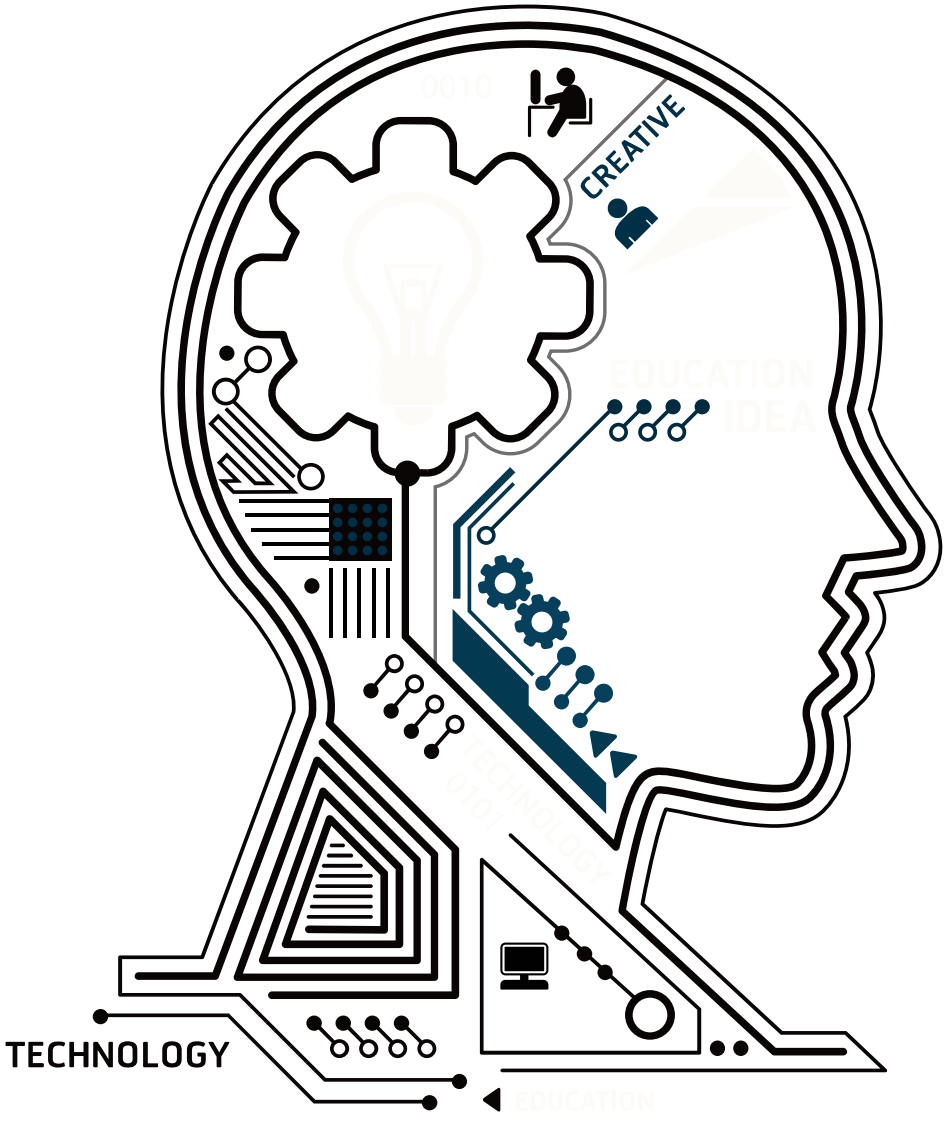
ITU Centres of Excellence for Europe

Training opportunities

2021



The Abdus Salam International Centre for Theoretical Physics

National Institute of Telecommunications

Technische Hochschule Brandenburg University of Applied Sciences Institute for Security and Safety

NRD Cyber Security

ITUAcademy
Empowering minds

Table of Content

OVERVIEW OF CoE INITIATIVE

The Centres of Excellence (CoE) programme was launched by the International Telecommunication Union (ITU) at the turn of the millennium, aiming to support capacity building in the field of ICTs. Designed to offer continuous education to ICT professionals and executives in the public and private spheres, the Centres serve as regional focal points for professional development, research, and knowledge sharing, as well as provide specialist training services to external clients. With the support from multilateral and regional organizations, CoE networks have been established in a number of regions including Africa, the Americas, Arab States, Asia-Pacific, Commonwealth of Independent States (CIS) and Europe. The network is composed of 29 Centres across the globe, six each in the Africa and Europe regions, five in the Americas and Asia & Pacific regions, four in the Arab region and one in the CIS region.

CENTRES OF EXCELLENCE FOR EUROPE

The second cycle of the new Centres of Excellence programme started in January 2019 and will end in December 2022. A total of 29 institutions were selected to operate as Centres of Excellence during this period. The following institutions were selected in Europe to provide trainings in particular six priority areas.

	Name of Institution	Country	Priority areas
	Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University, Skopje (FEEIT)	North Macedonia	Wireless & Fixed Broadband
Technische Hochschule Brandenburg University of Applied Sciences Institute for Security and Safety	Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences	Germany	Cybersecurity
National Institute of Telecommunications	National Institute of Telecommunications (NIT)	Poland	Internet Governance Wireless & Fixed Broadband
NRD Cyber Security	NRD Cyber Security (NRD CS)	Lithuania	Cybersecurity
ICTP The Abdus Salam International Centre for Theoretical Physics	The Abdus Salam International Centre for Theoretical Physics (ICTP)	Italy	Internet of Things Big Data & Statistics

SCOPE

This catalogue has been produced by the ITU Office for Europe in collaboration with five ITU Centres of Excellence in Europe to highlight and promote the capacity building courses provided by the centres.

While participation is open to applicants from all countries, stakeholders from the Member States of the Europe region (as defined at ITU) are primarily encouraged to participate in the courses. These countries are Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Georgia, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, North Macedonia, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, Vatican City State and the United Kingdom.

The courses aim to increase participants' understanding, knowledge and awareness in the following areas:

- Wireless & fixed broadband
- Digital broadcasting
- Cybersecurity
- Internet governance
- Big data & statistics
- Internet of things

Courses are provided either face to face or online – via the ITU Academy e-learning platform.

All courses have a test component. A certificate of achievement is given to candidates who successfully complete the end-of-course assessment(s).

Information on the registration process and payment methods can be found on the ITU Academy website: academy.itu.int

Changes in course dates may occur and are reflected on the ITU Academy website: academy.itu.int

TRAININGS OFFERED BY ITU CoEs FOR EUROPE

In 2021 the ITU Centres of Excellence for Europe is offering 21 trainings. Three different kind of courses are provided. Face-to-face courses (in blue), online courses (in yellow), self-paced courses (in green). Trainings are presented in chronological order with online and self-paced courses presented first, followed by all face-to-face courses. **Please note that due to the Covid-19 Pandemic, the information in this catalogue is subject to change as the situation in Europe and the greater world continues to evolve.*

NO.	Training course topic	CoE	Dates	Venue	Training fee	Type of training
1.	Strategic aspects for internet governance and innovations	NIT	1-8 February	ITU Academy Platform	150 USD	Online
2.	Cyber incident response	ISS	1 March-31 December	ITU Academy platform	249 USD	Online
3.	Cybersecurity techniques	ISS	1 March-31 December	ITU Academy platform	249 USD	Online
4.	Information security management system	ISS	1March-31 December	ITU Academy platform	249 USD	Online
5.	Wireless access technologies to internet network	NIT	8-15 March	ITU Academy Platform	150 USD	Online
6.	Security and OoS in internet network	NIT	12-19 April	ITU Academy Platform	150 USD	Online
7.	Building an effective cybersecurity team	NRD-CS	19-22 April	Vilnius, Lithuania	800 USD	Online
8.	Future broadband: ultra-broadband Internet, clouds, IoT and artificial intelligence	FEEIT	25 May-21 June	ITU Academy platform	150 USD	Online
9.	Data Privacy, Security & Governance	ICTP	1 June – 7 July	ITU Academy platform	150 USD	Online
10.	Speech and Natural Languages Processing	ICTP	1-30 June	ITU Academy platform	150 USD	Online
11.	Cyber Risk Management	ISS	1 June- 31 December	ITU Academy platform	249 USD	Online
12.	5G technologies for IoT	ICTP	7-8 June	ITU Academy platform	150 USD	Online
13.	Legal, regulatory and technical aspects of cloud computing in international data transfers	NIT	14-21 June	ITU Academy Platform	150 USD	Online
14.	Technical, business and regulatory aspects of 5G networks	NIT	23-30 August	ITU Academy Platform	150 USD	Online
15.	QoS technologies and regulation for fixed and mobile	NIT	27 September-4 October	ITU Academy Platform	150 USD	Online
16.	Applications of satellite based IoT networks	ICTP	15-16 November	ITU Academy platform	150 USD	Online

17.	Future mobile and wireless broadband: LTE-A-Pro, WiFi, satellites, 5G NR and AI	FEEIT	16 November-13 December 2021	ITU Academy platform	150 USD	Online
18.	Legal aspects of artificial intelligence in business, household and public sector	NIT	6-13 December	ITU Academy Platform	150 USD	Online
19.	Industrial cybersecurity and incident response	ISS	20-22 September	ISS, Ettlingen, Germany	999 USD	TBA
20.	Key aspects and governance of internet of things, big data, and artificial intelligence	NIT	28-29 October	Warsaw, Poland	500 USD	TBA
21.	Incidence response practice	NRD-CS	8-11 November	Vilnius, Lithuania	800 USD	TBA

STRATEGIC ASPECTS FOR INTERNET GOVERNANCE AND INNOVATIONS

| 1-8 February 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

1 February 2021

COURSE CODE

21OI26392EUR-E

Description:

Internet and Internet Protocol (IP) have become the norm for digital communications. Good understanding of the IP world requires not only knowledge of the technical and technological aspects of IP, but also strategic, political business issues. The course aims at presenting the current process of innovation in Internet from these perspectives.

Audience:

The course is addressed to corporate executives and managers, policy makers, regulators, i.e. middle-level managers, administrators, officials and engineers dealing with planning, developing, implementing and managing current and future telecom networks.

Trainer:

Prof. Dr. Toni Janevski

CYBER INCIDENT RESPONSE

| 1 March – 31 December 2021 |

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE

English

FEES

249 USD

MODE

Online

DURATION

Flexible (about 4 weeks)

REGISTRATION DEADLINE

No deadline

COURSE CODE

21OI26411EUR-E

The course will provide students with all necessary knowledge of cyber incident response activities, what are main goals and challenges, and explaining main roles and responsibilities in such important process.
They will get most up to date trends in this area with an emphasis on most important details of each cyber incident response stage.
Upon the successful completion of this course, students will be able take a part in development and implementation of cyber incident plan.
Students will have three months to complete the course. After this time, registrations will be reopened for new participants.

Audience:

Security engineers, computer security specialists, computer incident response plan participants, line managers, security consultants.

Trainer:

Dmytro Cherkashyn

CYBERSECURITY TECHNIQUES

| 1 March – 31 December 2021 |

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE

English

FEES

249 USD

MODE

Online

DURATION

Flexible (about 4 weeks)

REGISTRATION DEADLINE

No deadline

COURSE CODE

21OI26410EUR-E

This online course will provide theoretical and practical knowledge of it and cyber security and security methods for computer, network and electronic communication.
The course consists of various chapters and will cover fundamentals, such as IT versus ICS, threats and their sources, authentication, computer access control, cryptography, network security, network firewall concepts, intrusion detection.
The student will get a comprehensive view on security in the cyber space.
Students will have three months to complete the course. After this time, registrations will be reopened for new participants.

Audience:

Everybody working in the cyber as well as isolated computer environment.

Trainer:

Dmytro Cherkashyn

INFORMATION SECURITY MANAGEMENT SYSTEM

| 1 March – 31 December 2021 |

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE

English

FEES

249 USD

MODE

Online

DURATION

-

REGISTRATION DEADLINE

No deadline

COURSE CODE

21OI26476EUR-E

This online course will provide an introduction into ISO 27000 standard information security series as well as advanced theoretical knowledge and practical examples of development, integration as well as operation of ISMS according to ISO 27001 international standard.
Students will learn about information security-related processes like risk management, areas of standard application and necessary controls along with annex A to ISO 27001, which is compliance-related.
Students will have three months to complete the course. After this time, registrations will be reopened for new participants.

Audience:

Computer security specialists, security consultants, internal auditors, compliance specialists.

Trainers:

Dmytro Cherkashyn, Swantje Westpfahl

WIRELESS ACCESS TECHNOLOGIES TO INTERNET NETWORK

| 8-15 March 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

8 March 2021

COURSE CODE

21OI26403EUR-E

Description:

Internet and IP protocol is the winning technology in current telecommunications world. “Over IP” is the concept that can be considered in the context of almost all today’s telecommunications services. Current users want to have access to any telecommunications services, from any plays, and at any moment. That is why mobility and wireless access to Internet plays such an important role.

The course aims at presenting the key aspects of the current most important wireless access technologies to this Internet world.

Audience:

The course is addressed to corporate executives and managers, policy makers, regulators, i.e. middle-level managers, administrators, officials and engineers dealing with planning, developing, implementing and managing current and future telecom networks.

Trainer:

Prof. Dr Toni Janevski

SECURITY AND QOS IN INTERNET NETWORK

| 12-19 April 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

12 April 2021

COURSE CODE

21OI26404EUR-E

Description:

This course will focus on Security and Quality of Service (QoS) in Internet network from technology, regulation and business aspects. It will cover Internet fundamentals, including Internet protocols and architectures, Internet security standards and approaches as defined by IETF (Internet Engineering Task Force), as well as ITU's security architectures for end-to-end communications. Further, the course will incorporate cybersecurity approaches from the ITU viewpoint, and security aspects of emerging cloud computing and Internet of Things (IoT). Further, the course will incorporate Internet QoS, including the standardized solutions and practical approaches for provision of end-to-end QoS. In that manner it will cover QoS parameters as defined by the ITU and QoS for data (i.e., Over-The-Top services) and mobile services. Finally, the course will include network neutrality, Internet KPIs (Key Performance Indicators) and their measurements.

Audience:

This course is targeted at managers, engineers and employees from regulators, government organisations, telecommunication companies and academia, who are interested in understanding, implementation and regulation of Security and QoS in Internet Network, including technologies, standardization, regulation and content. Other institutions and individuals that are dedicated in building their capacity related to Security and QoS in Internet Network are also welcome to participate.

Trainer:

Prof. Dr Toni Janevski

BUILDING AN EFFECTIVE CYBERSECURITY TEAM

| 19 – 22 April 2021 |

ORGANISED BY

NRD Cyber Security

LANGUAGE

English

FEES

800 USD

MODE

Online

DURATION

4 days

REGISTRATION DEADLINE

10 April 2021

COURSE CODE

21OI26398EUR-E

Description:

Continuous growth and reliance on Information Communication and Technologies (ICT) results not only in benefits to organizations, but also in cyber incidents, which threatens ICT infrastructure and sensitive data inside it. The ability to timely detect, mitigate and recover from cyber incidents is a crucial capability to organizations, established and managed within Computer Security Incident Response Teams (CSIRTs/CERTs/CIRTs) and Security Operation Centers (SOCs), thereafter - cybersecurity team.

The course dives deep into CSIRT/SOC establishment practice, where combination of theory, unique experience with lessons learned, and hands-on practice give attendees a clear and actionable picture on how to build an effective cybersecurity team.

This training helps to successively prepare for cyber security team establishment and answers the main questions raised before starting:

- How to build an effective cybersecurity team? Overview, discussion, and practice about a mandate, governance, team and its structure, timeline, lessons learned from similar establishments, financial planning.
- What services in addition to incident management to introduce and how? Applied mandatory and complimentary services, best international practice for services models, incident management, incident management workflows and variations.
- What is technology behind it? Scrutiny of principal architecture for CSIRT stack, integrations and managerial (not technical) look into technologies, automation vs manual, and technology trends.
- How to mature security services and when? Elaboration of KPIs, SLAs and related metrics, security briefings, weekly/monthly/quarterly/yearly reports, analysis of examples and exercises on how to plan improvements for security services provided.
- What is the baseline for it? Presentation of best international models measuring the maturity of cybersecurity team and its various components, advice on how to use them and how they help in operational environment.

Audience:

The course is designed for non-technical professionals who are or will be responsible for cybersecurity teams/CSIRT/CERT/SOC establishment, management and growth in governmental and private sectors.

Trainer:

Vilius Benetis, CSIRT/SOC architect, cybersecurity incident handling expert, researcher practitioner, CEO of NRD Cyber Security

FUTURE BROADBAND: ULTRA-BROADBAND INTERNET, CLOUDS, IOT AND ARTIFICIAL INTELLIGENCE

| 25 May - 21 June 2021 |

ORGANISED BY

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

28 days (4 weeks)

REGISTRATION DEADLINE

24 May 2021

COURSE CODE

21OI26412EUR-E

This course will focus on Future Broadband: Ultra-broadband Internet, Clouds, IoT and Artificial Intelligence, including technologies, regulation and business aspects. It will cover Internet technologies, including IPv6, DNS, DHCP, IP networking, HTTP 2.0, IPX, IP QoS, Cybersecurity, as well as Internet governance. Also, it will include MPLS/VPN transport, Carrier Ethernet, as well as future gigabit copper, fiber optic, submarine cable, and satellite broadband access. Further, it will cover SDN and network virtualization (NFV) for fixed and mobile, ITU's Cloud Computing architectures, security and privacy, future OTT and telecom clouds (Machine Learning as a Service, Blockchain as a Service), clouds governance, uses of Artificial Intelligence (AI) for Internet and telecoms, as well as critical and massive IoT, data management, Big Data architectures, as well as IoT/data security, privacy and trust. Finally, it will also cover future broadband OTT services (video, social, AR/VR/XR, Web 3.0) and net neutrality, Tactile Internet for remote operations (TIRO), Intelligent operation network (ION), Digital twins (DT), Space-terrestrial integrated network (STIN), Industry 4.0, smart city as well as future clouds/IoT/AI services, including their business and regulatory aspects.

Audience:

This course is targeted at managers, engineers and employees from regulators, government organisations, telecommunication companies and academia, who are interested in understanding, implementation and regulation of Future Broadband: Ultra-broadband Internet, Clouds, IoT and Artificial Intelligence, including technologies, regulatory and business aspects. Other institutions and individuals that are dedicated in building their capacity related to Future Broadband: Ultra-broadband Internet, Clouds, IoT and Artificial Intelligence are also welcome to participate.

Trainer: Prof. Dr. Toni Janevski

DATA PRIVACY, SECURITY & GOVERNANCE

| 1 June – 7 July 2021 |

ORGANISED BY

The Abdus Salam International Centre for Theoretical Physics

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

5 weeks

REGISTRATION DEADLINE

31 May 2021

COURSE CODE

21OI26515EUR-E

Description:

The course reviews relevant terms and background from the field of information security. This is followed by a broad overview of the collection and analysis of data; leading to the dentification of valuable data and how to secure data against common threats such as loss of privacy arising from data breaches theft or loss and the aggregation or integration of data. Practical sessions and discussion will cover pertinent issues of Data Governance such as data security controls, international legislative issues, digital data forensics as well as Privacy and ethical issues.

Audience: This course is ideal for business decision-makers, researchers and security professionals, education practitioners involved in teaching and learning online.

Trainer: James Uhomoibhi, Clement Onime, Solomon Gizaw Tulu

SPEECH AND NATURAL LANGUAGES PROCESSING

| 1-30 June 2021 |

ORGANISED BY

The Abdus Salam International Centre for Theoretical Physics

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

4 weeks

REGISTRATION DEADLINE

31 May 2021

COURSE CODE

21OI26500EUR-E

Description:

This course is designed to teach students to understand the current state of the art of Automatic Speech Recognition (ASR) and Natural Language Processing. The first part provides background review and discussion on ASR background and introduction to probability. Student will learn key algorithms such as HMM, DNN, Hybrid (HMM/DNN) and Baum-Welch training algorithm. Students will also learn about representations of the acoustic signal like MFCC coefficients, and the use of Gaussian Mixture Models (GMMs) and context-dependent triphones for acoustic modeling. Finally, we will cover N-gram language modeling and perplexity. The students will be engaged in detail ASR system development tools such as HTK, Sphinx and ESPRESSO. Students also gain an understanding of Text-to-Speech (TTS): Grapheme-to-phoneme and Prosody (Intonation, Boundaries and Duration). The students will compare and contrast past ASR techniques and the current approaches to develop ASR system.

Audience: This training activity is designed for technical and mid-level managers of Telecom Operators, Business entities and organizations who would like to better understand automated voice/speech recognition and response systems and how to implement or provide automated voice services in local languages.

Trainer: Solomon Gizaw Tulu, Clement Onime

5G TECHNOLOGIES FOR IoT

| 7-8 June 2021 |

ORGANISED BY

The Abdus Salam International Centre for Theoretical Physics

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

2 days

REGISTRATION DEADLINE

1 June 2021

COURSE CODE

21OI26448EUR-E

5G advantages in terms of enhanced throughput are at the forefront, but the network slicing capabilities it offers are being leveraged to meet the requirements of both massive and critical IoT applications, in which the number of devices to be served and the duration of their batteries is the most important aspect. Moreover, for certain applications, the 5G reduced latency can be a game changer.

This course aims to provide the audience with an understanding of the 5G aspects relevant to IoT and how they compare with existing proprietary technology that are currently widely deployed.

Audience:

The training course is designed for:

Electrical engineers

Telecommunications engineers

Computer scientists

Regulators

Telecom Operators

Networks Operators

Trainer: Dr. Marco Zennaro, Research Officer, T/ICT4D Lab

LEGAL, REGULATORY AND TECHNICAL ASPECTS OF CLOUD COMPUTING IN INTERNATIONAL DATA TRANSFERS

| 14-21 June 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

14 June 2021

COURSE CODE

21OI26413EUR-E

Description:

The subject matter in this web seminar refers to international data transfers whereby cloud computing solutions will be applied. In relation to the subject matter various types of data will be discussed, including personal, which will be analysed in the context of different regulations. The web seminar will include technical aspects of application of various types of the cloud computing and its impact on the application of the legal framework. The seminar will also address different roles of cloud actors and its obligations under relevant regulations. In addition, the seminar will discuss liability issues for providing cloud services in an international dimension. At the outset of the seminar a knowledge test will be conducted. The seminar will include regulatory aspects of the use of cloud computing, including regulatory control issues.

Audience:

The target group of this workshop include representatives of regulatory bodies, dealing with cloud computing matters, telecommunications issues, consumer protection issues, cyber security issues, data protection issues.

Trainer:

Dr hab. Andrzej Krasuski

TECHNICAL, BUSINESS AND REGULATORY ASPECTS OF 5G NETWORKS

| 23-30 August 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

23 August 2021

COURSE CODE

21OI26414EUR-E

Description:

This course will focus on technical, business and regulatory aspects of the 5G mobile networks. It will include 4G mobile technology transition toward the 5G, considering the access and core networks as well as end-user services. Mobile broadband Internet after 4G will continue with the next generation, 5G, so the course will cover also IPv6 and its impact on 5G mobile networks. Further, it will include M2M (Machine-to-Machine) and mobile Internet of Things (IoT) services are foreseen types in future 5G mobile environments, as well as mobile cloud computing implementations. Also, the course will include spectrum management for IMT (International Mobile Telecommunications) including the 5G considerations. The QoS in mobile networks going from 3G/4G mobile world toward the 5G will continue to be important, hence the course will also focus on QoS and QoE in next generation mobile environments. Finally, the course will focus on emerging services and applications in 5G mobile networks in different verticals, including technology, as well as their business and regulation aspects.

Audience:

This course is targeted at managers, engineers and employees from regulators, government organisations, telecommunication companies and academia, who are interested in understanding, implementation and regulation of technical, business and regulatory aspects of 5G network, including technologies, standardization, regulation and content. Other institutions and individuals that are dedicated in building their capacity related to technical, business and regulatory aspects of 5G network are also welcome to participate.

Trainer:

Prof. Dr. Toni Janevski

CYBER RISK MANAGEMENT

| 1 June – 31 December 2021 |

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE

English

FEES

249 USD

MODE

Online

DURATION

-

REGISTRATION DEADLINE

No deadline

COURSE CODE

21OI26481EUR-E

This course aims to provide a student with an understanding of risk management processes according to ISO 27000 and ISO 31000.
The content will cover such topics as risk assessment and risk management as a core process for an ISMS, risk handling, and mitigation strategies. Besides that, a general introduction to emergency operation planning, crisis management, and cyber-insurance subjects will be provided.
Students will have three months to complete the course. After this time, registrations will be reopened for new participants.

Audience:

Professionals with information security responsibilities, managers, ISO, CISO.

Trainers:

Dmytro Cherkashyn, Swantje Westpfahl

QoS TECHNOLOGIES AND REGULATION FOR FIXED AND MOBILE

| 27 September – 4 October 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

27 September 2021

COURSE CODE

21OI26415EUR-E

Description:

This course will focus on technical, business and regulatory aspects of QoS for Fixed and Mobile Networks. It includes QoS (Quality of Service) and QoE (Quality of Experience) fundamentals by ITU, as well as traffic and QoS management in Internet and IP networks. Further, it includes QoS for fixed ultra-broadband access, including QoS solutions in metallic and optical networks, carrier grade Ethernet QoS, as well as end-to-end QoS. The course also covers QoS for mobile ultra-broadband access, including 4G and 5G mobile technologies and their QoS capabilities and approaches. The telecom networks are built for provision of services. In that manner the course covers QoS-enabled services provisioning, including QoS and QoE for VoIP, video and IPTV services, as well as QoS for Internet data services (i.e., Over-The-Top services). Each telecommunication network is interconnected to other networks forming the global network of Internet and managed IP networks, so the course includes interconnection and its QoS aspects. Further, it covers generic and specific QoS parameters, KPIs (Key Performance Indicators) and their measurements. The global Internet is based on network neutrality approach for OTT/data services, so the course also covers network neutrality and its regulation. The QoS constantly increases in its importance with the digitization and innovation of various critical services, so the course includes QoS regulatory framework based on technical, business/economic and regulatory principles of QoS for services over fixed and mobile networks.

Audience:

This course is targeted at managers, engineers and employees from regulators, government organisations, telecommunication companies and academia, who are interested in understanding, implementation and regulation of QoS for Fixed and Mobile networks, including technologies, standardization, and regulation. Other institutions and individuals that are dedicated in building their capacity related to QoS Technologies and Regulation for Fixed and Mobile Networks are also welcome to participate.

Trainer: Prof. Dr. Toni Janevski

APPLICATIONS OF SATELLITE BASED IoT NETWORKS

|15-16 November 2021|

ORGANISED BY

The Abdus Salam International Centre for Theoretical Physics

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

2 days

REGISTRATION DEADLINE

12 November 2021

COURSE CODE

21OI26450EUR-E

Satellite technologies have played a significant role in communications for many decades, since they are the only ones that can provide truly global coverage. Their applications in IoT have so far been limited, but recent advances in electronics and antenna technologies have ushered a new era of smaller satellites with improved characteristics, which coupled with improvements in launching vehicles open the door for unforeseen applications, sustainable even in budget constrained sectors.

IoT applications can be served by both Geostationary (GEO) and Low Earth Orbit (LEO) satellites, and their relative merits will be discussed in this course, which will enable the participants to make informed choices about the best technology for a given application.

Audience:

The training course is designed for:

Electrical engineers

Telecommunications engineers

Computer scientists

Regulators

Telecom Operators

Networks Operators

Trainer: Dr. Marco Zennaro – Research Officer, T/ICT4Lab

FUTURE MOBILE AND WIRELESS BROADBAND: LTE-A-PRO, WIFI, SATELLITES, 5G NR AND AI

| 16 November - 13 December 2021 |

ORGANISED BY

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

28 days (4 weeks)

REGISTRATION DEADLINE

15 November 2021

COURSE CODE

21OI26418EUR-E

Description:

This course will cover Future mobile and wireless broadband: LTE-A-Pro, WiFi, Satellites, 5G NR and AI, including technologies, regulation and business aspects. The course will cover mobile broadband LTE-Advanced/LTE-A-Pro, 4G QoS and mobile Internet access, and ITU's spectrum management. Further, the course will cover future wireless broadband, including WiFi Next Generation (WiFi 6), WiFi for mobile traffic offload, and Satellite broadband access. It will also include 5G New Radio (NR) access and 5G Next Generation core, then 5G network slicing and virtualization with SDN/NFV, 5G QoS, 5G spectrum management, 5G and Satellite networks, as well as Artificial Intelligence (AI) and Machine Learning (ML) in 5G networks. The course will also cover massive and critical Internet of Things (IoT) in 4G and 5G, Edge and Fog Computing, enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communication (URLLC), massive Machine Type Communication (mMTC), and IoT/BiData/AI/ML services in 5G. Finally, the course will cover VoLTE and VoNR, 5G streaming, AR/VR/XR, 5G broadcast, 5G FWA, V2X, industrial automation, future mobile OTT services and Internet net neutrality, as well as business and regulatory aspects of future mobile services.

Audience:

This course is targeted at managers, engineers and employees from regulators, government organisations, telecommunication companies and academia, who are interested in understanding, implementation and regulation of Future mobile and wireless broadband: LTE-A-Pro, WiFi, Satellites, 5G NR and AI, including technologies, regulatory and business aspects. Other institutions and individuals that are dedicated in building their capacity related to Future mobile and wireless broadband: LTE-A-Pro, WiFi, Satellites, 5G NR and AI are also welcome to participate.

Trainer: Prof. Dr. Toni Janevski

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE IN BUSINESS, HOUSEHOLD AND PUBLIC SECTOR

| 6-13 December 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

150 USD

MODE

Online

DURATION

8 days

REGISTRATION DEADLINE

6 December 2021

COURSE CODE

21OI26417EUR-E

Description:

The subject matter of this stationary workshop is the discussion of legal framework applicable to Artificial Intelligence with international focus. By discussing the application of Artificial Intelligence, various types of Artificial Agents in many spheres of life will be considered, including: business activity, household, and the public sector. During the workshop different definitions of Artificial Intelligence will be considered and discussed from a legal point of view. The workshop will also encompass liability issues connected with the use of Artificial Intelligence, including robots. Various concepts of liability will be assessed. During the workshop various examples of the application of Artificial Intelligence will be included. In addition, recommendations for future legislation will be presented and analysed. At the outset of the workshop a knowledge test will be conducted.

Audience:

The target group of this workshop include representatives of regulatory bodies, dealing specifically with Artificial Intelligence issues, but also with consumer protection issues, cyber security issues, data protection issues.

Trainer:

Dr hab. Andrzej Krasuski

INDUSTRIAL CYBERSECURITY AND INCIDENT RESPONSE

| 20-22 September 2021 |

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE

English

FEES

999 USD

MODE

TBA

VENUE

DURATION

3 days

REGISTRATION DEADLINE

1 September 2021

COURSE CODE

21WS26477EUR-E

Description:

This course will provide students with unique expertise in the area of critical infrastructure cyber security. The course will cover typical threats and vulnerabilities typical to it and industrial control systems.
Another part of the course will be dedicated to a case study on incident response in a hypothetical environment. This will be continued by the practical part, where students will play the role of hackers, who a targeting industrial control and security systems of the improvised company with the break-out session on consequences and potential mitigation strategies.

Audience:

Operational engineers, inhouse security specialists, or security specialists

Trainer:

Dmytro Cherkashyn

COVID-19 Info:

Participants, who are registered and paid the course fees, are still subject to additional requirements for traveling to Germany. This information will be provided and checked against each participant's situation a few weeks prior to the course.

KEY ASPECTS AND GOVERNANCE OF INTERNET OF THINGS, BIG DATA AND ARTIFICIAL INTELLIGENCE

| 28-29 October 2021 |

ORGANISED BY

National Institute of Telecommunications

LANGUAGE

English

FEES

500 USD

MODE

TBA

DURATION

2 days

REGISTRATION DEADLINE

18 October 2021

COURSE CODE

21WS26416EUR-E

Description:

This course will focus on technical, business and regulatory aspects of Internet of Things (IoT), Big Data and Artificial Intelligence (AI). It will cover Internet technologies for IoT, then IoT standards, architectures and interoperability, as well as IoT policies and regulations, including IoT security and privacy issues. The course will include IoT services in 4G and 5G mobile systems, including massive IoT and critical IoT use cases. The IoT generates large amounts of data that cannot be processed by traditional techniques, and such data is referred to as Big Data. In that manner, the course will include Big Data overview, Big Data ecosystem and reference architecture, Big Data technologies and use cases, as well as business and regulatory challenges for Big Data. Artificial Intelligence (AI) is targeted for processing Big Data in Internet and telecom networks. In that regard the course will cover introduction to AI in ICT/telecom world, and AI applications in Internet and telecom worlds, including Machine Learning aspects for 5G mobile networks. The course will further include Big Data and AI challenges, business aspects, as well as policies and regulation. Finally, the course will cover Internet governance with regard to IoT, Big Data, and AI.

Audience:

This course is targeted at managers, engineers and employees from regulators, government organisations, telecommunication companies and academia, who are interested in understanding, implementation and regulation of Internet of Things (IoT), Big Data and Artificial Intelligence (AI), including technical, business and regulatory aspects. Other institutions and individuals that are dedicated in building their capacity related to IoT, Big Data and AI, including technical, business and regulatory aspects, are also welcome to participate.

Trainer: Prof. Dr. Toni Janevski

INCIDENT RESPONSE PRACTICE

| 8 - 11 November 2021 |

ORGANISED BY

NRD Cyber Security

LANGUAGE

English

FEES

800 USD

MODE

TBA

DURATION

4 days

REGISTRATION DEADLINE

30 October 2021

COURSE CODE

21WS26399EUR-E

Description:

For the efforts towards strengthening cyber security to be successful, technical teams must be specifically trained on practicalities of incident response. The course is designed to empower incident handlers to be effective at their work.

The training course presents a comprehensive overview of cybersecurity teams' issues on a technical level, vulnerability handling, trend/technology watch, security tools, and also issues of artefact handling and forensics. The course is technical in nature, relying heavily on hands-on and practical experience. The most recent threats and vulnerabilities are treated.

Data breaches are everywhere, and they're showing no signs of slowing down. Internal and external threats pose big risks to all types of organizations, only the damage and recovery time could be different. The training is dedicated to measure the readiness of CSIRT to deal with the most often real-world cases of cyber security incidents. The course is composed of series of exercises by providing participants with questionnaires and practical assignments on specific types of cyber security incidents.

Participants will be provided a set of specific pre-defined real-life incident scenarios. Several different incident handling cases are simulated to students and focused on incident detection and description, information gathering, analysis tools and techniques and incident handling phases by using RTIR (or related) tool. Cyber threat hunting tips are also provided to deeper knowledge in incident handling.

During hands-on exercises, participants will work with the following topics:

- Incident management key components;
- Information sources available, such as zone-h, shodan, pastebin, host and network logs;
- E-mail incidents investigation;
- Network logs-based incidents investigation;
- Host logs-based incidents investigation.

Prerequisite: participants are required to bring a laptop with them.

Audience:

The course is designed for CIRT members and all incident handlers who wish to be effective at their work.

Trainer:

The training is led by prominent experts who are on daily basis involved in CSIRT related activities at national and organizational level in Lithuania and abroad.

Marius Urkis - NRD CIRT lead, cyber security incident handling and forensics expert

Rimtautas Černiauskas - Technical cyber security consultant and investigator

Prof Dr Toni Janevski
Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University in Skopje (FEEIT)
North Macedonia
Email: tonij@feit.ukim.edu.mk
Priority area:

- Wireless & Fixed Broadband

Dr Sylwester Laskowski
National Institute of Telecommunications (NIT)
Poland
Email: S.Laskowski@itl.waw.pl
Priority areas:

- Internet Governance
- Wireless & Fixed Broadband

Ms Ruta Jasinskiene
Head of Training
NRD Cyber Security
Lithuania
Email: rj@nrdcs.lt
Priority areas:

- Cybersecurity

Mr Dmytro Charkashyn
Research Fellow
Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences
Germany
Email: macori@th-brandenburg.de
Priority areas:

- Cybersecurity

Mr Marco Macori

Research Fellow
Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences
Germany
Email: macori@th-brandenburg.de
Priority areas:

- Cybersecurity

Dr Marco Zennaro
Research OfficerT/ICT4 Lab
The Abdus Salam International Centre for Theoretical Physics (ICTP)
Italy
Email: mzennaro@ictp.it
Priority areas:

- Internet of Things
- Big Data & Statistics

ITU Office for Europe
International Telecommunication Union (ITU)
Place des Nations, 1211 Geneva 20
Switzerland
https://www.itu.int/en/ITU-D/RegionalPresence/Europe/Pages/default.aspx
Email: EURregion@itu.int
Phone: +41227306320