NATO ENERGY SECURITY CENTRE OF EXCELLENCE

Energy Security: NATO ENSEC COE perspective

Symposium Union de l'Energie, Paris

15th May 2019

Dr Tadas Jakstas

NATO ENERGY SECURITY CENTRE OF EXCELLENCE

Agenda

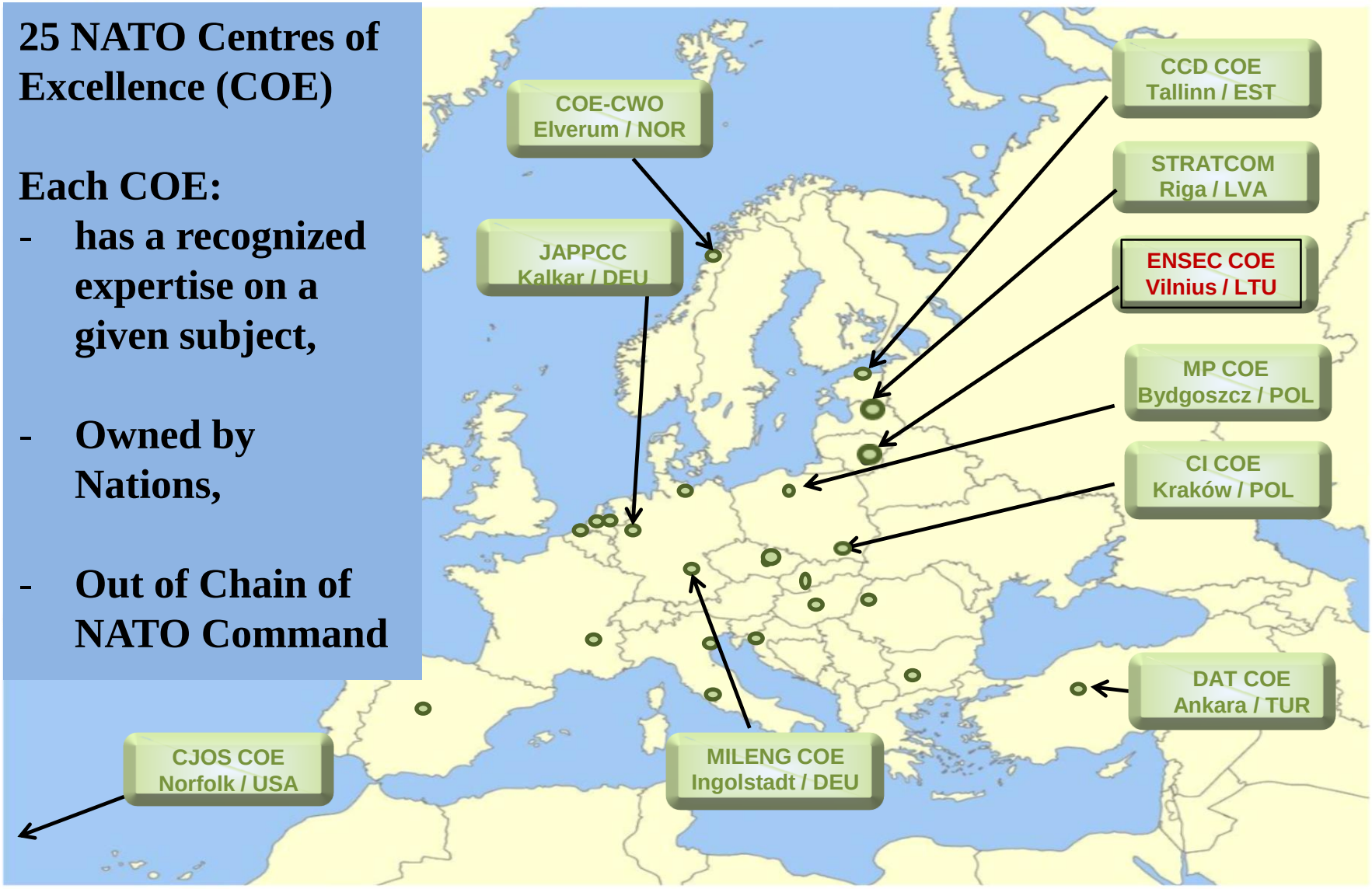
- Community of COE's
- NATO ENSEC COE: mission, structure
- NATO ENSEC COE: means, activities
  - Coherent Resilience 2019
  - NATO CEPS Cyber Security Study
- NATO ENSEC COE upcoming projects

Community of NATO COEs

25 NATO Centres of Excellence (COE)

Each COE:

- **has a recognized expertise on a given subject,**
- **Owned by Nations,**
- **Out of Chain of NATO Command**



NATO ENSEC COE: Mission

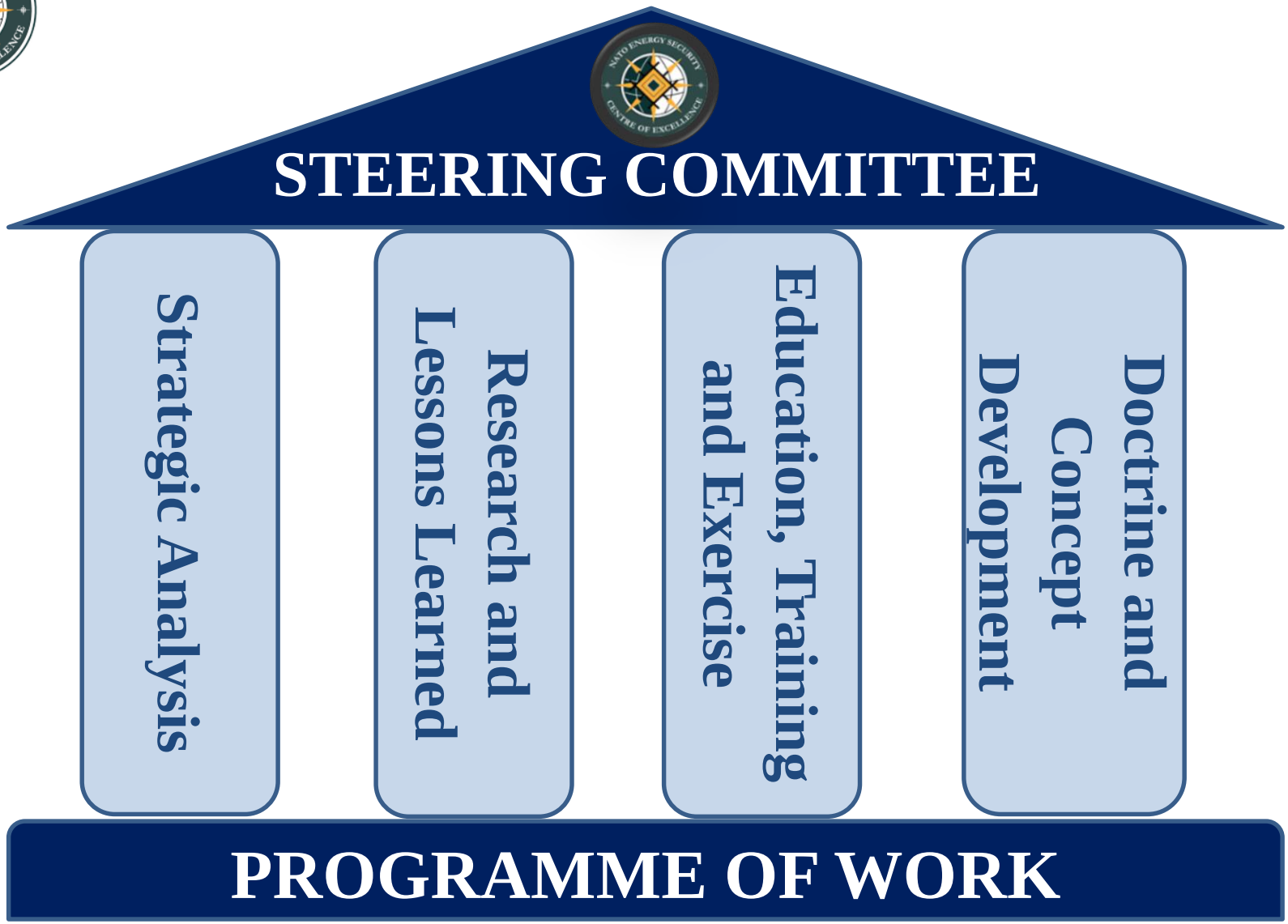
To **assist NATO**, **Nations, Partners** and other bodies by supporting NATO's capability development process, mission effectiveness and interoperability providing comprehensive and timely **expertise on all aspects of energy security**.

NATO ENSEC COE: Mission

- **Raising awareness of energy developments with security implications;**
- **Developing NATO's competence in supporting the protection of critical energy infrastructure and enhancing resiliency;**
- **Improving the energy efficiency of military forces.**

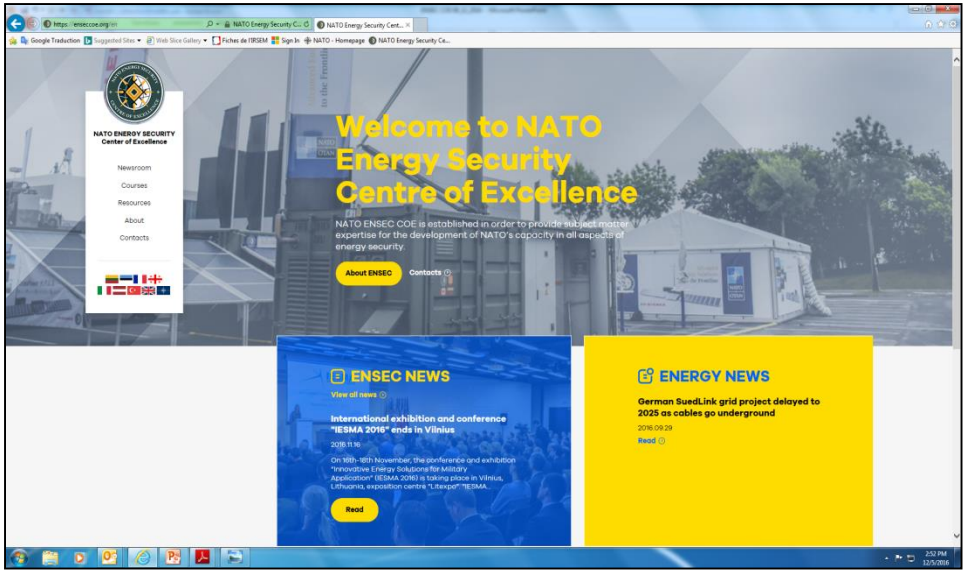
- ***No interference*** *with national energy and economic policies;*
- ***No duplication*** *of other stakeholders' roles and responsibilities.*

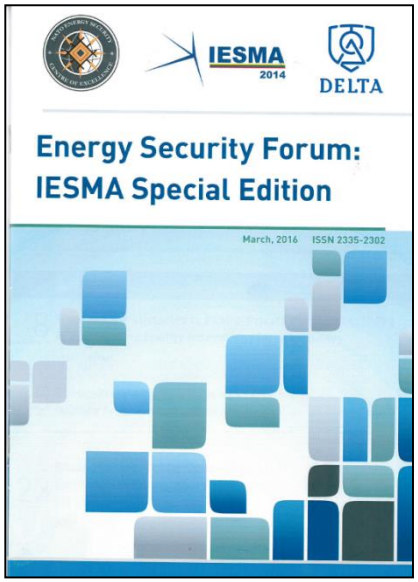
NATO ENSEC COE: Structure

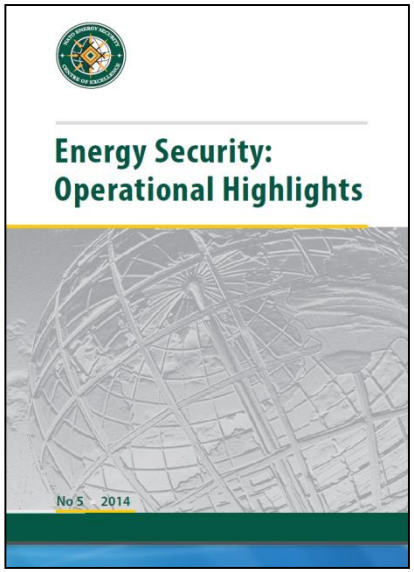


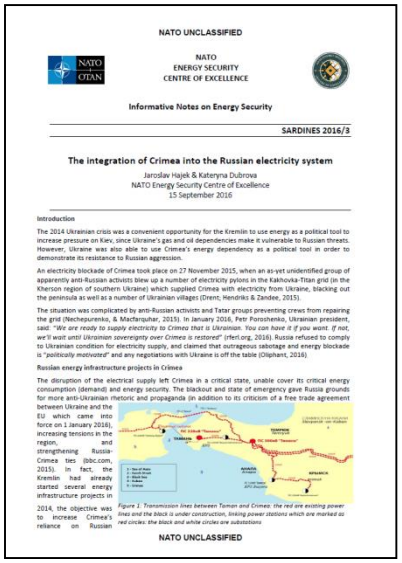
NATO ENSEC COE: Means/Partners

NATO ENSEC COE: Means/Publications








NATO UNCLASSIFIED

NATO ENERGY SECURITY CENTRE OF EXCELLENCE

Informative Notes on Energy Security

SARDINES 2016/3

The integration of Crimea into the Russian electricity system

Jaroslav Hajek & Kateryna Dubrova
NATO Energy Security Centre of Excellence
15 September 2016

Introduction

The 2014 Ukrainian crisis was a convenient opportunity for the Kremlin to use energy as a political tool to increase pressure on Kiev, since Ukraine's gas and oil dependencies make it vulnerable to Russian threats. However, Ukraine was also able to use Crimea's energy dependency as a political tool in order to demonstrate its resistance to Russian aggression.

An electricity blockade of Crimea took place on 27 November 2015, when an as-yet unidentified group of apparently anti-Russian activists blew up a number of electricity pylons in the Kakhovka-Titan grid (in the Kherson region of southern Ukraine) which supplied Crimea with electricity from Ukraine, blacking out the peninsula as well as a number of Ukrainian villages (Drent; Hendriks & Zandee, 2015).

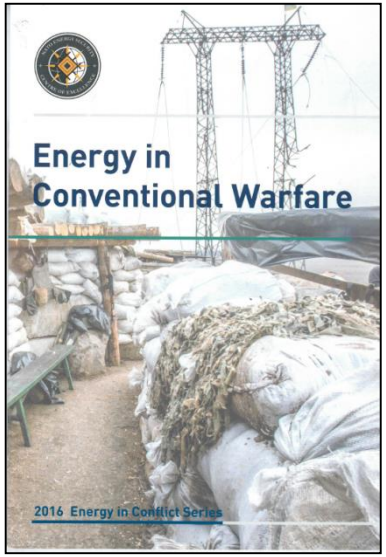
The situation was complicated by anti-Russian activists and Tatar groups preventing crews from repairing the grid (Nechepurenko, & Mackinnuhar, 2015). In January 2016, Petr Poroshenko, Ukrainian president, said: *"We are ready to supply electricity to Crimea that is Ukrainian. You can have it if you want. If not, we'll wait until Ukrainian sovereignty over Crimea is restored"* (rferl.org, 2016). Russia refused to comply to Ukrainian condition for electricity supply, and claimed that outrageous sabotage and energy blockade is "*politically motivated*" and any negotiations with Ukraine is off the table (Oliphant, 2016).

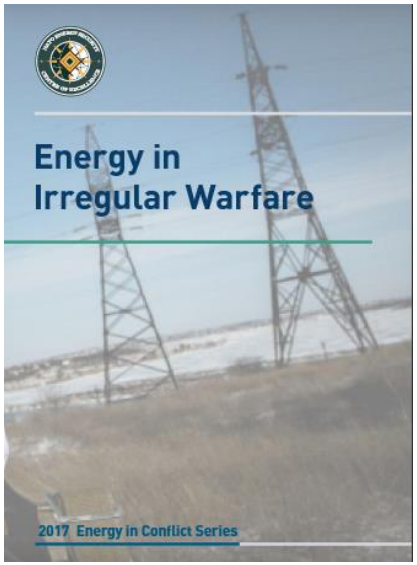
Russian energy infrastructure projects in Crimea

The disruption of the electrical supply left Crimea in a critical state, unable cover its critical energy consumption (demand) and energy security. The blackout and state of emergency gave Russia grounds for more anti-Ukrainian rhetoric and propaganda (in addition to its criticism of a free trade agreement between Ukraine and the EU which came into force on 1 January 2016), increasing tensions in the region, and strengthening Russia-Crimea ties (bbc.com, 2015). In fact, the Kremlin had already started several energy infrastructure projects in 2014, the objective was to increase Crimea's reliance on Russian

Figure 1. Transmission lines between Taman and Crimea: the red are existing power lines and the black is under construction, linking power stations which are marked as red circles; the black and white circles are substations

NATO UNCLASSIFIED





NATO ENSEC COE: Means/Table top exercises

Critical Energy Infrastructure Protection

Support to National Authorities

Natural Gas Transmission Operators

Nickname: Coherent Resilience 2019

Level: Middle Level Managers and Policy Makers

Type: Tabletop Exercise (TTX)

Dates:

Academic Seminar – 14 May 2019;

TTX and AAR (including DVD) – 14-16 May

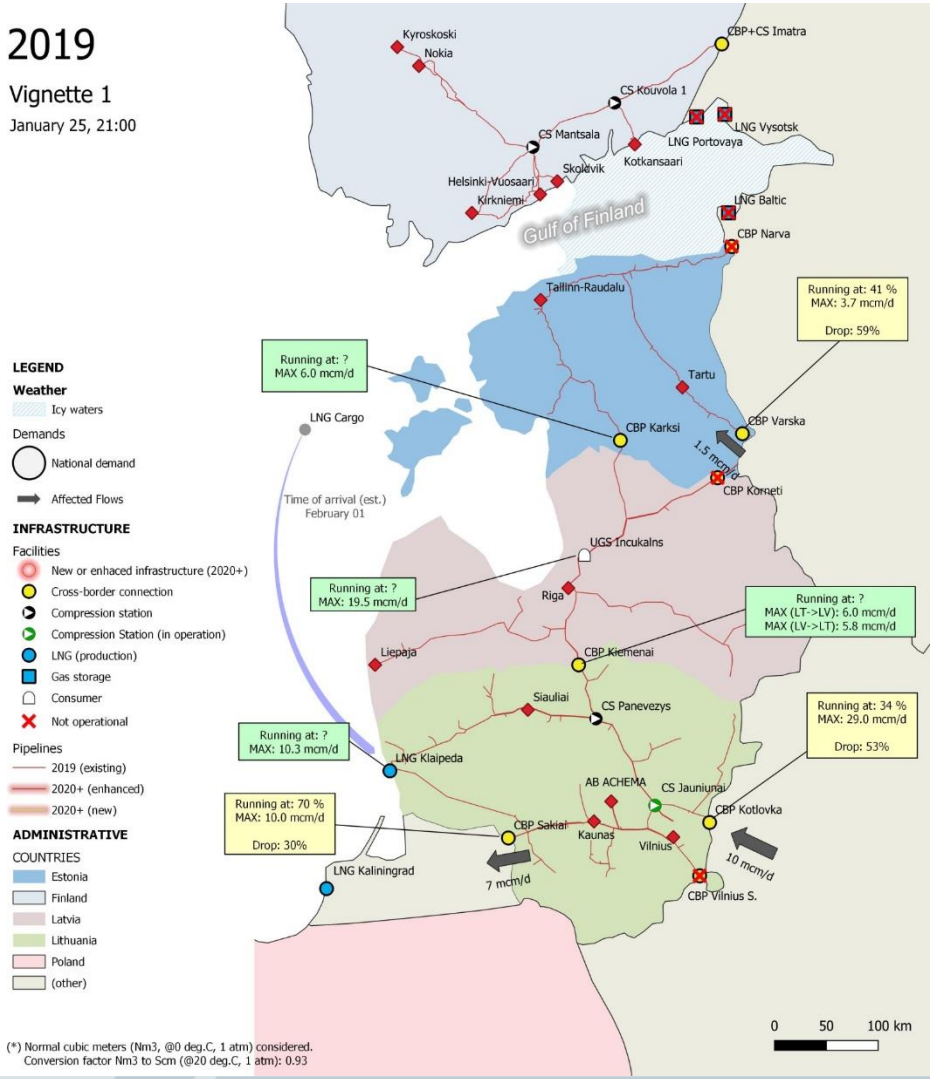
Area: Baltic States (Estonia, Latvia, Lithuania+Finland and Poland, Ukraine as observers)

Aim: to support the national authorities and gas transmission system operators (TSO) of the Baltic States in ensuring supply of gas to consumers and mitigating the disruption over the Baltic region.

Coherent Resilience-2019

Participants are grouped in 4 syndicates:

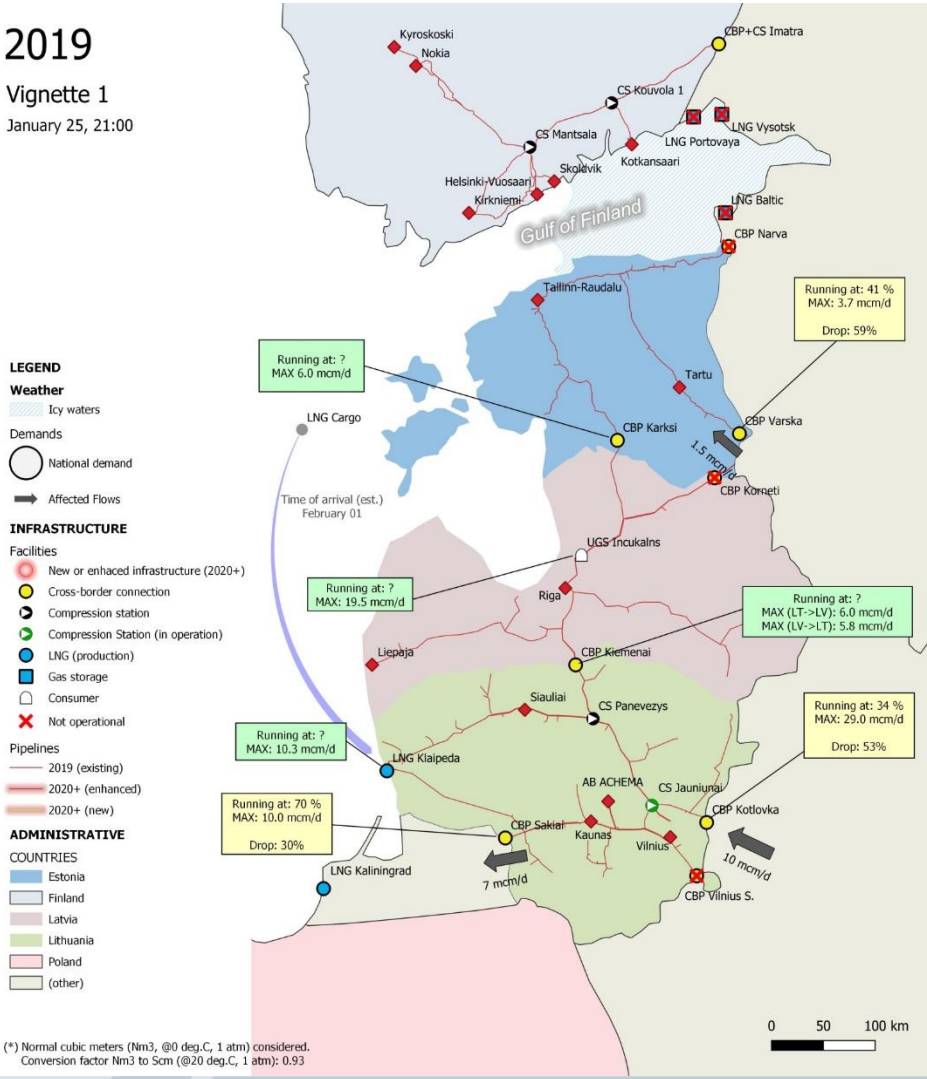
- Syndicate 1 – Solidarity Mechanism of the EU;
- Syndicate 2 – National Preventive Action and Emergency Plans;
- Syndicate 3 – Strategic (Crisis) Communication;
- Syndicate 4 – Cyber Security



Coherent Resilience-2019

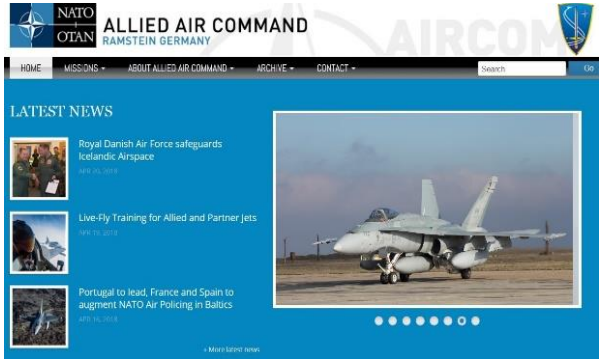
Seek to find out:

- What TSO does? Who is informed?
- What Ministries do?
- What LNG operator does?
- How flows to Kaliningrad are managed when CS supply is reduced?
- Any demand side measures?
- Demand limitations/customer priotisation?
- Supply to power plants?
- Reporting to the EC?
- Any crisis meetings/boards/announcements
- Public communication



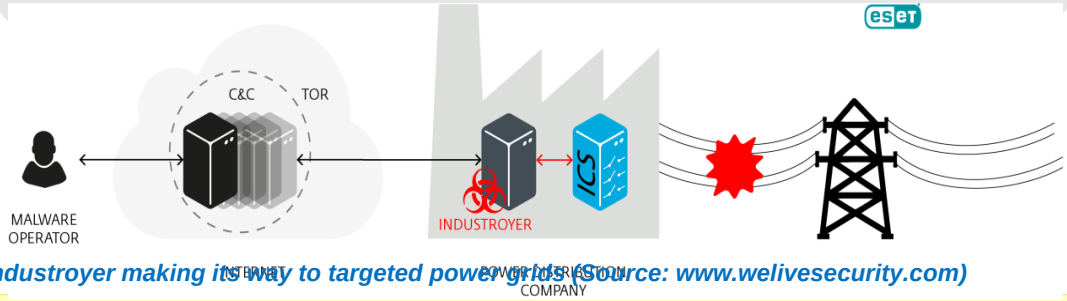
NATO ENSEC COE: Means/Research

NATO CEPS Cybersecurity Risk Study

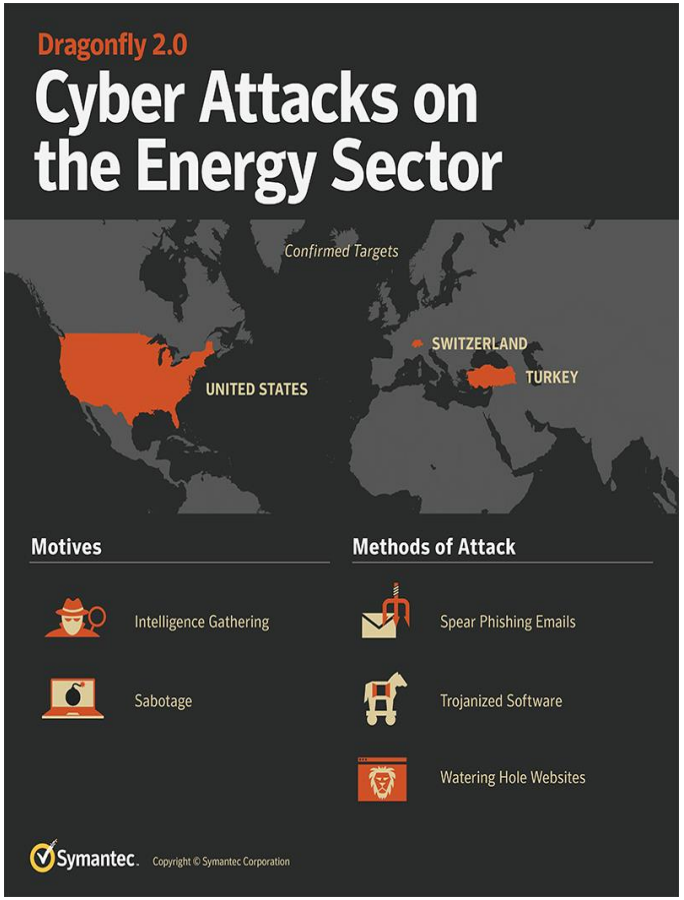


Cyber Threats against Critical Energy Infrastructure

- ***Sandworm*** **attacks against Ukrainian power grids led to blackouts in 2015 and 2016**
- **Extensive ransomware attacks against Ukraine since May 2017; group responsible likely linked to *Sandworm***
- ***Dragonfly 2.0*** **campaign has targeted the power sector in a number of European countries. Cyberattacks on US natural-gas pipeline operators**
- ***Sandworm*** **and *Dragonfly*** **likely state-sponsored actors**
- **Triton/Hatman targeted SIS in OT environment**



(Industroyer making its way to targeted power grids (Source: www.welivesecurity.com)

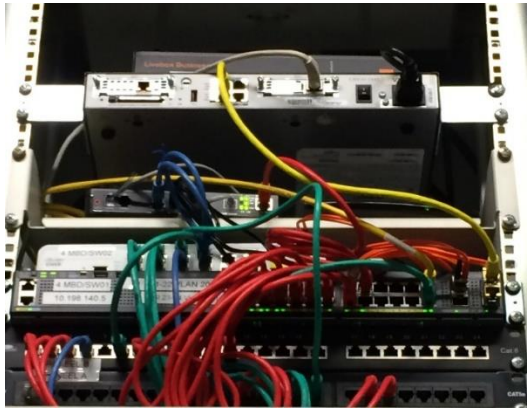


An outline of the Dragonfly group's activities in its most recent campaign (Source: Symantec)

The cyber threat against critical infrastructure not only affects the power sector but also other sectors such as oil and gas providers. It is highly likely that cyberattacks of this nature will continue – especially ones that help advance the goal of undermining or probing Euro-Atlantic cohesion.

Purpose

To evaluate cyber risks to CEPS industrial operations and propose recommendations on improving the safety and availability of CEPS in the context of the cyber threat environment.



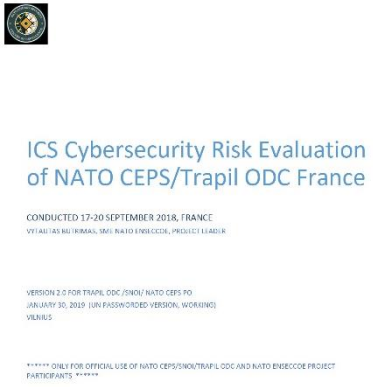
Scope of the study

Focus on the cybersecurity aspects relevant to the operational technology used to ensure the safety and availability of CEPS

1. National Dispatch Centers
2. Pumping stations
3. Storage facilities
4. Other sites (Seaport facilities) relevant to the safety and availability of CEPS

Methods/Progress

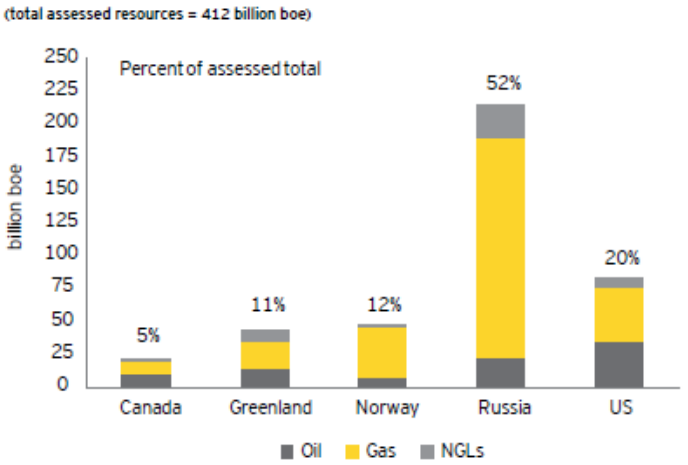
1. Four site visits (2-4 days on site) to 4 national operators
2. Completion of last Site Visit and country report
3. Comprehensive report due Fall 2019



NATO ENSEC COE: Upcoming works and projects

The implications of the access to energy resources and transportation routes in the Arctic for NATO energy security

- Energy resources in the Arctic region
- Costs and benefits of energy resources exploration and extraction in the Arctic region
- Transportation routes in the Arctic region
- The Arctic region: opportunities and challenges for NATO
- NATO's interests in the Arctic region
- The consequences of the EU and US sanctions on Russia for the energy resources extraction in the Arctic region
- The militarization of the Arctic region in the context of national strategies



LNG as Propellant for Ships Study

- **Liquefied Natural Gas (LNG) as an alternative propellant in the naval field**.

- Study focused on:

  - overview of state of the art
  - logistic implications and
  - technical solutions

  in NATO navies on using LNG
  as propellant for military ships.

- ENSEC's Doctrine and Development Division provides additional support.

Questions ?