to quantum attacks, particularly those based on RSA, ECDSA, and EdDSA. These algorithms are expected

to be deprecated after 2030 and fully disallowed after 2035, depending on their security strength. The guidelines suggest a gradual transition toward quantum-resistant algorithms such as ML-DSA, with different parameter sets that offer varying levels of security strength (128-bit to 256-bit).

4. Key Establishment Schemes

Similar to digital signature algorithms, traditional key establishment schemes such as finite-field Diffie-Hellman (DH) and elliptic curve-based Diffie-Hellman (ECDH) are vulnerable to quantum attacks. NIST plans to deprecate these schemes after 2030, with the goal of completely disallowing them by 2035. In parallel, new quantum-resistant key-establishment techniques are being considered, with ML-KEM being the first approved post-quantum option. ML-KEM, which utilizes multivariate polynomial systems, will eventually replace classical key-exchange protocols.

NIST's guidelines also emphasize the importance of protecting systems against "harvest now, decrypt later" (HNDL) attacks, where quantum adversaries collect encrypted data today with the intention of decrypting it in the future using quantum computers.

5. Symmetric Cryptography

NIST highlights that symmetric cryptographic algorithms, such as block ciphers (AES), hash functions (SHA-2 and SHA-3), and key derivation functions (KDFs), are less vulnerable to quantum attacks than public-key cryptographic systems. However, algorithms that provide less than 128 bits of security (such as AES-128) are at risk and will be deprecated in the coming years.

The document provides detailed security strength categories for hash functions and other symmetric algorithms. For example:

- **SHA-1**: 80 bits of security, deprecated due to vulnerability.
- **SHA-256**: 128 bits of security, categorized under security strength 5.
- **AES-128**: 128 bits of security, categorized under security strength 1.

NIST will continue to support symmetric cryptography for the foreseeable future, but it encourages migration to higher security levels (e.g., AES-256) for better protection.

6. Application-Specific Standards and Guidelines

NIST has developed various standards for cryptographic algorithms applied to specific technologies or systems. For example, FIPS 201-3 outlines the standards for Personal Identity Verification (PIV) in federal systems, which include the use of PKI-based credentials for employee authentication. As part of the PQC transition, NIST plans to revise these application-specific guidelines, including recommendations for the migration to quantum-resistant algorithms.

The guidelines are tailored to different application areas, recognizing that each area has unique security risks and needs. For instance, protocols like Transport Layer Security (TLS) and Internet Key Exchange (IKE) will be prioritized for migration to quantum-resistant key establishment techniques. These protocols are critical for securing network communications and protecting against quantum-enabled eavesdropping and future decryption.

7. Coordination with Standards Organizations

To ensure a smooth transition to post-quantum cryptography, NIST plans to collaborate with various standards-developing organizations and industry leaders. This collaboration is vital to integrate PQC into existing standards, products, and services. NIST emphasizes the need for timely updates to security protocols, recognizing the different adoption challenges faced by different industries.

8. Timeline and Transition Strategy

NIST has outlined a timeline for the gradual deprecation and disallowance of vulnerable cryptographic algorithms. The document stresses that while quantum-resilient algorithms are being developed, there is no immediate need to discard classical algorithms, as quantum computers capable of breaking current cryptography are still theoretical and years away. Nevertheless, the transition to PQC will be a gradual process, with recommendations for early adoption in high-risk sectors like government, finance, and healthcare.

References

1. Directive (EU) 2018/1972 of the European parliament and of the council, establishing the European Electronic Communications Code, 11 December 2018.
2. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient Brussels, 16 December 2020
3. Artificial intelligence act, European Commission, September, 2024
4. National Institute of Standards and Technology. (2024). Transition to post-quantum cryptography standards (NIST IR 8547). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

3. Existing study programmes and courses analysis

3.1. AI/ML Technologies for Security of 5G and Beyond Networks

The course on **AI/ML Technologies for Security of 5G and Beyond Networks** is highly relevant in today's rapidly evolving technological landscape. The increasing reliance on 5G networks and the Internet of Things (IoT) introduces new security challenges that require innovative solutions driven by AI and ML technologies. To design a practical and impactful course as part of the **SECURE project**, it is essential to analyze the best practices from leading European universities offering similar programs.

For this purpose, universities across Europe with AI/ML and cybersecurity courses were selected for detailed analysis. The content, theoretical and practical components, the number of ECTS credits, and the targeted educational levels of these courses were examined. This analysis provides a comprehensive understanding of the key elements and structures of successful programs.

The results of this analysis are summarized in Table 3, offering a clear overview of how European universities approach the integration of AI/ML technologies in cybersecurity. These insights will guide the development of a course that aligns with international standards and addresses modern challenges in 5G security.

Table 3 - AI/ML technologies in cybersecurity courses analysis

№	Institution	Course Title	Description	Number of ECTS points	EQF level	Link
1	Imperial College London (UK)	MSc in Artificial Intelligence	Offers modules such as Advanced Security, Database Systems, and advanced topics in machine learning.	90	EQF Level 7	https://www.imperial.ac.uk/media/imperial-college/study/programme-specifications/computing/24x2f25/G5T1-MSc-Artificial-Intelligence-2024-25.pdf

2	King's College London (UK)	MSc in Artificial Intelligence	Aims to develop knowledge in building, designing, and evaluating intelligent systems, with optional modules in Data Mining, Computer Vision, and Nature-Inspired Learning Algorithms.	90	EQF Level 7	https://www.kcl.ac.uk/study/postgraduate-taught/courses/artificial-intelligence-msc
3	KU Leuven (Belgium)	Advanced Master of Artificial Intelligence	Provides training in engineering, psychology, technology, and other areas, with options for Big Data Analytics, Engineering and Computer Science, and Speech and Language Technology.	60	EQF Level 7	https://www.kuleuven.be/programmes/master-artificial-intelligence#About
4	Radboud University (Netherlands)	Erasmus Mundus Joint Master's in AI (EMAI)	A 2-year program providing a comprehensive framework of theory and practice in AI, in collaboration with three other European universities.	120	EQF Level 7	https://www.upf.edu/web/emai/about-this-master

5	UNED (Spain)	Course on Cybercrime and Artificial Intelligence	Explores the impact of AI on criminal activities, including deepfakes, fake news, and autonomous weapon systems. Aimed at students and professionals in criminology, law, and computer science.	60	EQF Level 6	https://descargas.uned.es/publico/pdf/guias/posgrados/INGLES_310801_2023.pdf
6	Universidade de Évora (Portugal)	Master in Artificial Intelligence and Data Science	Trains professionals to respond to labor market demands in AI and data science, covering applications in health, retail, finance, communications, logistics, and transport.	90	EQF Level 7	https://www.uevora.pt/en/study/courses/master-degrees?cod=ME93
7	Universitat Politècnica de Catalunya (Spain)	Master's Degree in Machine Learning and Cybersecurity for Internet-Connected Systems	Provides advanced training in AI and cybersecurity, focusing on applications in internet-connected systems and the Internet of Things. Organized within the European MERIT project framework.	90	EQF Level 7	https://www.upc.edu/en/masters/machine-learning-and-cybersecurity-for-internet-connected-systems

8	University College London (UCL)	MSc in Machine Learning	Focuses on algorithms and approaches to designing intelligent systems, with optional modules in Applied Machine Learning, Graphical Models, and Machine Vision.	180		https://www.ucl.ac.uk/prospective-students/graduate/taught-degrees/machine-learning-msc
9	University of Aberdeen (UK)	Cybersecurity and Machine Learning MSc	Offers advanced knowledge to develop, design, and analyze security solution architectures, focusing on the evaluation of AI systems' effectiveness.	120	EQF Level 7	https://www.abdn.ac.uk/study/postgraduate-taught/degree-programmes/2023/cybersecurity-and-machine-learning/
10	University of Amsterdam (Netherlands)	MSc in Artificial Intelligence	A two-year program covering machine and deep learning, information retrieval, and natural language processing.	120	EQF Level 7	https://www.uva.nl/en/programmes/masters/artificial-intelligence/artificial-intelligence.html
11	University of Edinburgh (UK)	MSc in Artificial Intelligence	Offers modules such as Probabilistic Modelling and Reasoning, Automatic Speech Recognition, and Reinforcement Learning.	120	EQF Level 7	http://www.drps.ed.ac.uk/24-25/dpt/ptmscaintl1f.htm

12	University of Klagenfurt (Austria)	Master in Artificial Intelligence and Cybersecurity	A double degree program with the University of Udine, focusing on AI and cybersecurity, with opportunities to study courses relevant to both fields.	120	EQF Level 7	https://www.aau.at/en/studien/master-artificial-intelligence-and-cybersecurity/
13	University of Limerick (Ireland)	MSc in Artificial Intelligence	Provides a comprehensive grounding in AI, covering areas such as machine learning, data mining, and natural language processing.	90	EQF Level 7	https://www.ul.ie/gps/artificial-intelligence-msc-online
14	University of Manchester (UK)	MSc in Artificial Intelligence	Includes modules in Text Mining, Foundations of Machine Learning, Data Engineering, Cyber Security, and Cryptography.	120	EQF Level 7	https://www.manchester.ac.uk/study/masters/courses/list/21574/msc-artificial-intelligence/#course-profile
15	University of Minho (Portugal), University of Granada (Spain), Vilnius University (Lithuania), University of Padua (Italy)	Joint Master's Programme in International Cybersecurity and Cyberintelligence	A full-time program offering specialized education in cybersecurity, cyberintelligence, and international relations and law for cybersecurity. Involves mobility across four European universities.	120	EQF Level 7	https://arqus-alliance.eu/study-in-arqus/joint-masters-programmes/master-in-cybersecurity-cyberintelligence

16	University of Oxford (UK)	Artificial Intelligence for Cyber Security (Online)	Designed for cybersecurity professionals seeking to understand AI, and AI professionals aiming to work in cybersecurity. Covers the impact of AI on various cybersecurity personas and includes practical coding demonstrations.	10	EQF Level 7	https://conted.ox.ac.uk/courses/artificial-intelligence-for-cyber-security-online#programme_details_container
17	University of Sheffield (UK)	Cybersecurity and Artificial Intelligence MSc	Provides grounding in both cybersecurity and AI, teaching application in business and industry. Includes modules from both disciplines and a research project at their interface.	120	EQF Level 7	https://www.sheffield.ac.uk/postgraduate/taught/courses/2025/cybersecurity-and-artificial-intelligence-msc
18	University of Sussex (UK)	MSc in Artificial Intelligence and Adaptive Systems	Focuses on the development of AI systems that can adapt and learn, with applications in robotics, software agents, and more.	135		https://www.sussex.ac.uk/study/masters/courses/artificial-intelligence-and-adaptive-systems-msc
19	University of Liverpool	MSc in Artificial Intelligence	Online program broadening horizons in intelligent systems and enhancing skills in this rapidly growing sector.	120	7	https://online.liverpool.ac.uk/programmes/msc-artificial-intelligence/

20	SANS Institute	Artificial Intelligence Cyber Security	Incorporates GenAI/ML training across broader cybersecurity education, equipping professionals to tackle AI-related complexities and defend against sophisticated cyber threats.	60-120	n/a	https://www.sans.org/ai/
21	Coursera (Various Universities)	AI for Cybersecurity Specialization	Explores advanced techniques for detecting and mitigating cyber threats, including AI-driven fraud prevention and malware analysis.	60-120	n/a	https://www.coursera.org/search?query=Advanced%20Artificial%20Intelligence

Key aspects of the courses

1. Focus on AI/ML

Most programs emphasize integrating AI/ML across various fields, ranging from automation to cybersecurity. Core topics include machine learning (ML), deep learning (DL), natural language processing (NLP), and graph neural networks (GNNs). These components equip students with the tools to analyze and address complex problems, making AI/ML central to modern technological advancements.

2. Cybersecurity

Several courses, such as those offered by the University of Sheffield, University of Oxford, and Universitat Politècnica de Catalunya, prioritize using AI/ML in cybersecurity. These programs focus on network monitoring, securing IoT devices, and protecting 5G networks while addressing emerging threats. This integration demonstrates how AI-driven solutions are becoming indispensable for proactive and adaptive cybersecurity measures.

3. Interdisciplinary Approach

Programs like those at the University of Nottingham and KU Leuven blend AI with cognitive sciences, engineering, and legal frameworks. This multidisciplinary approach ensures students can apply AI solutions in diverse contexts, balancing technical, ethical, and social considerations. It prepares graduates for roles that require both technical expertise and an understanding of broader societal impacts.

4. Flexibility in Learning

Some courses, such as those from the University of Liverpool and Coursera, offer online formats tailored for working professionals. This flexibility allows students to balance their studies with professional commitments while gaining advanced knowledge. Online options also broaden accessibility, making AI/ML education available to a global audience.

5. ECTS Structure

Most programs provide 120 ECTS, aligning with full master's degree requirements at EQF Level 7. However, some offer flexible formats, with 60–90 ECTS, catering to specialized or

condensed learning needs. This variation ensures that both full-time students and professionals seeking targeted skill development can find suitable options.

Common themes across courses

1. **Machine Learning (ML)**

All programs incorporate fundamental ML algorithms such as regression, classification, and clustering. These foundational methods are complemented by hands-on experience with tools like TensorFlow, PyTorch, and Scikit-learn. This ensures students not only understand theoretical concepts but also gain practical skills to develop and deploy ML models in real-world scenarios.

2. **Deep Learning (DL)**

A significant focus is placed on advanced DL techniques, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). These methods are crucial for processing large datasets, analyzing network traffic, and tackling complex AI-driven challenges. This emphasis highlights the importance of DL in addressing critical issues across various technological domains.

3. **IoT and 5G Security**

IoT and 5G security are pivotal topics in many programs, such as those offered by Universitat Politècnica de Catalunya and the University of Sheffield. These courses explore how AI and ML can be leveraged to identify and mitigate vulnerabilities in IoT devices and safeguard 5G networks. This focus prepares students to tackle emerging challenges in the rapidly evolving landscape of connected technologies.

4. **Ethical and Legal Considerations**

Programs address essential ethical and legal aspects, including GDPR compliance, data privacy protection, and the societal impacts of AI technologies. For example, King's College London integrates these discussions into its curriculum, ensuring students are equipped to navigate the ethical challenges of deploying AI solutions. This balance of technical and regulatory knowledge fosters responsible AI implementation.

5. **Research and Practical Applications**

Universities emphasize research projects and practical laboratories, enabling students to apply their knowledge to real-world cases. These opportunities bridge the gap between theoretical learning and practical problem-solving, fostering innovation and hands-on expertise. Such experiences are integral to preparing graduates for complex challenges in industry and academia.

Key Conclusions on Relevant Topics for AI/ML security course

- **Real-Time Threat Detection**

AI/ML technologies are increasingly being utilized for real-time analysis of network traffic, anomaly detection, and automating security processes. These capabilities allow for faster identification and mitigation of threats, making them essential for modern cybersecurity. Real-time threat detection ensures that organizations can proactively defend against sophisticated cyberattacks.

- **IoT Security in 5G**

The integration of IoT and 5G requires specialized security solutions tailored to the unique vulnerabilities of these technologies. AI can predict attacks, analyze device behaviors, and enhance the overall security framework for IoT within 5G networks. This is critical for safeguarding smart devices and ensuring the reliability of connected ecosystems.

- **Explainable AI (XAI)**

Explainable AI plays a pivotal role in providing transparency and building trust in AI-driven decisions, particularly in critical systems like cybersecurity. XAI ensures that stakeholders can understand and validate AI outputs, which is essential for sensitive applications such as network monitoring and threat mitigation. This fosters ethical and reliable use of AI technologies.

- **Ethical Challenges**

Data privacy protection and the ethical use of AI in cybersecurity remain critical concerns. Addressing issues like GDPR compliance and the societal impacts of AI deployment is necessary to ensure responsible innovation. These challenges emphasize the need for a balanced approach that integrates technical solutions with regulatory frameworks.

- **Practical Orientation**

Practical coursework, including hands-on tasks, laboratory exercises, and interdisciplinary research, is a common feature of leading AI/ML programs. By working on real-world cases, students develop the skills to address practical challenges in cybersecurity. This approach bridges the gap between academic learning and industry demands.

Recommended structure of the course: AI/ML technologies for cybersecurity

Based on the analysis of courses from leading EU universities such as KU Leuven, Radboud University, and the University of Amsterdam, the proposed structure integrates practical skills, the adaptation of theoretical knowledge to real-world cases, and the use of advanced technologies.

Table 4 – Recommended Structure of the course

#	Module	Topics	Skills	Inspiration	Assessment
1	Introduction to 5G, Beyond Networks, and AI/ML (15 ECTS)	5G architecture: key technologies, use cases. IoT, MEC (Mobile Edge Computing), Massive MIMO. Fundamentals of AI/ML: concepts and applications in cybersecurity.	Analyzing the structure of 5G networks. Understanding AI/ML in the context of modern technologies.	KU Leuven, University of Amsterdam	Theoretical exam and analysis of network security case studies.
2	Threats to 5G and Beyond Networks (15 ECTS)	Common attacks: DDoS, man-in-the-middle, spoofing. IoT security challenges in the context of 5G. Privacy and data protection in 5G.	Identifying threats to network systems. Analyzing attack scenarios and their impacts.	University of Sheffield, University of Aberdeen	Practical case study on modeling 5G attacks.
3	AI/ML for Cybersecurity (15 ECTS)	Core ML algorithms: classification, clustering,	Building foundational AI/ML models.	Radboud University, KU Leuven	Practical task on training ML models.

		regression. Deep learning (DL) and its role in security. Tools for threat analysis (TensorFlow, PyTorch).	Using AI/ML to detect threats.		
4	IoT Security in the Context of 5G (15 ECTS)	IoT in 5G networks: architecture and vulnerabilities. IoT device attacks: detection methods. Data encryption and IoT security mechanisms.	Analyzing IoT traffic to identify threats. Developing IoT protection systems in 5G.	University of Cambridge, University of Limerick	Laboratory work on securing IoT devices.
5	Anomaly Detection in 5G with AI/ML (15 ECTS)	Network traffic analysis for anomaly detection. Explainable AI (XAI) for threat analysis. Behavioral models of users.	Using AI for traffic monitoring. Building and training models for anomaly analysis.	Imperial College London, KU Leuven	Task involving XAI for traffic analysis.
6	Advanced Machine Learning for Security (15 ECTS)	Deep neural networks (CNN, RNN) for threat analysis. NLP for phishing detection and email attack analysis. Graph neural networks for monitoring large networks.	Applying CNN and NLP for complex threat analysis. Using graph-based algorithms for network structure analysis.	University of Manchester, University College London (UCL)	Project involving CNN or NLP applications.
7	AI for Critical Infrastructure Protection (15 ECTS)	The role of AI/ML in protecting industrial systems and energy networks. Adaptive security models for critical infrastructures.	Analyzing real-world cases (energy grids, transportation). Developing solutions for	University of Amsterdam, University of Klagenfurt	Practical case study on designing adaptive security systems.

		Investigating cyberattacks with AI.	automating security.		
8	Ethical, Legal, and Social Aspects of AI/ML in Cybersecurity (10 ECTS)	Ethical challenges in using AI/ML for security. EU legislation on data privacy (GDPR). Social impacts of AI in 5G networks.	Analyzing ethical issues in cybersecurity. Understanding regulatory requirements.	King's College London, University of Sussex	Essay or group discussion on ethical aspects.

Advantages of recommended course structure

1. **Adaptability to Real-World Needs**

The course is designed based on widely recognized themes from EU programs, ensuring its relevance to the current demands of the field. By integrating best practices and addressing the challenges faced in modern networks, the course provides students with the tools to tackle real-world cybersecurity and AI/ML problems. This adaptability ensures graduates are well-prepared to meet the expectations of employers and the evolving industry landscape.

2. **Balance of Theory and Practice**

This course strikes a balance between theoretical knowledge and practical application. Students gain a solid foundation in AI/ML concepts while participating in hands-on laboratory exercises that simulate real-world scenarios. This combination enhances their problem-solving abilities and equips them with actionable skills that can be immediately applied in professional settings.

3. **Relevance**

The course focuses on addressing modern challenges related to 5G and Beyond Networks, which are critical to the advancement of global technology. By emphasizing cybersecurity in IoT and AI-driven anomaly detection, the program ensures that students are trained in the most pressing and emerging areas. This focus on contemporary issues increases the course's value and appeal in the rapidly evolving tech industry.

4. **Preparation for Critical Infrastructure Roles**

The structure is tailored to prepare professionals for roles in critical infrastructure protection, leveraging AI/ML technologies. The course equips students to design and implement security solutions for energy grids, industrial systems, and connected networks. Graduates will leave with the knowledge and skills necessary to safeguard essential systems against complex cyber threats.

3.2. Cybersecurity in 5G and beyond

№	Institution	Course Title	Description	Number of ECTS points, hours	EQF level	Link
1	Imperial College London (UK)	5G Security	This course presents current security aspects and new functions to improve security of 5G networks for communication with regular users and the growing number of IoT devices.	30 hours	N/A	https://apistraining.com/5g-security/
2	P1 Security (UK)	5G Telecom Security hands-on course (TS-501)	This online training will help security and telecom professionals get an understanding of the key concepts of 5G, their security, the implementation of such architectures and the impact in terms of related risks.	3 days	N/A	https://online-training.p1sec.com/course/5g-telecom-security-ts-501
3	Tonex, US	5G Cybersecurity Training Bootcamp | 3GPP Version	5G cybersecurity training bootcamp is a 4-day course that focuses on 5G cybersecurity issues and mitigation techniques. The scope of this training is to leverage the 5G security features which are defined in standards to provide enhanced cybersecurity capabilities	1 day	N/A	https://www.tonex.com/training-courses/5g-cybersecurity-training-bootcamp-3gpp-version/

			addressing needs for service providers, network equipment manufacturers, software vendors and end-user devices.			
4	Tonex, US	5G Core Network Security Threat and Risk Assessment	This specialized course is designed for network security professionals, system engineers, and IT personnel focusing on the emerging domain of 5G networks. It explores the unique security challenges posed by 5G technology, including vulnerability assessments for 5G applications, Network Functions Virtualization (NFV), and Software-Defined Networking (SDN).	2 days	N/A	https://www.tonex.com/training-courses/5g-core-network-security-threat-and-risk-assessment/
5	Tonex, US	5G Security Training	5G Security Training is a hands-on practical 2-day course where participants garner a strong and intuitive understanding of what security in the wireless systems is and how the security functions are implemented in the 5G, 5G NR, 5GC, Service Based Architecture (SBA), HTTP2/JSON and REST API, and	2 days	N/A	https://www.tonex.com/training-courses/5g-security-training/

			optional non 3GPP radio including 802.11ax, mmWave/802.11ay radio and core network.			
6	Tonex, US	6G Cybersecurity Course by Tonex	6G Cybersecurity is a 2-day course where participants identify and assess the unique security risks and vulnerabilities in 6G networks as well as apply security frameworks and strategies for securing 6G network architecture.	2 days	N/A	https://www.tonex.com/training-courses/6g-cybersecurity-course/
7	Blackbird for training, UK	The 5G Network Security	5G Network Security Training course presents old and new threats, security aspects, requirements, and recommendations from various organizations, and then the new, improved functions and procedures designed to improve the security of the future 5G networks for communication with regular users and a growing number of IoT devices.	5 days	N/A	https://blackbird-training.com/course-The-5G-Network-Security

8	Nokia Bell Labs, FInland	5G Secured Networks	The 5G Secured Networks course is part of the Professional Level of the Nokia Bell Labs 5G Certification Program. In this course we will examine the role of security in 5G systems, and look at different security threats and how to protect against them especially in light of network security in the 5G world. Additionally, we will look at specific case studies to further our knowledge of security.	5 days	N/A	https://www.nokia.com/networks/training/5g/bell-labs/secured-networks/
9	MPIRICAL,	5G Security	This course seeks to explore each of these areas by initially evaluating the end to end 5G System, in terms of architecture and overall operation, with emphasis on security roles. 5G AKA will then be explored in detail, including signalling flows and API exchange, before concluding with a breakdown of SBI security.	6 days	N/A	https://www.mpirical.com/courses/5g-security

10	Glasspaper	5G Security	This course takes an end to end view of 5G security, first of all determining what assets are applicable to the 5G architecture and which threats are relevant. The course then moves on to examine the security techniques being relied upon to provide end to end security, before concluding with a detailed analysis of 5G Authentication and Key Agreement.	1 day	N/A	https://www.glasspaper.no/en/courses/5g-security/
11	London Premiere Centre, Barcelona, Spain	The 5G Network Security Training	5G Network Security Training course presents old and new threats, security aspects, requirements, and recommendations from various organizations, and then the new, improved functions and procedures designed to improve the security of the future 5G networks for communication with regular users and a growing number of IoT devices.	1 week	N/A	https://www.lpcentre.com/barcelona/safety-security/5g-network-security-training

12	Apis Training, Stockholm, Sweden	5G Security	This course presents old and new threats, security aspects, requirements, recommendations from various organizations and then the new, improved functions and procedures designed to improve the security of the future 5G networks for communication with regular users and the growing number of IoT devices.	2 days	N/A	https://apistraining.com/5g-security/
13	IEEE	5G Security	5G incorporates some significant changes and enhancements to security, compared to LTE systems, especially in terms of the threat model and security architecture. However, the scope of what is 5G is rather large, as 5G includes traditional mobile broadband services, as provided by 4G systems, as well as whole new application areas like IoT, URLLC, etc., and a revolutionary network architecture. Consequently, the scope of what could be said to be "5G Security" is also huge. In this course, however, we focus	2 days	N/A	https://www.comsoc.org/education-training/training-courses/online-courses/2021-12-5g-security

			on the essence of 5G security in terms of security of the 5G network subscription (concepts of authentication, SIM, etc., some of which have evolved from 3G and 4G, but enhanced with the benefit of lessons learnt from operation of the earlier networks), including but not limited to mobile broadband services. We cover protocols that extend the protections to 5G scenarios of IoT, V2X, etc.			
14	NobleProg, Dublin, Ireland	5G Mobile Communication Penetration Testing Training Course	The arrival of the 5G mobile wireless network has brought with it new security challenges. This instructor-led, live training (online or onsite) is aimed at engineers who wish to implement security policies and technologies to secure 5G wireless networks.	35 hours	N/A	https://www.nobleprog.ie/cc/5gtesting

15	University of Surrey Guildford Surrey, Great Britain	5G and Future Generation Communication Systems	Our 5G and Future Generation Communication Systems MSc degree equips you with the skills and knowledge needed to design, implement, and manage cutting-edge communication networks that will shape the future of connectivity.	6	Masters	https://www.surrey.ac.uk/postgraduate/5g-and-future-generation-communication-systems-msc
16	Technical University of Sofia, Sofia, Bulgaria	5G networking	The course will provide 64 hours of in-depth training on 5G technology and standards, and be held in Bulgarian by professors from the Faculty of Telecommunications based on Ericsson learning materials covering 5G RAN, 5G Core and 5G Cloud. The course lasts two semesters in the 2022-2023 academic year.	64	N/A	https://www.ericsson.com/en/news/3/2022/ericsson-and-technical-university-of-sofia-collaborate-to-prepare-bulgarian-students-for-a-5g-ready-future
17	University of Essex, Wivenhoe Park, Colchester CO4 3SQ, Great Britain	5G and Emerging Communication Systems	5G and emerging communications systems will be the future of a modern life. 5G is the latest mobile technology that the UK's leading network operators are rolling out across the country, which can connect almost everything in the world with much higher speeds and capacity.	1 year	Master	https://www1.essex.ac.uk/programmespecs/Details.aspx?prog=12859

			Starting from the concept of a signal, on this course you'll cover the fundamentals of how signals are acquired, processed and transmitted over a wide range of media — electronic, optical and radio. You'll learn how these principles are put into practice and you'll improve your software development skills through lectures, exercises and assignments.			
18	Lund University, Sweden	ESoA course on mobile radio communication for 5G and beyond	The course cover propagation aspects for cellular and vehicular communication. Starting with the basics of propagation, modern methods used in cellular network planning as well as aspects relevant for future 5G networks, e. g. MIMO, multi-link aspects, localisation, car2X and spectrum regulation are taught.	5 days	N/A	https://www.tu-braunschweig.de/en/ifn/news-events/news-details/esoa-course-on-mobile-radio-propagation-for-5g-and-beyond

19	Lund University, Sweden	EITP30 Modern Wireless Systems - 5G and Beyond 2024/2025	This course considers the latest technology development in wireless communications, including 5G and LTE systems. These systems are high performing and represent "state-of-the-art" in many aspects. A central part of this course is to give detailed knowledge of the communication methods that are used in down-link and up-link. This course also includes trends for future system solutions. The aim of this course is to give fundamental knowledge concerning principles, concepts, functioning, performance, and limitations for such systems for mobile communications.	1 semester	Masters	https://www.eit.lth.se/?ciuid=1750&courspage=11113

Key Aspects of the Courses

1. **Technical Focus Areas**:
    - All analyzed courses emphasize foundational topics, such as securing Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Open RAN (ORAN).
    - Modules addressing end-to-end encryption, authentication mechanisms, and vulnerability assessments in 5G systems are prevalent.
2. **Application-Specific Modules**:
    - Courses often explore sector-specific use cases, such as smart cities, autonomous vehicles, and healthcare systems, to contextualize 5G security challenges.

- Emphasis on securing massive IoT deployments, ultra-reliable low-latency communication (URLLC), and network slicing was common.

3. **Hands-on Labs and Tools**:
   - Practical activities, including penetration testing of 5G networks and simulated cyberattacks, are integral. Tools like Wireshark, GNS3, and custom-built simulation platforms are frequently used.
4. **Regulatory and Compliance Training**:
   - Many courses include modules on global cybersecurity standards (ETSI, NIST) and compliance frameworks like GDPR and ISO 27001.

Common themes across courses

1. **Emerging Threat Landscape**:
   - Recognition of evolving threats, such as denial-of-service (DoS) attacks on network slices, vulnerabilities in ORAN, and risks to edge computing.
2. **Interdisciplinary Approach**:
   - Integration of concepts from networking, cryptography, AI/ML, and data security to address the multifaceted nature of 5G security.
3. **Critical Infrastructure Security**:
   - Courses often highlight securing 5G's role in critical sectors like healthcare, energy, and transportation.
4. **Collaboration and Knowledge Sharing**:
   - Emphasis on industry-academia partnerships to stay ahead of emerging threats and foster innovation.

Key Conclusions on Relevant Topics for the Course

1. **Focus on Vulnerability Management**:
   - Addressing vulnerabilities in NFV, SDN, and IoT ecosystems is critical for 5G security.
2. **Enhanced Real-Time Monitoring**:
   - Real-time threat detection and incident response strategies, using tools like AI-driven anomaly detection, are essential.
3. **Importance of Network Slicing Security**:
   - Since 5G relies on network slicing for diverse applications, its security is paramount and needs dedicated modules.
4. **Scalability and Flexibility**:
   - Security solutions should account for the dynamic nature of 5G deployments, ensuring resilience against large-scale attacks.

Recommended Structure of the Course

1. **Module 1: Fundamentals of 5G Security (20 Hours)**
   - Overview of 5G architecture, key components, and unique security challenges.
   - Introduction to NFV, SDN, ORAN, and their role in 5G.
2. **Module 2: Threats and Vulnerabilities in 5G (20 Hours)**
   - Analysis of the 5G threat landscape, including IoT vulnerabilities and network slice attacks.
   - Case studies of major 5G security incidents.
3. **Module 3: Securing Network Slices and Applications (20 Hours)**
   - Best practices for securing URLLC, eMBB, and mMTC slices.

- Real-world applications in smart cities, healthcare, and autonomous vehicles.

4. **Module 4: Cybersecurity Frameworks and Compliance (20 Hours)**
   - Standards and frameworks: ETSI, NIST, GDPR, and ISO 27001.
   - Regulatory challenges in global 5G rollouts.
5. **Module 5: Hands-On Labs and Practical Tools (30 Hours)**
   - Penetration testing of 5G networks using simulation tools.
   - Anomaly detection and real-time monitoring using AI/ML models.
6. **Module 6: Capstone Project (10 Hours)**
   - Design and implement a security framework for a 5G-enabled critical infrastructure.

3.3. Post-quantum and quantum cryptography

№	Course title	Institution	Link
1	IIK8105 - Post-Quantum Cryptography	Norwegian University of Science and Technology	https://www.ntnu.edu/studies/courses/IIK8105#tab=omEmnet
2	NFYK23002U Introduction to Quantum Information Science	University of Copenhagen	https://kurser.ku.dk/course/NFYK23002U
3	NMAK23007U Introduction to Quantum Computing	University of Copenhagen	https://kurser.ku.dk/course/NMAK23007U
4.	Practical Quantum Computing with IBM Qiskit for Beginners	IBM	https://www.coursera.org/learn/packt-beginners-guide-to-practical-quantum-computing-with-ibm-qiskit-w6mos
5	Quantum for Everyone	Open Quantum Institute	https://open-quantum-institute.cern/edulink/qureca-online-training-quantum-for-everyone/
6.	Post-Quantum Cryptography (PQC)	University of Maryland	https://www.umbctraining.com/courses/pqc
7.	Introducing a developer's course on post-quantum cryptography	IBM	https://developer.ibm.com/blogs/quantu

			m-introducing-course-post-quantum-cryptography/
8	Quantum random numbers in Machine Learning (research paper, interesting for teaching process)	Lamarr Institute for Machine Learning and Artificial Intelligence	https://lamarr-institute.org/blog/quantum-random-numbers-ml/
9.	Implement a quantum random number generator in Q#	Microsoft	https://learn.microsoft.com/en-us/azure/quantum/tutorial-qdk-quantum-random-number-generator?tabs=tabid-copilot
10.	Quantum Random Number Generation	Fraunhofer Institute for Applied Optics and Precision Engineering IOF	https://www.iof.fraunhofer.de/en/events/quantum-random-number-generation.html

Course detailed description:

1. The course focuses on post-quantum cryptography, exploring topics like lattice-based, code-based, hash-based, and isogeny-based cryptography, with an emphasis on standardized algorithms. It includes quantum algorithms, hardness estimation, and side-channel attacks. The learning outcomes cover advanced knowledge of post-quantum cryptography, protocol construction, and scientific discussion. Students engage in lectures, presentations, and discussions. Prior knowledge in applied cryptography or secure implementations is recommended. Evaluation involves oral presentations on assigned topics.
2. The *Introduction to Quantum Information Science* course covers the quantum mechanical principles of quantum bits (qubits), their evolution, measurements, noise effects, and links to classical information science. It includes theoretical and experimental components, focusing on quantum states, quantum gates, and their implementation in photonics. The course also introduces classical information theory concepts such as error correction and communication complexity. Students will gain the skills to explain quantum bit operations, assess quantum state evolution, and compare quantum and classical computing methods. This course prepares students for further quantum information studies.
3. The course in Quantum Computing and Information introduces quantum computing, covering fundamental topics like quantum states, superposition, and measurement, along with protocols like teleportation and quantum key distribution. It explores quantum algorithms, computational supremacy, and cryptographic schemes. Students will also work with real quantum computers through cloud-based access. The course aims to provide knowledge of quantum information principles, develop computational skills, and enhance the ability to analyze and apply quantum protocols.

4. This course introduces quantum computing through IBM's Qiskit framework, providing both theoretical understanding and practical experience. Students will learn fundamental concepts such as quantum states, qubits, and quantum gates, exploring how these concepts differ from classical computing. The course covers quantum circuits, algorithms like Deutsch-Jozsa, and quantum key distribution, with hands-on exercises using real quantum computers via the cloud. Additionally, students will explore more advanced topics like quantum teleportation and multi-qubit states. Designed for beginners, the course only requires basic Python knowledge and no prior quantum computing experience.

5. The Open Quantum Institute offers a non-technical course aimed at equipping participants with an understanding of the emerging quantum technologies and their business applications. The course covers key topics such as quantum computing, cloud-quantum computing, and quantum cryptography. Participants will improve their technical, business, and management skills by exploring real-world use cases, learning to identify industry partners, and acquiring strategies for deploying quantum computing projects within their organizations while addressing cybersecurity risks. The course is suitable for both individuals and businesses looking to navigate the quantum landscape.

6. This course is designed to help organizational leaders, security officers, and IT professionals prepare for the imminent arrival of quantum computing. It focuses on the threat quantum computing poses to current cryptographic systems, as adversaries are already collecting encrypted data that could be decrypted once quantum computers become available. The course emphasizes the need to adopt Post-Quantum Cryptography (PQC) to secure communications and information assets, and provides strategies for mitigating these emerging risks to organizational security.

7. The "Practical Introduction to Quantum-Safe Cryptography" course on IBM's Quantum Learning platform provides a primer for developers interested in updating their application security. It covers four core areas: cryptographic hash functions, symmetric and asymmetric key cryptography, and quantum-safe cryptography. The course explains how quantum computing could undermine existing cryptographic methods and provides steps to transition to quantum-safe solutions. It emphasizes the need to address the risks of "harvest now, decrypt later" attacks and the importance of adopting quantum-resistant algorithms ahead of industry standards.

8. The article discusses the importance of random numbers in machine learning (ML) and artificial intelligence (AI), particularly for tasks like stochastic optimization, data sampling, and initializing neural networks. High-quality random numbers play a crucial role in how models are trained and how efficiently they converge. The piece distinguishes between pseudorandom numbers (generated by deterministic algorithms) and quantum random numbers (generated using quantum mechanical principles). While pseudorandom numbers are commonly used in ML, quantum random numbers—derived from the behavior of qubits—are considered to have superior randomness. The idea was that quantum randomness might improve the initialization of neural networks and lead to better performance. However, research from the Lamarr Institute for Machine Learning and Artificial Intelligence (formerly ML2R) and others has shown that quantum random numbers, when generated on current quantum computers, exhibit certain distortions that make them less random than pseudorandom numbers. For example, they found that quantum-generated numbers on IBM's quantum computers had an average probability of 48.88% for being 1 (slightly less than the expected 50%), which resulted in a non-uniform distribution. Despite these imperfections, the researchers found no significant advantage in using quantum random numbers over pseudorandom numbers in the training of ML models. This is largely due to the high-quality

pseudorandom number generators available today and the current limitations of quantum computers, which are prone to errors that distort the randomness of the generated numbers. The conclusion highlights that while quantum computing holds potential for new ML insights, especially in generating random numbers, the technology is still evolving. As quantum computing improves, it may eventually lead to breakthroughs in machine learning, but for now, pseudorandom numbers remain a robust and effective tool for model training.

9. This course offers an introduction to **Quantum Random Number Generation (QRNG)**, focusing on how quantum mechanics can be used to produce high-quality random numbers. These random numbers are essential for a wide range of applications, from cryptography and machine learning to simulations and secure communications. Students will learn to create quantum random number generators using **Q#** and **Azure Quantum**, providing them with hands-on experience in implementing quantum randomness for real-world applications. Students will explore the basics of quantum mechanics, qubits, superposition, and measurement, and understand how these concepts are applied to generate truly random numbers. The course covers the use of quantum mechanics to produce random numbers with greater unpredictability compared to classical methods, with applications in cryptography and machine learning. Students will learn how to implement quantum random number generators using **Q#** programming language, allowing them to apply their knowledge practically. The course demonstrates how QRNGs can enhance security in quantum-safe cryptography and improve machine learning model performance through better initialization. Students will develop the ability to combine quantum and classical computing methods to solve problems related to random number generation, cryptography, and machine learning. Students will gain experience running quantum programs on **Azure Quantum** and other platforms to generate random numbers.: Students will learn to write quantum programs using **Q#** and understand how to apply quantum mechanics to random number generation. They will explore how quantum-generated random numbers can strengthen encryption methods and secure digital communications. The course will also cover how quantum randomness can improve the training of machine learning models by providing better initialization methods. Students will learn to apply quantum principles practically, evaluating the quality of quantum-generated randomness and distinguishing it from classical randomness. The course is for quantum computing enthusiasts who want to explore real-world applications of quantum technologies, cryptographers and security experts interested in enhancing digital security using quantum randomness, machine learning engineers looking to improve model training using quantum techniques, and developers interested in quantum programming and implementing quantum random number generators.

10. This course introduces Quantum Random Number Generation (QRNG), highlighting how quantum mechanics can be leveraged to generate high-quality random numbers. QRNG is essential for a wide array of applications, including cryptography, machine learning, simulations, and secure communications. The course teaches students how to build quantum random number generators using Q# and Azure Quantum, offering practical experience with quantum randomness. Students explore fundamental quantum mechanics concepts such as qubits, superposition, and measurement, and see how these principles are used to generate truly random numbers. The course explains how quantum-generated random numbers offer superior unpredictability compared to classical methods, with applications in cryptography and machine learning. Students also learn to implement quantum random number generators in Q#, giving them the tools to apply quantum randomness in real-world projects. QRNG enhances security in quantum-safe cryptography and improves machine learning model performance by providing better initialization. The course combines both quantum and classical computing to

solve problems in random number generation, cryptography, and machine learning. Students run quantum programs using Azure Quantum to generate random numbers and explore various applications. Students learn to write quantum programs in Q#, apply quantum mechanics to random number generation, and explore the use of quantum randomness in securing digital communications. The course also teaches how quantum randomness benefits machine learning model training through improved initialization. Students assess the quality of quantum-generated randomness and understand its distinctions from classical methods. This course is ideal for quantum computing enthusiasts, cryptographers and security professionals looking to enhance digital security with quantum randomness, machine learning engineers seeking to improve model performance, and developers interested in quantum programming and implementing quantum random number generators. A basic understanding of quantum mechanics is helpful but not required. Familiarity with programming (especially Q#) is also beneficial, though not mandatory.

3.4. DevSecOps

№	Course title	Institution	Link
1	DevOps and Continuous Software Engineering	University of Limerick	https://www.ul.ie/gps/devops-and-continuous-software-engineering-graduate-diploma
2	Bachelor of Science (Honours) in Cloud Computing with DevOps	TU Dublin	https://www.tudublin.ie/study/part-time/courses/cloud-computing-tallaght-tu066/
3	DevOps and Cloud Computing	University of Europe for Applied Sciences	https://www.iu.org/master/devops-and-cloud-computing/
4.	Bachelor in DevOps and Cloud Engineering	Amsterdam Tech	https://amsterdam.tech/devops-cloudengineering/
5	Computing in DevOps	Atlantic Technological University	https://www.atu.ie/courses/master-of-science-computing-in-devops
6.	Continuous Delivery and DevOps	University of Southern Denmark	https://studyindenmark.dk/portal/university-of-southern-denmark-

			sdu/odense/continuous-delivery-and-devops
7.	DevOps	The University of Chicago	https://professional.uchicago.edu/find-your-fit/courses/devops
8	3957 - Foundations of DevOps I: Principles and Practices	University of Toronto - School of Continuing Studies	https://lamarr-institute.org/blog/quantum-random-numbers-ml/
9.	3958 - Foundations of DevOps II: Ecosystem, Architecture and Continuous Software Delivery	University of Toronto - School of Continuing Studies	https://learn.utoronto.ca/programs-courses/courses/3958-foundations-devops-ii-ecosystem-architecture-and-continuous-software
10.	Kickstart DevOps Quickly	Stanford University	https://uit.stanford.edu/service/techtraining/class/kickstart-devops-quickly

Course detailed description:

1. The course helps students build practical skills and knowledge in a growing field. The program is closely connected to industry needs, ensuring students learn current practices and tools in DevOps and Software Engineering, including machine learning. The course emphasizes hands-on learning, allowing students to apply their knowledge to real-world projects. The course focuses on modern techniques for software development and operations, preparing students to work on realistic projects in industrial and large-scale settings.
2. The *course focuses on cloud architecture, DevOps practices like CI/CD, IT automation, and enterprise performance architecture, providing a strong technical foundation for careers in cloud and DevOps engineering. Graduates of this course will have specialized knowledge and skills positioning them to compete for sought after roles such as: DevOps engineers, security specialists, it automation engineers.*
3. This program combines DevOps with Cloud Computing and also covers topics like Serverless Computing and Container Orchestration. Students will learn agile working methods through courses like Agile Software Development Techniques and Design Thinking. Other areas of study include Computer Science and Society, Cyber Security and Data Protection, and Cyber Risk Assessment and Management. The program also includes an AI prompt engineering course to teach the student how to use tools like ChatGPT effectively in daily life, work, and studies.

4. This course provides a comprehensive and flexible approach to mastering software engineering, designed to accommodate the needs of professionals balancing career and education. Delivered entirely online, it allows learners to study from anywhere in the world while maintaining their professional commitments. Participants will engage in weekly workshops with course facilitators and live interactive sessions with mentors and peers, fostering a collaborative and supportive learning environment. The curriculum emphasizes practical, real-world application, enabling students to develop their skills through hands-on projects. These projects culminate in a professional portfolio, showcasing their expertise in critical areas of software engineering and preparing them for competitive roles in the job market. Beyond technical competencies, the course also focuses on essential leadership skills, such as effective communication, teamwork, and consultancy, to prepare participants for advanced roles in technology-driven industries. Key technical topics include agile programming for front-end and back-end development, software development and deployment, requirements analysis, data structures and algorithms, software design and architecture, and software security. This program equips learners with the knowledge and skills to excel in both technical and leadership capacities, ensuring they are well-prepared for the evolving demands of the technology sector.

5. This Master of Science in Computing in DevOps offers flexible study options, with the program available as a one-year, full-time course (typically on campus) or a two-year, part-time course (delivered online, contingent on demand). DevOps integrates the practices of development and operations engineers, encompassing the entire service lifecycle from design and development to deployment and production. The program emphasizes the application of developer methodologies to operational systems, reflecting the collaborative nature of DevOps. Core topics include DevOps Software Engineering, Project Management, and Deployment Pipelines. Graduates of this program will be well-equipped to pursue a variety of roles in the IT sector, with opportunities to work for leading multinational companies such as Amazon, Hewlett Packard, and Datahug. Potential career paths include positions such as DevOps Support Engineer, Senior Software Engineer in DevOps, and DevOps Project Manager. This program is designed to meet the growing demand for professionals with expertise in DevOps, providing a pathway to impactful careers both locally and internationally.

6. This course in Software Delivery and DevOps, organized by Eficode and the University of Southern Denmark (SDU), focuses on equipping participants with practical skills and tools commonly used by professional software developers. Participants will gain hands-on experience with technologies such as Git, Docker, and Jenkins, as well as receive valuable insights and best practices for their application. By the end of the course, students will be able to construct and implement a continuous delivery pipeline for small software projects, utilize professional tools for automating builds, tests, and deployments, and adopt a DevOps mindset. Additionally, they will learn to compare Continuous Delivery and DevOps with other software engineering approaches, understanding their prerequisites, benefits, and challenges. The course also explores how continuous delivery supports innovation experiments and value creation, providing a strong foundation in modern software engineering practices. This program is designed to prepare participants for the dynamic requirements of the DevOps and software delivery fields, emphasizing both theoretical understanding and practical application. This course is designed to help organizational leaders, security officers, and IT professionals prepare for the imminent arrival of quantum computing. It focuses on the threat quantum computing poses to current cryptographic systems, as adversaries are already collecting encrypted data that could be decrypted once quantum computers become available. The course emphasizes the

need to adopt Post-Quantum Cryptography (PQC) to secure communications and information assets, and provides strategies for mitigating these emerging risks to organizational security.

7. The University of Chicago offers an eight-week DevOps course that covers essential topics such as deployment, release, versioning, testing, packaging, and cloud computing. Students will gain practical experience with tools like Datadog, Docker, Git, Jenkins, Kubernetes, Linux, Maven, and VMware. The course is intended for individual contributors, engineers, technicians, or other professionals interested in technology who wish to learn about DevOps processes and the software development life cycle. DevOps combines practices and tools that help organizations deliver services and applications faster and more efficiently. It improves the creation and deployment of products compared to traditional methods. In this course, students will learn to integrate key teams and processes to create more value in less time. Upon completing the course, students will be able to implement continuous integration, reduce the time it takes to bring software to market, design a complete infrastructure to deploy, configure, test, and monitor software, and create cloud and virtualization architectures related to DevOps. Graduates will receive a credential from the University of Chicago and join the UChicago network.

8. In this micro course, students will explore the history, values, principles, and philosophy of DevOps. Students will learn how DevOps can help organizations deliver software more efficiently, with greater agility and quality. The course will also cover the kind of culture and structure organizations need to make DevOps successful, as well as how to value the people who contribute to its success. Additionally, students will examine different approaches for seamlessly delivering software products and the processes involved in continuous delivery. Upon successful completion of the course, which typically takes 4-6 weeks, students will receive a micro-credential indicating achievement of the outlined learning outcomes and competencies. These micro-credentials are verifiable, blockchain-based, tamper-proof, and 100% digital. They can be shared on social media platforms like LinkedIn and Facebook, embedded in websites, or downloaded as PDFs. By the end of the course, students will be able to define DevOps and describe its benefits compared to other approaches. Students will also understand the DevOps lifecycle and processes, as well as the differences between Agile and Waterfall software delivery models. Furthermore, students will be able to describe agile techniques such as Lean, Scrum, and Kanban, and understand when and how to apply them. The course will help students develop competencies in Agile methods, including Scrum, Kanban, and Lean, as well as in agile planning, software development, release planning, continuous improvement, cross-collaboration, and change management.

9. This micro course is designed for individuals who already understand DevOps practices and benefits, as well as the organizational changes and structures required for DevOps to succeed. In this course, students will learn about DevOps architecture and the overall DevOps ecosystem. Students will also explore continuous integration, along with other relevant practices and tools. Additionally, career opportunities and DevOps roles in mature organizations will be discussed. Upon successfully completing the course, which typically takes 4-6 weeks, students will receive a micro-credential reflecting their achievement of the learning outcomes and competencies. These micro-credentials are tamper-proof, verifiable, blockchain-based, and 100% digital. They can be shared on social media platforms like LinkedIn and Facebook, embedded in websites, or downloaded as PDFs. By the end of the course, students will be able to describe the DevOps ecosystem and compare different architecture models, such as monolithic and microservices architectures. Students will understand key DevOps concepts, including Configuration Management, Continuous Integration, and Continuous Delivery. Students will also be able to select appropriate test and

deployment strategies and identify best practice tools and applications for implementation. The course will also cover Cloud DevOps, focusing on platforms like Azure, GCP, and AWS. The competencies developed in this course include application architecture, application infrastructure, agile application development, software development, software automation, automation testing and monitoring, cloud infrastructure management, and team collaboration.

10. This course is designed for individuals interested in getting started with DevOps, including Data Engineers, DevOps Engineers, Release Engineers, Database Administrators, Infrastructure Engineers, Software Engineers, and System Administrators. A basic understanding of Linux/Unix and some programming knowledge in Python is required as a prerequisite. By completing this course, students will learn the steps involved in the DevOps methodology, how to use Docker in daily developer or sysadmin roles, and how to deploy applications to Kubernetes. Students will also gain hands-on experience with DevOps tools like Git, Docker, and Jenkins. The course covers the principal concepts and practices in DevOps methodology, including Continuous Integration and Continuous Delivery (CI/CD). Students will learn about the principles of continuous software development, integration, and deployment, and be introduced to tools such as Git, Docker, Jenkins, and Ansible. The course also covers repositories, artifacts, and the CI/CD pipeline, using GitLab as an example. Additionally, Students will learn how to apply DevOps practices on Cloud platforms like Azure, GCP, and AWS.

4. R&D Laboratories

4.1. 5G security laboratories

№	Lab title	Institution	Link
1	Secure 5G4ioT Lab	Oslo Metropolitan University	https://5g4iotlab.com/ https://www.concordia-h2020.eu/secure-5g4iot-lab-5g-cellular-iot/
2	Network Security Lab	University of Technology Sydney	https://www.uts.edu.au/research-and-teaching/our-research/global-big-data-technologies-centre/our-research/iot-communications-and-networking/network-security-lab
3	Networks and Telecommunications Research Lab (NetsLab)	University College Dublin	https://netslab.ucd.ie/
4	SecurityGen 5G Cyber-Security Lab	SecurityGen	https://security-gen.com/5g_cyber_security_lab
5	Network, Information, and Computer Security (NICS) Lab	University of Málaga	https://www.nics.uma.es:8082/
6	S2N (Smart and Secure Networks) Lab	CNIT	https://s2n.cnit.it/
7	Cyber Data Science Laboratory (CyberDataLab)	University of Murcia	https://cyberdatalab.um.es/
8	WiMuNet Research Laboratory	University of Granada	https://wimunet.ugr.es/
9	Infocommunication and Information Technology National Laboratory (InfoLab)	Hungary	https://infolab.nemzetilabor.hu/en

Labs detailed description:

1. **The Secure 5G4ioT Lab** is a unique initiative that focuses on accelerating the development of a secure 5G mobile network capable of accommodating the next wave of communication, namely the communication between billions of Internet of Things (IoT) Devices.

Situated in the premises of the Oslo Metropolitan University, the Secure 5G4IoT Lab (part of the ASN Research Group) focuses on the establishment of 5G and beyond interoperable networks, Cloud infrastructure for mobile communications, Edge computing, Network Slicing, Security and IoT support. Among these traits lays an in-depth knowledge, shared between the research fellows in the lab. The members of the Secure 5G4IoT Lab are continuously working on discovering new and improving existing use cases; i.e., applications for Smart Infrastructure, Smart Homes, Industrial, Automotive, Healthcare sectors, etc. The Secure 5G4IoT Lab is actively publishing new papers and attending relevant conferences in the field

To accomplish its mission Secure 5G4IoT lab has identified the following research areas:

- Virtualization of the mobile network
- Isolated Adaptable Network slices
- Cross-layer security using AI and Machine learning
- Cross-layer Identity Management for IoT; Unification of IoT verticals

2. The **Network Security Lab** at the University of Technology Sydney (UTS) is part of the Global Big Data Technologies Centre (GBDTC). The lab specializes in network security research, focusing on the Internet of Things (IoT), 5G, and emerging communication networks. Lab explores innovative solutions for secure data transmission, privacy protection, and resilient network architectures. The lab collaborates with industry partners and academic institutions to develop cutting-edge security frameworks, ensuring the integrity and reliability of modern and future communication systems.

3. The **Networks and Telecommunications Research Lab (NetsLab)** at University College Dublin focuses on advanced research in networking, with a significant emphasis on 5G technologies and beyond. The lab addresses challenges in wireless communications, software-defined networking (SDN), network function virtualization (NFV), and 5G security. Research efforts include the development of innovative solutions for secure, scalable, and efficient communication systems in 5G and future networks. NetsLab collaborates with academic, industrial, and governmental partners to drive advancements in cutting-edge telecommunications technologies.

4. The **SecurityGen 5G Cyber-Security Lab** is a specialized platform launched to advance research, training, and innovation in 5G security. This state-of-the-art facility is designed to help telecom security teams understand the unique challenges and threats of 5G networks. The lab offers tools to test vulnerabilities, simulate threat scenarios, and develop robust security measures. It serves as a resource for improving security awareness, enhancing technical expertise, and creating custom solutions for protecting 5G infrastructures.

5. The **Network, Information, and Computer Security (NICS) Lab** at the University of Málaga is a prominent research group specializing in cybersecurity across advanced and emerging technologies. One of its key focus areas is **5G Security**, where the lab explores innovative solutions to address vulnerabilities in 5G networks, including the protection of critical communication infrastructures, secure service orchestration, and privacy-preserving mechanisms for 5G-enabled environments. Research also includes ensuring trust in software-defined networks (SDN) and network function virtualization (NFV) integral to 5G systems.

Beyond 5G, the lab works on IoT security, blockchain technologies, and critical infrastructure protection, collaborating with academic, industrial, and governmental organizations to drive advancements in secure and resilient systems.

6. The **S2N (Smart and Secure Networks) Lab** at CNIT focuses on innovative research and development in the areas of network security, privacy, and intelligent networking, with a strong emphasis on 5G and beyond. The lab is dedicated to enhancing the security and resilience of modern communication systems, addressing challenges such as 5G security architectures, intrusion detection, and network function virtualization (NFV) protection.

Key research areas include:

- **5G and Beyond Security**: Developing secure protocols and frameworks for 5G networks, with a focus on protecting network slicing, SDN, and NFV.
- **IoT and Cyber-Physical Systems**: Securing IoT devices and critical infrastructures connected via 5G networks.
- **Artificial Intelligence for Security**: Leveraging AI and machine learning for detecting and mitigating network attacks in real-time.

Through its multidisciplinary approach and collaborations with academia, industry, and governmental organizations, the S2N Lab aims to provide cutting-edge solutions for smarter and more secure networked systems.

7. The **Cyber Data Science Laboratory (CyberDataLab)** at the University of Murcia is a leading research center specializing in cybersecurity, data science, and next-generation network technologies, including **5G security**. The lab focuses on the intersection of machine learning, artificial intelligence, and cybersecurity to develop innovative solutions for protecting critical infrastructures and emerging technologies.

Key focus areas:

- **5G Security**: Research on securing 5G networks, including mitigating vulnerabilities in network slicing, edge computing, and IoT devices connected via 5G.
- **Artificial Intelligence and Cybersecurity**: Leveraging AI to detect and respond to cyber threats in real-time, enhancing the resilience of communication systems.
- **Privacy and Data Protection**: Ensuring compliance with data protection regulations and developing privacy-preserving technologies for modern digital infrastructures.
- **Collaboration and Impact**: Engaging with academic, governmental, and industrial partners to deploy practical solutions for secure and efficient communication systems.

The lab actively contributes to the global research community by developing state-of-the-art technologies to address emerging challenges in cybersecurity and data science, particularly within the rapidly evolving **5G ecosystem**.

8. The **WiMuNet Research Laboratory** at the University of Granada specializes in wireless communications and networking, focusing on cutting-edge research in **5G technologies**, **IoT**, and **cybersecurity**. The lab is dedicated to advancing wireless network design, optimization, and security to meet the challenges of modern communication systems.

Key focus areas:

- **5G Security and Resilience**: Developing robust protocols to secure 5G networks, addressing vulnerabilities in network slicing, SDN/NFV, and edge computing. Research includes protecting against cyberattacks and ensuring data integrity in high-speed, low-latency environments.

- **Wireless Networks Optimization**: Enhancing the performance of wireless communication systems, including 5G, through advanced algorithms for resource allocation and interference management.
- **IoT and Sensor Networks**: Innovating secure and efficient communication frameworks for IoT ecosystems and smart environments powered by 5G.
- **Collaboration and Real-World Applications**: Partnering with industry and academia to apply research findings in fields such as healthcare, smart cities, and industrial automation.

The WiMuNet Lab combines theoretical research and practical applications to push the boundaries of wireless communication technologies, with a strong commitment to addressing the evolving security needs of 5G and beyond.

9. The **Infocommunication and Information Technology National Laboratory (InfoLab)** in Hungary focuses on the secure implementation of emerging technologies and supports the digital transformation of public administration. A key area of their research is **5G security**, where they analyze protocols used in future mobile networks, specifically the "New Radio (NR)" standard. Their goal is to ensure high-level data protection and secure operation of 5G systems, preventing information leaks and unauthorized access. citeturn0search1

InfoLab's cybersecurity research emphasizes real-time vulnerability detection and management. They assess threats to IT systems and develop strategies to mitigate potential risks, enhancing the resilience of critical infrastructures. citeturn0search20

In the realm of artificial intelligence, InfoLab explores AI-based solutions for e-government. Their research aims to automate administrative processes, reduce the need for redundant data provision by citizens, and create seamless, contactless digital services. citeturn0search21

By collaborating with academic institutions, industry partners, and government agencies, InfoLab contributes to the development of secure and efficient digital solutions, ensuring the safe application of 5G and future technologies. citeturn0search23

4.2. Quantum R&D Labs

#	Lab Title	Institution	Link
1	AI OILab - Quantum Computing	Oxford	https://www.aioilab-oxford.eu/quantum-computing
2	Oxford Quantum Circuits - R&D	Oxford	https://oqc.tech/tech/research-and-development/
3	Quantum Computing Laboratory	University of Porto	https://dei.fe.up.pt/qclab/
4	Quantum Computing Centre	Masaryk University	https://qicz.fi.muni.cz/
5	Deep Tech Lab	BioInnovation Institute	https://deeptechlab.bii.dk/
6	Quantum Lab	University of Luxembourg	https://www.uni.lu/snt-en/research-groups/apsia/quantum-lab/
7	Quantum Software Lab	University of Edinburgh	https://www.quantumsoftwarelab.com/

8	Applied Cyber Security Quantum Lab	Lucerne School of Information Technology	https://www.hslu.ch/en/lucerne-school-of-information-technology/research/labs/applied-cyber-security/quantumlab/
9	Nano and Quantum Technologies Lab	Wrocław University of Science and Technology	https://www.nlqt.wppt.pwr.edu.pl/
10	Quantum Lab Italy	Sapienza University of Rome	https://www.quantumlab.it/
11	Quantum Hacking and Certification Lab	University of Vigo	https://vqcc.uvigo.es/groups/quantum-hacking-and-certification-lab/
12	Quantum Engineering Technology Labs	University of Bristol	https://www.bristol.ac.uk/qet-labs/
13	QuTech	Delft University of Technology	https://qutech.nl/
14	Quantum Nanoscience Lab	ETH Zurich	https://qns.ethz.ch/
15	PhotonLab	Max Planck Institute for Quantum Optics	https://www.mpq.mpg.de/photonlab-en
16	Research Unit on Neuromorphic Computing and Photonics (RNCP)	University of the Aegean and University of West Attica	https://rncp.eu/
17	Quantum Applications and Research Laboratory (QAR-Lab)	Ludwig Maximilian University of Munich	https://qarlab.de/en/category/qar-lab-en/

Labs detailed description:

1. **AI OILab - Quantum Computing**

Located in Oxford, United Kingdom, the AI OILab focuses on the intersection of artificial intelligence and quantum computing. Their research aims to develop quantum algorithms that enhance machine learning processes, exploring how quantum computing can solve complex AI problems more efficiently than classical methods. The lab is equipped with quantum simulators and access to quantum processors through cloud-based platforms, enabling the testing and implementation of quantum algorithms in real-world scenarios.

2. **Oxford Quantum Circuits - Research and Development**

Based in the UK, Oxford Quantum Circuits (OQC) specializes in designing and building quantum hardware. Their R&D focuses on developing scalable superconducting quantum circuits, aiming to create more stable and error-resistant qubits. OQC's facilities include state-of-the-art fabrication equipment for creating superconducting qubits and dilution refrigerators that cool quantum processors to millikelvin temperatures, essential for maintaining qubit coherence.

3. **Quantum Computing Laboratory, University of Porto**

Situated in Porto, Portugal, this lab is part of the Faculty of Engineering at the University of Porto. Their research encompasses quantum algorithms, quantum cryptography, and quantum information theory. The laboratory is equipped with quantum programming environments and

access to quantum annealers, facilitating the development and testing of quantum algorithms for various applications.

4. **Quantum Information Group, Masaryk University**

Located in Brno, Czech Republic, the Quantum Information Group at Masaryk University focuses on quantum information processing, including semi-device independent protocols, Bell inequalities, and quantum cryptography. Their research also delves into randomness extraction and applications. The group utilizes quantum simulators and has access to quantum communication devices for experimental validation of theoretical models.

5. **Deep Tech Lab - Quantum, BioInnovation Institute**

Based in Copenhagen, Denmark, Deep Tech Lab – Quantum is an initiative by the BioInnovation Institute. It supports early-stage startups developing quantum technologies with potential life science applications. The lab provides funding, mentorship, and infrastructure to help startups transition from research to commercial viability. Facilities include access to quantum computing resources and collaboration spaces designed to foster innovation.

6. **Quantum Lab, University of Luxembourg**

Part of the University of Luxembourg's Interdisciplinary Centre for Security, Reliability, and Trust, this lab focuses on applied security in quantum information. Research areas include quantum key distribution, quantum cryptography, and the development of quantum-resistant algorithms. The lab is equipped with quantum communication systems and classical computing resources to simulate and test quantum security protocols.

7. **Quantum Software Lab, University of Edinburgh**

Affiliated with the University of Edinburgh, the Quantum Software Lab is dedicated to developing quantum-enhanced solutions that are demonstrable, verifiable, and co-designed for emerging quantum hardware. Their research areas include quantum algorithms, machine learning, quantum cybersecurity, and programming architectures. The lab comprises over 50 researchers and collaborates with more than 18 partners, contributing to over 130 publications.

8. **Applied Cyber Security Quantum Lab, Lucerne School of Information Technology**

Located in Switzerland, this lab is part of the Applied Cyber Security Research Lab. It conducts applied research related to quantum cryptography, quantum-safe security, and quantum computing. The lab provides infrastructure and services related to these topics, including quantum random number generators and post-quantum algorithm testing environments.

9. **Nano and Quantum Technologies Lab, Wrocław University of Science and Technology**

Situated in Poland, this national laboratory focuses on quantum technologies, including quantum cryptography, photovoltaics, and quantum modeling. The lab is equipped with systems for quantum key distribution, Raman spectrometers, atomic force microscopes, and computational clusters for quantum modeling. It actively collaborates with leading scientific centers in quantum cryptography.

10. **Quantum Lab, Sapienza University of Rome**

Based in Italy, the Quantum Lab at Sapienza University conducts research in quantum information, quantum foundations, and quantum technologies. Their laboratories focus on areas such as quantum simulations, quantum communications, and photonics of spin–orbit optical phenomena. The lab is equipped with advanced photonic systems and quantum communication devices.

11. **Quantum Hacking and Certification Lab, University of Vigo**

Located in Spain, this lab focuses on testing the practical security of quantum communication systems, identifying potential loopholes, and developing countermeasures. The lab contributes

to certification standards for quantum communication systems and their components. It is equipped with tools for security analysis and testing of quantum key distribution systems.

12. Quantum Engineering Technology Labs, University of Bristol

Based in the UK, QET Labs pioneers science and technology for the quantum age. They translate ideas into experiments that prototype hardware for quantum computing, simulation, imaging, sensing, and communication. A key technology platform is integrated quantum photonics, invented in Bristol. The lab is equipped with state-of-the-art fabrication facilities and quantum photonic devices.

13. QuTech, Delft University of Technology

QuTech is a collaboration between Delft University of Technology and TNO (Netherlands Organization for Applied Scientific Research). It focuses on developing scalable quantum computing and quantum communication systems. Their primary mission includes the creation of a quantum internet and scalable fault-tolerant quantum computers. Key research areas include quantum algorithms, quantum error correction, and quantum network protocols. QuTech is known for its advanced quantum hardware, including superconducting qubit systems and nanofabrication facilities. They employ dilution refrigerators to cool qubits to near absolute zero and have dedicated setups for testing quantum entanglement and coherence in communication channels.

14. Quantum Nanoscience Lab, ETH Zurich

The Quantum Nanoscience Lab at ETH Zurich is dedicated to studying quantum phenomena in nanoscale systems. Research spans from quantum information processing and quantum sensing to exploring materials for quantum device development. Their work often bridges theoretical insights with experimental applications in solid-state quantum systems. The lab is equipped with state-of-the-art nanofabrication facilities for creating solid-state qubits, high-precision measurement instruments for quantum sensing, and cryogenic equipment to maintain the extremely low temperatures required for quantum experiments. They also utilize advanced spectroscopy tools for material characterization and quantum device testing.

15. PhotonLab, Max Planck Institute for Quantum Optics

PhotonLab is dedicated to educating students about quantum physics and optics. They have developed a QRNG experiment that allows students to explore quantum randomness by observing the behavior of photons at a beam splitter. This hands-on approach helps in understanding the fundamental principles of quantum mechanics and randomness. The lab utilizes laser sources, beam splitters, photon detectors, and polarization rotators to demonstrate QRNG concepts.

16. Research Unit on Neuromorphic Computing and Photonics (RNCP), University of the Aegean and University of West Attica

RNCP specializes in photonic neuromorphic computing systems and their applications, including the development of secure pseudo-random generators based on quantum-mechanical processes. Their research aims to create non-replicable authentication tokens and secure QRNGs for integration into Internet of Things (IoT) ecosystems, enhancing resilience against cyber-physical attacks. The unit develops optical modules serving as authentication tokens and secure QRNG devices, combining neuromorphic engineering and cryptographic systems to produce advanced electronic-photonic neuro-cryptographic devices.

17. Quantum Applications and Research Laboratory (QAR-Lab), Ludwig Maximilian University of Munich

The Quantum Applications and Research Laboratory (QAR-Lab) at LMU Munich is a premier hub for advancing quantum computing technologies and their practical applications. Established in 2016 under the leadership of Professor Dr. Claudia Linnhoff-Popien, QAR-Lab

bridges the gap between theoretical research and industrial needs. The lab specializes in quantum-assisted optimization, machine learning, and AI, enabling breakthroughs in solving complex problems across diverse fields such as logistics, finance, and healthcare. It also pioneers middleware solutions, such as the Universal Quantum Optimizer (UQO), for architecture-independent programming, which simplifies quantum application development across different hardware platforms.

4.3. AI/ML R&D Lab

№	Lab Title	Institution	Link
1	MOSAIC Lab	Aalto University	https://mosaic-lab.com/
2	European Laboratory for Learning and Intelligent Systems (ELLIS)	Various Institutions	https://ellis.eu/
3	Munich Center for Machine Learning (MCML)	Ludwig Maximilian University of Munich and Technical University of Munich	https://mcml.ai/
4	EURECOM	EURECOM Consortium	https://www.eurecom.fr/en/
5	Laboratory for AI Security Research (LASR)	University of Oxford	https://www.ox.ac.uk/news/2024-12-04-oxford-university-lead-ai-security-research-through-new-national-laboratory
6	AI and Cybersecurity Lab	University of Edinburgh	https://informatics.ed.ac.uk/eliai
7	Centre for Telecommunications Research	King's College London	https://www.kcl.ac.uk/research/ctr
8	Networked Systems Security Group	KTH Royal Institute of Technology	https://nss.proj.kth.se/
9	Cybersecurity and AI Group	University of Luxembourg	https://www.uni.lu/snt-en/research/
10	Security and Privacy Group	ETH Zurich	https://ethz.ch/en/research/research-infrastructure.html

AL/ML Labs detailed description:

1. MOSA!C Lab focuses on mobile network softwarization and service customization, aiming to create an autonomous telco cloud. The lab strives to improve the efficiency, adaptability, and resilience of mobile networks to address the challenges posed by 5G and beyond.

This lab specializes in zero-touch network orchestration and automated cloud management. It employs advanced AI/ML algorithms to optimize resource allocation, ensure quality of service (QoS), and automate maintenance. Its technical infrastructure includes cloud-native platforms, SDN (Software-Defined Networking) technologies, and NFV (Network Function Virtualization) environments.

The MOSA!C Lab conducts projects related to network virtualization, edge computing, and autonomous network management. It actively collaborates with international partners on EU-funded projects. The lab is known for its research on predictive network control, AI-driven QoS optimization, and secure 5G communications.

2. European Laboratory for Learning and Intelligent Systems (ELLIS) aims to advance the state of AI research in Europe by focusing on excellence in machine learning, robotics, and intelligent systems. The laboratory strives to drive scientific breakthroughs and ensure Europe remains competitive in the global AI race.

ELLIS is structured as a network of units operating across various European institutions, each focused on specific research domains such as deep learning, reinforcement learning, and computer vision. It leverages high-performance computing clusters, cloud-based AI infrastructures, and collaborative research platforms.

ELLIS conducts research in a wide range of AI-related fields, including machine learning, computer vision, and natural language processing. It also explores the ethical implications of AI, AI safety, and fairness. The lab provides PhD training programs, summer schools, and collaborative research opportunities. ELLIS is actively involved in developing explainable AI (XAI) solutions for critical systems.

3. Munich Center for Machine Learning (MCML). The mission of MCML is to advance fundamental research in machine learning while fostering collaboration across different scientific domains. It aims to develop new AI models, algorithms, and applications for industrial and societal challenges.

MCML has access to powerful supercomputing resources and high-performance AI training platforms. The lab employs deep learning frameworks like TensorFlow and PyTorch to develop innovative ML models. Its infrastructure also includes facilities for large-scale data processing and real-time analysis.

The lab conducts research on robust machine learning, adversarial attacks on AI systems, and secure data analytics. It is actively involved in projects focusing on privacy-preserving AI, human-AI collaboration, and anomaly detection. MCML works closely with industry partners to co-develop AI solutions for real-world applications, particularly in telecommunications, healthcare, and smart manufacturing.

4. EURECOM focuses on digital security, data science, and communication systems to create innovative solutions for next-generation networks, including 5G and beyond. The lab aims to enhance network resilience and develop secure communication protocols.

EURECOM provides access to a 5G testbed, security testing frameworks, and advanced machine learning models for security analysis. It uses SIEM (Security Information and Event Management) systems, network traffic analysis tools, and AI-driven threat detection engines.

EURECOM's research focuses on AI-based threat detection, intrusion detection systems (IDS), and secure communication protocols. It also explores privacy-preserving AI models, federated learning, and machine learning for security automation. EURECOM partners with industry leaders and governmental bodies to create tools for real-time threat detection and response in 5G environments.

5. Laboratory for AI Security Research (LASR). The mission of LASR is to create secure and trustworthy AI systems. The lab focuses on protecting AI models from adversarial attacks and ensuring ethical deployment in critical infrastructure.

The laboratory is equipped with high-performance AI infrastructure, GPU clusters, and environments for testing adversarial machine learning (AML). LASR focuses on secure model training, explainable AI (XAI), and safe deployment of AI-driven solutions.

The lab's main research areas include AI vulnerability detection, adversarial robustness, and the ethical use of AI in critical sectors such as finance and healthcare. LASR collaborates with policymakers and industry leaders to develop guidelines for the responsible use of AI. It also focuses on cybersecurity solutions to protect AI models against data poisoning and adversarial input attacks.

6. AI and Cybersecurity Lab. The mission of this lab is to bridge AI technologies with cybersecurity practices. The lab aims to create AI-driven models that enhance threat detection and automate cyber defense.

The lab's technical environment includes a secure, isolated environment for analyzing cyber threats and experimenting with AI models for anomaly detection and predictive threat analysis. The lab also uses advanced data visualization and network monitoring tools.

Research areas include AI-driven threat intelligence, automated threat detection, and anomaly detection. The lab explores the development of explainable AI (XAI) tools to support security analysts. It also works on models for predictive attack prevention in 5G networks.

7. Centre for Telecommunications Research. The mission of the center is to advance telecommunications technologies with a focus on 5G and beyond. It aims to secure communication channels and enable AI-enhanced network management.

The center operates state-of-the-art telecommunications facilities, 5G testbeds, and advanced network emulators. It supports real-time traffic analysis, machine learning for network optimization, and simulation of next-generation networks.

The lab's research includes network security, automated network slicing, and anomaly detection. It works on AI-powered network optimization, resilience mechanisms, and resource management in 5G and beyond networks.

8. Networked Systems Security Group focuses on secure networked systems, emphasizing AI-driven approaches to network security and resilience. Its mission is to create robust, self-defending networks.

The lab offers network simulators, security analytics platforms, and tools for real-time attack detection. It uses big data analytics to monitor and secure IoT devices and networked systems.

Research focuses on anomaly detection, AI-driven malware detection, and network traffic analysis. The lab works on federated learning models to ensure security in distributed AI systems. It also collaborates with industry on securing IoT devices and edge networks.

9. Cybersecurity and AI Group. The mission of this lab is to develop AI methodologies to address key cybersecurity challenges, particularly in protecting critical infrastructures.

The group operates in a secure laboratory with access to dedicated cyber ranges, SIEM systems, and advanced data visualization tools. It also utilizes privacy-preserving AI models to ensure the security of sensitive information.

Research includes the development of AI-driven threat intelligence, federated learning for cybersecurity, and privacy-aware machine learning models. It focuses on proactive threat detection and the development of predictive analytics tools.

10. Security and Privacy Group aims to protect user privacy and system security in AI-driven technologies. The main goal is to design secure AI models that are privacy-compliant and robust against adversarial attacks.

The group has access to GPU clusters and data privacy testing environments. It focuses on building encrypted AI pipelines and secure federated learning models.

The group works on privacy-enhancing technologies, secure AI models, and secure federated learning. It explores the trade-offs between model accuracy and privacy and develops methods to protect against model inversion and membership inference attacks.

Conclusions

The survey highlights the European Union's proactive and comprehensive efforts to address the security challenges of 5G and beyond networks. The key conclusions drawn from this analysis are as follows:

1. Strategic vision and regulatory leadership. The EU's integrated approach to 5G and emerging 6G technologies demonstrates its commitment to fostering secure digital transformation. Regulatory initiatives such as the EU AI Act and the transition to post-quantum cryptography reflect a forward-looking strategy.

2. Innovation through R&D projects. EU-funded research projects play a pivotal role in developing novel security solutions for 5G networks. These projects offer valuable models for collaboration and innovation.

3. Importance of education and training. Academic programs and study courses provide the necessary skills and knowledge for building a workforce capable of tackling 5G security challenges. These programs emphasize practical applications of AI/ML, quantum technologies, and DevSecOps methodologies.

4. Cutting-edge research infrastructure. Dedicated R&D laboratories across Europe are advancing the security of 5G networks through experimental research and applied solutions.

5. Global relevance. The EU's practices and frameworks offer scalable solutions and can inspire international efforts to enhance the security and resilience of digital infrastructure.

By leveraging the EU's comprehensive approach, other countries, like Ukraine and Georgia, can strengthen their digital resilience, ensuring secure adoption of next-generation networks.