11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS 2016

„CEIP and Energy Security in Perspective of NATO Energy Security Centre of Excellence“

Dr. Artūras Petkus

Head of Strategic Analysis and Research Division
NATO Energy Security Centre of Excellence

Framework for CEIP within NATO

NATO Warsaw Summit Communique (Art. 135)

- "<…> develop NATO's capacity to *support* national authorities in protecting critical infrastructure, as well as *enhancing* their **resilience** against energy supply disruptions that could affect national and collective defence, **including hybrid and cyber threats**."

- "<…> include energy security considerations in *training, exercises, and advance planning*. We will continue to *engage with our partner countries* where appropriate."

Strategic Foresight Analysis & Framework for Future Alliance Operations

- **SFA**:

There is an increased necessity to protect critical infrastructure, as it increasingly becomes part of how military capability is delivered, not just meeting a civil societal use.

- **FFAO** (instability situations/drivers)

Cyber Conflict - the cyber domain could develop in numerous ways in the future.

One possibility is that Cyber domain conflict tomorrow could look like that of today: high levels of crime and espionage but no massive cyber wars.

Another possibility is that the Cyber domain could break into national freedoms: with no one Internet, just a collection of national internets.

Cyber domain could also become an overwhelmingly secure place, as espionage, warfare, and crime have no hold.

Another possibility is that Cyber domain, always unruled and unruly, has become a “failed state” in a near-permanent state of disruption*.

*http://journal.georgetown.edu/wp-content/uploads/2015/07/110_gj124_Healey-CYBER-20111.pd

A proposed definition of “Critical Infrastructure” for NATO

CRITIS 2016

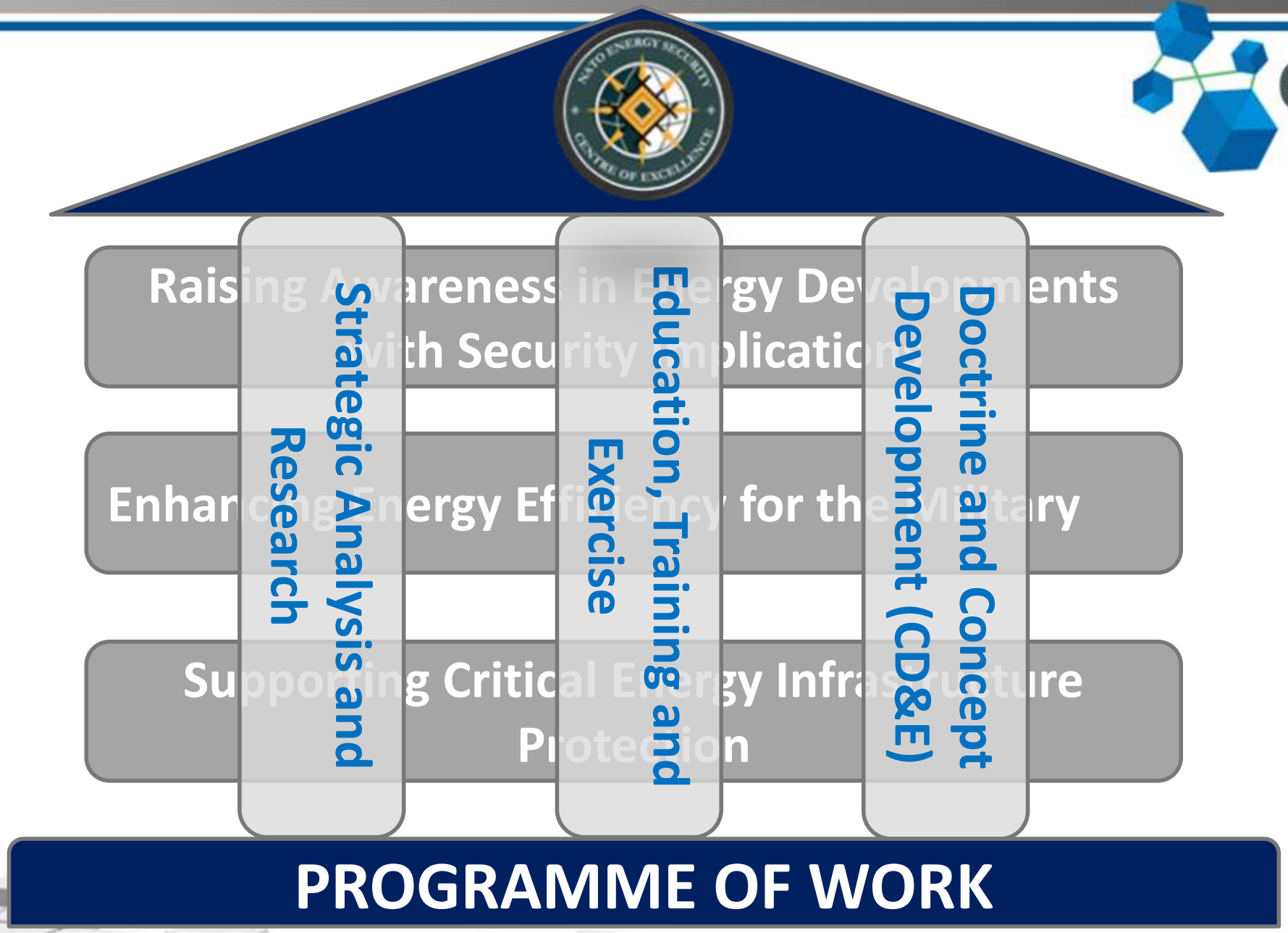
All services, facilities, and assets (physical and virtual) that play a decisive role in the success or failure of NATO’s activities worldwide.

The definition is inclusive of different objects that could be considered critical energy infrastructure, whether virtual or physical. The division between critical infrastructure and “normal” infrastructure is made and NATO’s international activities are highlighted by adding “worldwide” to the definition.

NATO ENSEC COE

- NATO ENSEC COE **established on July 10, 2012**;
  - **Lithuania** = framework nation;
  - **Estonia, Italy, France, Latvia, Turkey** = sponsoring nations;
- granted the status of International Military Organization and activated by **NAC on 12 October 2012**;
- inaugurated by NATO SG on the **6th September 2013.**

- **2014**: First enlargement: **UK** (Sponsoring Nation), **Georgia** (Contributing Partner);
- **2015:**  **Check Republic** initiated joining procedures, providing a VNC;
- **2016:**  ***USA* – (EUCOM) effective joining expected,**
   **Germany initiated joining procedures.**


Raising Awareness in Energy Developments with Security Implications
Enhancing Energy Efficiency for the Military
Supporting Critical Energy Infrastructure Protection
Strategic Analysis and Research
Education, Training and Exercise
Doctrine and Concept Development (CD&E)
PROGRAMME OF WORK

Main projects/researches/activities on CEIP in NATO ENSEC COE agenda

- **Studies** (On “Criticality” assessment, on Critical Energy Infrastructure and Cybersecurity)
- **Publications** (“Energy Security: Operational Highlights”; “Forum”)
- **Ad hock reports** (“SARDINES”)
- “Ukrainian project” (Contribution to **Green Book**; CEIP study…)
- **Conferences on CEIP** (Vilnius 2015, Warsaw 2016, Warsaw 2017…)
- **Participation and organization of specific training or exercises** (for military and or civilian)
  - Education;
  - Exercises, i.e TTX on CEIP;

NATO
ENERGY SECURITY
CENTRE OF EXCELLENCE

CRITIS 2016

Informative Notes on Energy Security

SARDINES 2016/1

Ukraine cyber-attack targets electricity suppliers

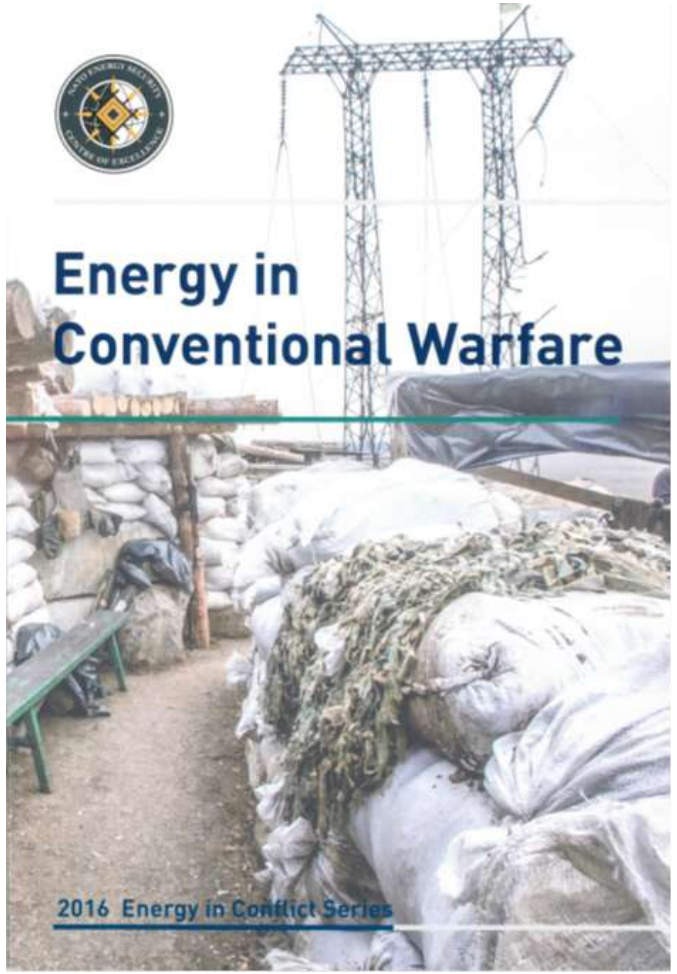
Larry Hughes and Jaroslav Hajek
NATO Energy Security Centre of Excellence
25 January 2016

On 23 December 2015, a number of Ukrainian electricity suppliers were subject to a seemingly coordinated cyber-attack which disrupted electricity supply across western parts of the country, including the central part of Ivano-Frankivsk, Horodenka, Kalush, Dolyna, Kosiv, Tysmenytsia, Nadvirna districts, and the Yaremche zone. Within a few hours, services were restored.

The disruption has been traced to the unexpected disconnection of customers from the electricity supply by the apparent automated opening of high-voltage circuit-breakers by control signals sent from the electricity-providers' SCADA (Supervisory Control and Data Acquisition) systems. While this can be done by an operator instructing the SCADA directly, it can also be done by software installed on the SCADA (for example, an immediate disconnection if certain conditions arise) [1]. This second feature is particularly useful in large networks if the operators are busy with other work [2]. However, it is this capability that allows an adversary to perform a cyber-attack on the electricity system.

Hybrid Conflict and Critical Energy Infrastructure: the Case of Ukraine

The task: based on Ukrainian experience, deliver an **analytical study** for NATO and partner countries to build **resilience** in energy sector; (2015-2017)



Hybrid Conflict and Critical Energy Infrastructure: the Case of Ukraine

- Study is on **military/terrorist** threat (& hybrid warfare) on energy infrastructure;
- Work out a **conceptual approach** how to build resilience in energy sector.
  - Propose **practical measures** for countries to resist these threats, to build resilience.

Experience and best practices sharing

Klaipeda (LTU) LNG Terminal Security Roundtable (12 December, 2014)

Aim: discuss the potential means of ensuring the safety and protection of energy infrastructure related to the LNG terminal.

Organizers:

- the NATO Energy Security Centre of Excellence
- the Ministry of the Interior of the Republic of Lithuania
- together with Joint Stock company ‘Klaipėdos nafta’ (operator)

Security proposals for LTU LNG terminal were based on good practices:

- at the Gate Terminal at Gasunie (Rotterdam) and
- future LNG terminal in Swinoujscie (Poland)

NATO-ICI Table Top Exercise on the Protection of Critical Energy Infrastructure (20-23 October 2014)

- ✓ Terrorist attack based scenario
- ✓ Cyber attack based scenario
- ✓ STRATCOM based scenario

Table Top Exercise on CEIP

- NATO Table Top Exercise on CEIP-2016

Challenges

- Find partners
- Find participants
- TTX planning conference
- Creation/development of scenario
- Execution of TTX
- Report on TTX

Exercise Specifications

❖ TTX on CEIP- 2016

- **Exercise Name:** Table Top Exercise on Critical Energy Infrastructure Protection – 2016 (TTX on CEIP-2016)
- **Theme:** Protection of Electrical Infrastructure
- **Region:** Baltic Sea Region
- **Scenario**: Skolkan Scenario

Exercise Specification

Exercise Aim:

To support national authorities in building resilience through improved emergency preparedness, planning, prevention, response and strengthen their capability to protect critical energy infrastructure and contribute to the development of NATO's competence in supporting the protection of critical energy infrastructure.

NATO ENSEC COE – TTX - Platform

Exercise Specification

Exercise Objectives:

- To analyze vulnerabilities of critical energy infrastructure
- To determine the consequences of failure, attack and/or damage to critical energy infrastructure
- To determine cooperation and coordination between military and civilian organizations
- To exercise crisis management processes, including military and civil emergency planning

PARTICIPANTS

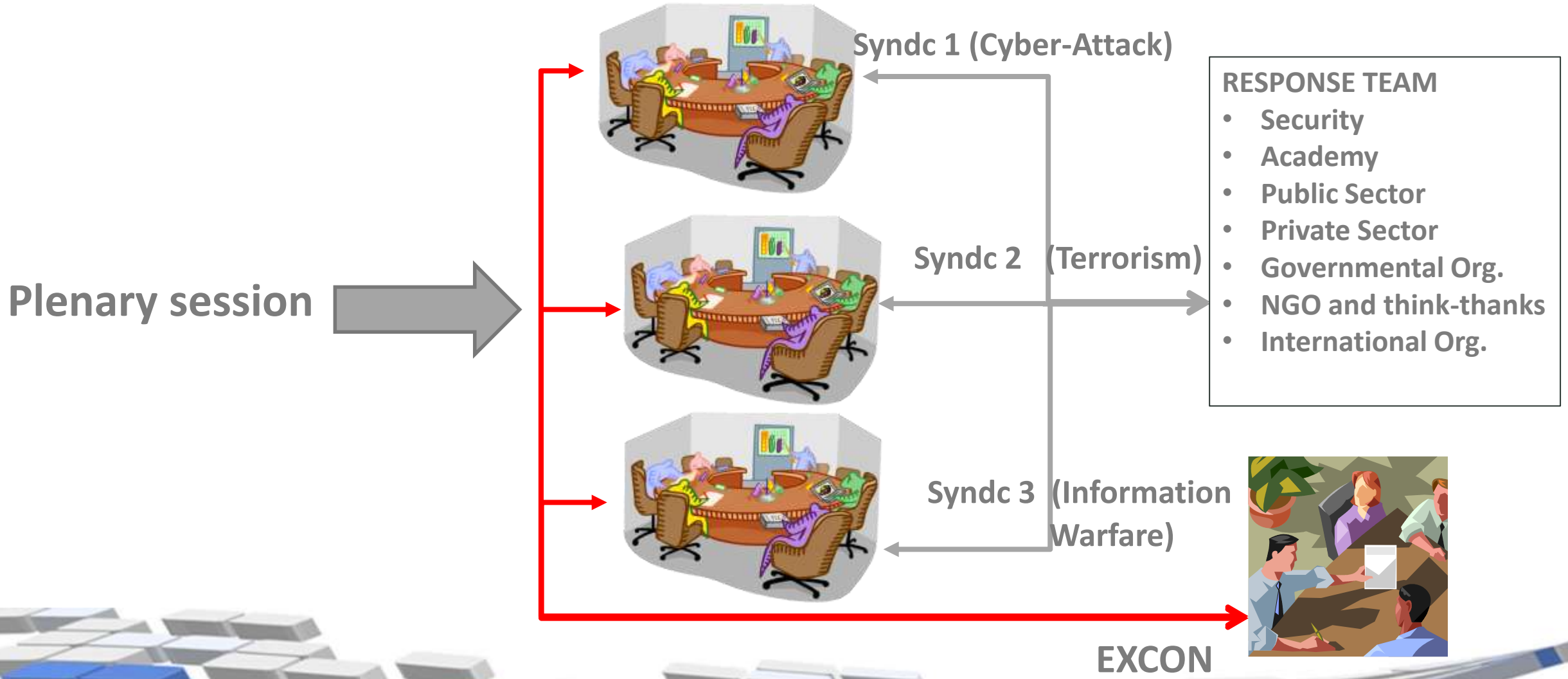
55 participants from 12 NATO member and partner countries;

- **Czech Republic, Estonia, Latvia, Lithuania, Poland, Slovakia, Spain, Turkey, USA, Finland, Sweden, Ukraine**

- **Security, Academia, Public Sector, Private Sector, Ministries, NATO Force (Multinational Corps NorthEast, NFIU LTU)**

- **Experts from NATO HQ, DAT COE, STRATCOM COE**

Execution of the Exercise



Outcomes

- Tangible recommendations for
  - ✓Managers of grids
  - ✓Security companies
  - ✓Policy makers
  - ✓…
- Contacts for cooperation
- Rising awareness
- LI/LL

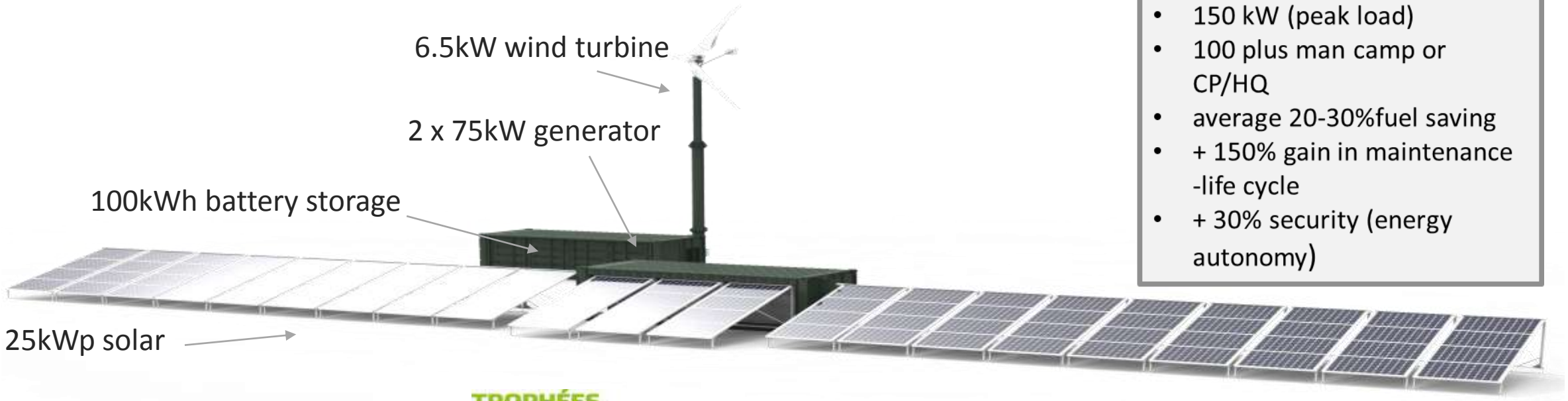
Deployable modular Hybrid Power Generation & management System - HPGS

CRITIS 2016

Foreign Affairs, Trade and Development Canada

System Performance:

- 2500 kWh/day
- 150 kW (peak load)
- 100 plus man camp or CP/HQ
- average 20-30%fuel saving
- + 150% gain in maintenance -life cycle
- + 30% security (energy autonomy)



HPGS is the winner of TROPHÉES DE LA TRANSITION ÉNERGÉTIQUE 2016 ***among 135 participants***

CRITIS 2016

NATO ENSEC COE
Šilo str. 5a,
Vilnius
Lithuania
http://enseccoe.org

...Thank you!

Dr. Artūras Petkus
Had of Strategic Analysis and Research Division
NATO ENERGY SECURITY CENTRE OF EXCELLENCE
Email: Arturas.Petkus@enseccoe.org
www.enseccoe.org