COURSE PROGRAMME

COURSE PROGRAMME

CEER has arranged an annual training on cybersecurity for NRAs since 2016. The goal is not only to learn about security issues and solutions and the role of National Regulatory Authorities on Energy (NRAs). We also provide a platform to let NRAs staff on management level with interest for cybersecurity and those who are working with cybersecurity for NRAs, either from a technical or legal angle, to connect and create useful relationships.

With increased digitalization comes increased cybersecurity risk. Processes such as producing and distributing energy is becoming digitally dependent and we connect operational technology to digital networks to ease process control. As a consequence, we become vulnerable to cyberattacks where the attackers may be located and be hiding anywhere in the world. While before, personnel performing physical sabotage may be found and arrested, we may never know who broke into our digital systems and shut down operations remotely. The lack of accountability for digital attackers, and the increased use of technology that can be attacked, makes important processes such as energy supply prominent targets.

One typical reason for attacking the energy sector may be financial. One example is the Colonial Pipeline attack in 2021, where data was stolen and encrypted. According to internet sources, Colonial Pipeline decided to pay a ransom of nearly $ 5 million to stop the attackers from spreading their data and being able to resume fuel distribution. Another reason for cyberattacks may be connected to nation state conflicts. A well-known example is the cyberattacks on Ukraine electricity distribution in 2015 and 2016, both leading to blackouts for hours. The latter reason may be more actual than ever, after the last development in Ukraine.

Everybody using technology must prepare for this new reality, including NRAs. NRAs must understand their roles and responsibilities and take the necessary steps to monitor cyber-risk preparedness in the sector and add measures to improve cybersecurity where necessary. The role of NRAs has become clearer during the work with a network code on cybersecurity. NRAs has been involved in the development of this piece of legislation, especially through the Agency for the Cooperation of Energy Regulators (ACER).

This CEER training course targets NRA staff on management level with interest for cybersecurity and those who are working with cybersecurity for NRAs, either from a technical or legal angle. The course aim to provide an overview of the latest policy developments in cybersecurity and practical experiences on the technical aspects of cybersecurity risk management and preparedness in Europe. The programme will also explain the links between cybersecurity and data management and privacy and how cybersecurity could be enhanced to ensure data protection and privacy.

This training will be a hybrid event, where participants may decide themselves if they wish to join in person or online. We look forward to seeing you 31 May – 2 June.

COURSE PROGRAMME

COURSE STRUCTURE

Week 1: 23-27 May 2022
Individual preparation to the course: Literature review, reading materials, preparation of course work
Online Live Session: 11:00-12:00 (CET) on 24 May 2022

Week 2:
Hybrid Class 1: 10:00-17:00 (CET) on 31 May 2022
Hybrid Class 2: 09:00-17:00 (CET) on 1 June 2022
Hybrid Class 3: 09:00-15:00 (CET) on 2 June 2022

Tuesday, 31 May 2022
10:00-17:00 CET

10:00 - 10:20 **Opening remarks and round-table introduction of the participants**

Catharina Hovind and Øyvind Toftegaard, Course Directors

10:20 - 10:30 **Introducing the participants – platform orientation**

Giulia Carpentieri CEER Programme and Training Coordinator

SESSION 1 UNDERSTANDING CYBERSECURITY RISK

10:30 - 11:15 **Industry example: Cybersecurity breach**

Brynjar Larssen, Volue ASA - Online

11:15 – 11:30 **Coffee break**

11:30 – 12:15 **How to Attack and Defend Wind Farms**

Sujeet Shenoi, University of Tulsa – Onsite

12:15 – 13:15 **Lunch break**

SESSION 2 RISK MANAGEMENT

13:15 – 13:45 **Introduction to cyber security and risk management**

Renate Verheijen, ENISA – Online

13:45 – 14:15 **Role of National Competent Authority on Cybersecurity**

Nicolas Broutin, ANSSI – Online

14:15 – 14:25 **Coffee break**

14:25 – 14:55 **NRAs responsibility and example of work on cybersecurity**

Matthew Cowlard and Ray Robinson, Ofgem - Onsite

14:55 – 15:25 **Industry example of DSO work on reducing cybersecurity risk**

Anders Åhlgren, Jönköping Energi & EU DSO - Onsite

15:25 – 15:30 **Short Break**

15:30 – 16:00 **Discussion panel**

Moderator Øyvind Toftegaard, Course director
Panel: Sujeet Shenoi – Matthew Cowlard - Ray Robinson - Catharina Hovind

16:00 -16:10 **Final remarks and wrap up of Day 1**

Catharina Hovind and Øyvind Toftegaard, Course Directors

16:10 – 17:10 **Reception drinks at the CEER office – all participants and lecturers welcome!**

- END OF DAY 1 –

Wednesday, 1 June 2022
09:00-16:00 CET

SESSION 3 INTRO TO REGULATING ENERGY CYBERSECURITY

9:00 – 9:30 **Orchestrating cybersecurity regulation in Europe**

Felipe Castro Barrigon, European Commission – Onsite

9:30 - 10:00 **Implementation of EU regulation in national cybersecurity legislation**

Anders Åhlgren, Jönköping Energi & EU DSO - Onsite

10:00 – 10:10 **Short Break**

10:10 – 10:40 **National risk preparedness plan for the electricity sector**

Luka Strnad, ELES – Onsite

10:40 – 11:00 **Coffee Break**

11:00 – 11:30 **Cybersecurity Landscape of European Energy Markets**

Leontini Kaffentzaki and Kostas Prosmitrellis
Regulatory Authority for Energy (RAE), Directorate of European and International Affairs - Online

11:30 – 12:00 **Effect of cybersecurity legislation on maturity level**

Jon-Martin Storm, Norwegian Water Resources and Energy Directorate – Online

12:00 – 13:00 **Lunch break**

SESSION 4 CYBERSECURITY FOR PIPELINES AND EXERCISE

13:00 – 13:45 **Gas pipeline cybersecurity risk**

John Ransom, CISA – Onsite

13:45 – 13:55 **Coffee break**

13:55 – 15:50 **Practical Exercise**

Course Director Øyvind Toftegaard

15:50 - 16:00 **Final remarks and wrap up of Day 2**

Catharina Hovind and Øyvind Toftegaard

16.00 -16.15 **Short break**

16.15-17.00 **1. How Stuxnet Attacked Iran's Uranium Hexafluoride Centrifuges: Lessons on Cyber Warfare**
2. How Open-Source Intelligence is Used to Penetrate Infrastructure Assets
This is a bonus session for in-person participants only. Due to the sensitiveness of the topic, this session will NOT be broadcasted online. No photographs of slides will be allowed during the lecture.

Sujeet Shenoi, University of Tulsa – Onsite

17.00: – 19:30 **Relax and freshen up break before dinner**

19.30 **Dinner reservation – all participants and trainers welcome!**
RESTAURANT STROFILIA
Rue du Marché aux Porcs 11/13, 1000 Bruxelles, België

- END OF DAY 2 –

Thursday, 2 June 2022
09:00-15:00 CET

SESSION 5 REGULATING CYBERSECURITY

9:00 – 10:00 **The development of a network code on cybersecurity**

Stefano Bracco, ACER - Online

10:00 – 10:45	**NIS2 directive – What does it mean and what is the process**
	Boryana Hristova, European Commission - Online
10:45 – 11.00	**Coffee break**
11.00 – 11.30	**Developing a cybersecurity strategy for NRAs**
	Lynn Costantini, Naruc - Online

SESSION 6 PRIVACY AND DATA PROTECTION

11:30 - 12:30	**Regulation for a privacy preserving smart grid**
	Staal Vinterbro, NTNU - Online
12:30 –13:45	**Lunch break**
13:45 –14:15	**The role of NRAs regarding privacy protection**
	Vincent Harrop, CRE - Online
14:15 – 14:45	**Discussion – End of the training**
	Catharina Hovind and Øyvind Toftegaard

- END OF DAY 3 –