# CyberEDU Project

Oliver Popov – Stockholm University

Jacek Gajewski – NCBJ

on behalf of all project partners

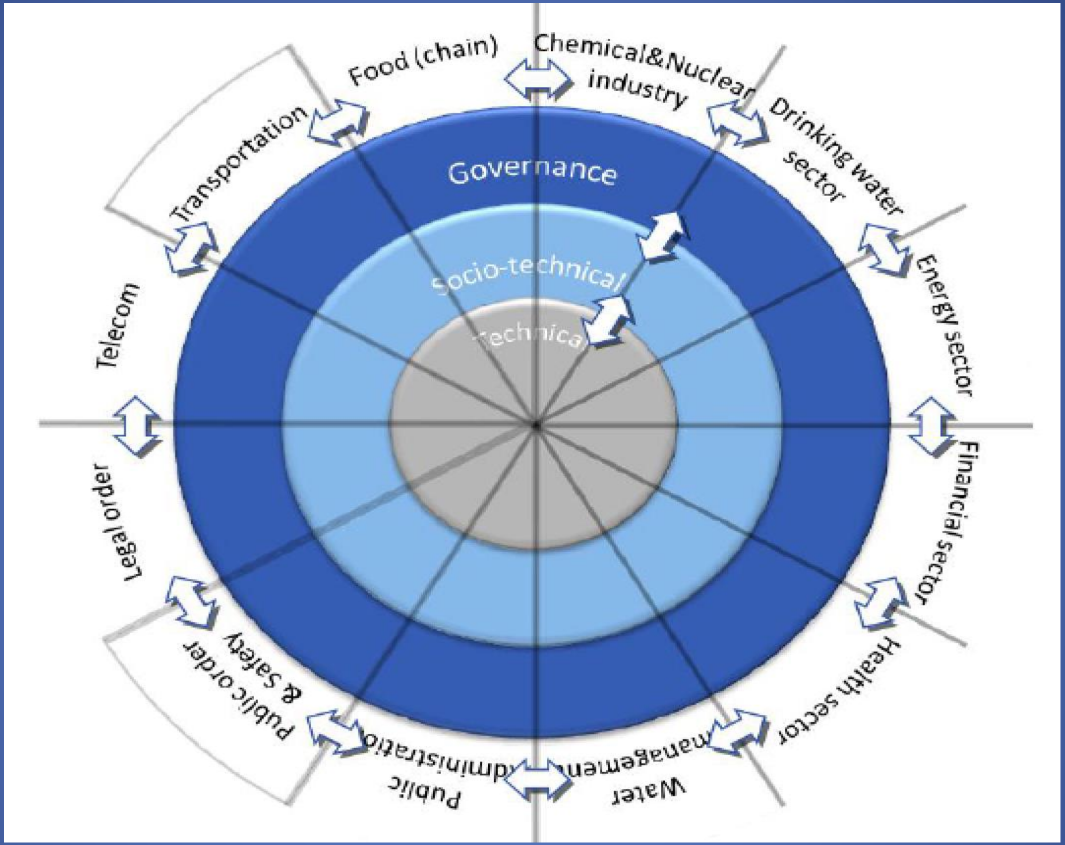
February 9 - 10, 2022

Tbilisi, Georgia

# *CyberEDU project: 2021 - 2022*

- *Baltic region and EaP countries – Sweden, Poland, Ukraine, Georgia, Azerbaijan*
- *Under the umbrella of and funding from the Swedish Institute (SI)*
- *Cyber security of Industrial CI in higher education*
- *Evaluating the state-of-play and the reflections among the industry, academia (including the students)*
- *Producing primers for graduate education*
- *Design few modules on CS of CII*

# Challenges



*Conceptualisation of cyberspace in layers and subdomains (Van Der Berg et. All, 2014)*

# *Challenges/2*

- ***Securing*** *cyberspace has been a long time* ***lagging behind*** *its constant* ***growth*** *in size and complexity.*
- *Research shows the* ***gap*** *can be* ***reduced*** *by increased* ***international collaboration*** *and knowledge exchange.*
- *The cybersecurity of information and the communication is well recognized, contrary to the cubersecurity if industrial systems. There are* ***very few*** *decent (or specifically designed and developed) and focused* ***programmes*** *in C-S of Industrial CI even in developed countries, they ary typically fragmented and distributed over a number of areas and disciplines*
- *There is a* ***need*** *for better* ***concentration and modularisation*** *for better interoperability between various areas ranging from computer science and engineering, taking into account the management, policy, decision making, and legal aspects.*

CyberEDU

# Consortium Partners

*A partner from Sweden and one from Poland,*
*two from Azerbaijan, two from Georgia, and one from Ukraine*

| Acronym | Full name | Country |
|---|---|---|
| **DSV/SU** | *Department of Computer and System Sciences, Stockholm University* | *Sweden, SE* |
| **BHOS** | *Baku Higher Oil School* | *Azerbaijan, AZ* |
| **ASOIU** | *Azerbaijan State Oil and Industry University* | *Azerbaijan, AZ* |
| **UG** | *The University of Georgia* | *Georgia, GE* |
| **GRENA** | *Georgian Research and Educational Networking Association* | *Georgia, GE* |
| **KhAI** | *National Aerospace University "Kharkiv Aviation Institute"* | *Ukraine, UA* |
| **NCBJ** | *National Centre for Nuclear Research* | *Poland, PL* |

# *Purpose*

- *Studying the current state of cybersecurity (graduate) education*
- *Exploring and defining the current and future needs of the*
  - *Academia*
  - *Industry, and*
  - *Public organisations*
- *Detailed examination of*
  - *The curricula, and*
  - *The gap*

*between the existing and desired practices concerning the interplay between*

  - *Research and education, and*
  - *Theory and practice.*

# *Purpose/2*

- *Raising the awareness about the role of cybersecurity in protecting the (national, regional and international) Critical Infrastructures*
  - *Cyber Physical Systems*
  - *Internet of Things (IoT)*
  - *Industrial Internet of Things (including the industrial control systems such as SCADA)*
- *Creating, developing and running (provided there is time) a test module of future "Cybersecurity of critical infrastructures" course, as a primer towards a complete cybersecurity graduate curriculum*

# *Situation Analysis (SI)*

- *SI fosters cooperation between Swedish academia and academia from the Baltic region and EaP countries via short-term projects and bilateral exchange of scholars and experts.*
- *Very few, if any, projects related to innovative cybersecurity research and education.*
- *Inducing a culture of collaboration*
  - *a unique opportunity for a multinational projects where each parttner brings unique perspectives and prospectives about the way we work*
  - *Occasional, diverse views on the importance and the place of cybersecurity*
  - *Individual and joint (shared) responsibilities to keep our infrastructures safe, secure, and resilient.*

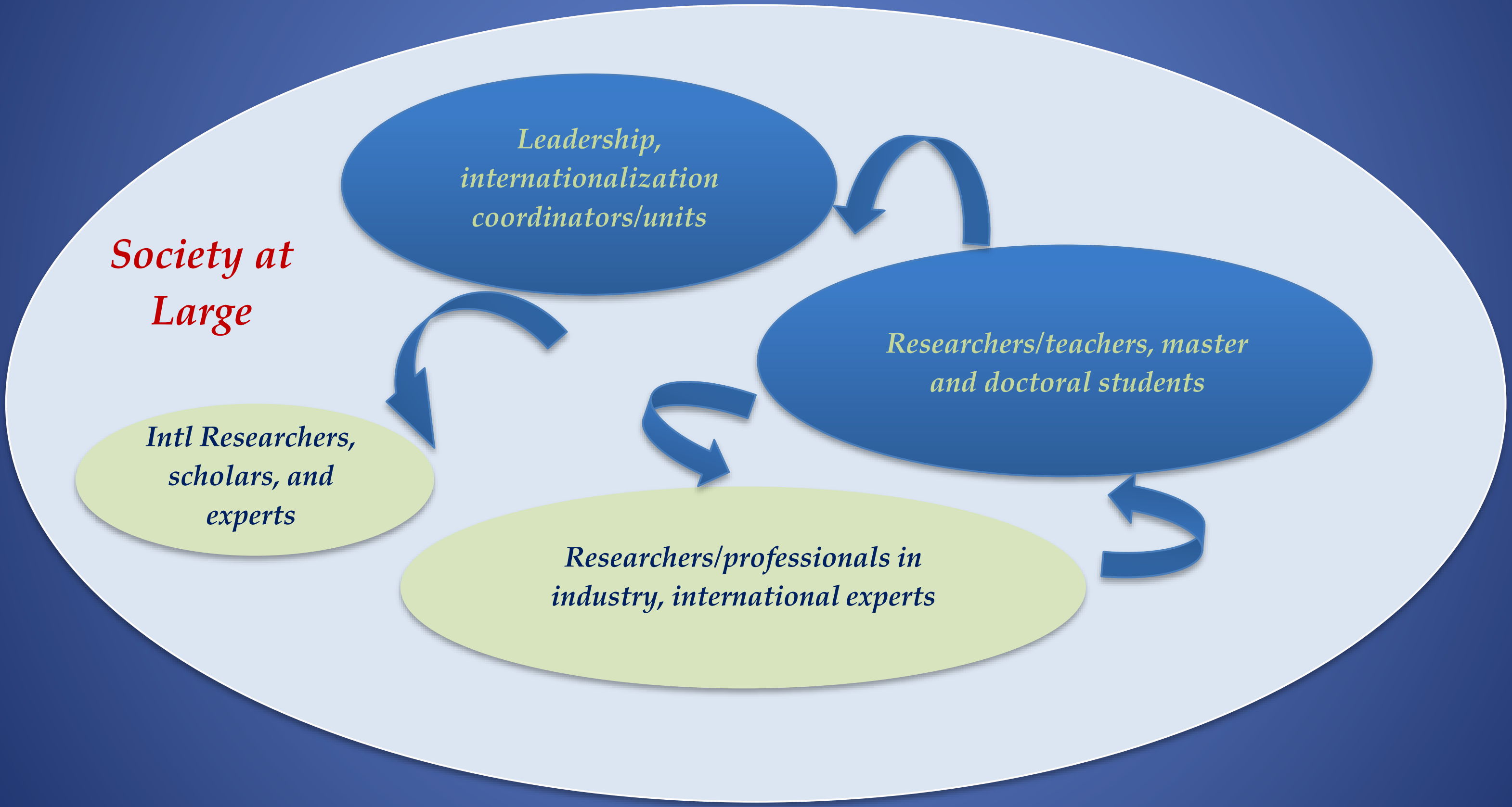
# Situation Analysis/2

- CyberEDU partners are either
  - Established state universities (ASOIU, KhAI) with links to critical infrastructures (in oil, aviation, and space industries), or
  - Private universities (UG, BHOS - specializing in high-tech and cybersecurity, including industry overtures).
- They all have computer science departments with labs based on advanced technologies and ambitious undergraduate programmes
- There is a strong interest and presence of the international industry players in cyber-physical systems such as ABB and Hitachi Energy Systems, Emerson, Schnider, and Siemens.

# *Situation Analysis (EaP)*

- *Strive for internationalization, yet in reality is still rather declarative with some Low-level activities*
- *The history of collaboration with Swedish institutions is short*
- *The absence of the research dimension in higher education (which is a Soviet legacy)*
- *Political tensions that have impaired the old relations with the Russian scientific communities*
- *Need to interface with EU and the rest of the word, where our partners are an integral part of and belong to*
- *While computer science programs are ambitious, usually, they are reduced to traditional curricula that do not include cybersecurity of CIs*

# Target Groups



Society at Large

Leadership, internationalization coordinators/units

Researchers/teachers, master and doctoral students

Intl Researchers, scholars, and experts

Researchers/professionals in industry, international experts

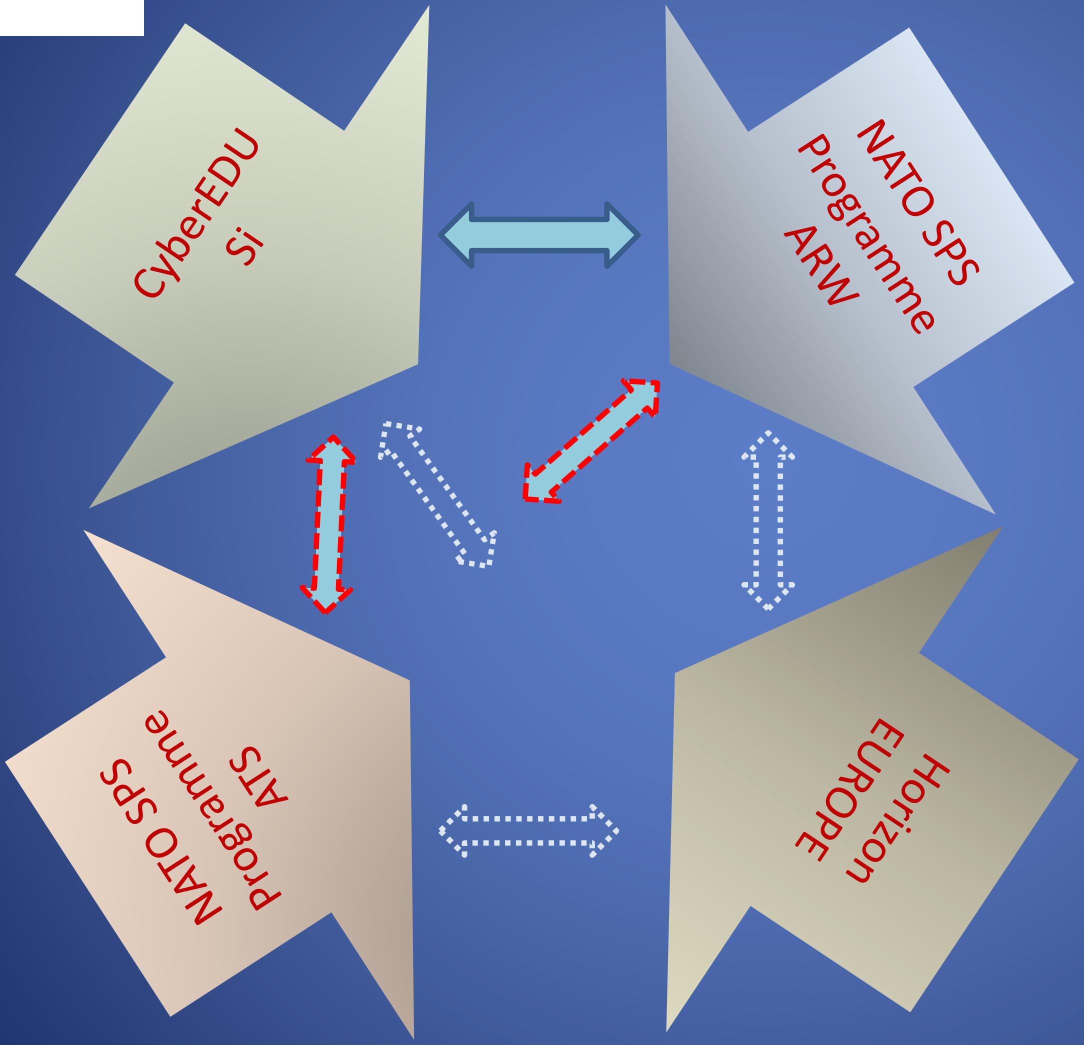
# *Target Groups/2*

- *The primary target group consists of the leadership of the partner institutions and the coordinators/organisation units responsible for internationalisation.*
- *The secondary target group includes the researchers/teachers in the area of cybersecurity at the partner institutions and the students studying cybersecurity at the master or doctoral level.*
- *The tertiary group involves researchers and professionals in the cybersecurity field, international experts in the area and the society at large.*
- *The position of the **international experts** is to increase the awareness about the needs in cybersecurity of national critical infrastructures and industrial control systems to become an integral part of the research and education programmes.*

# Current Status

- Existing graduate (two) and undergraduate programmes (three) related to cybersecurity **have been surveyed** and evaluated. Reviewing the final revision – deadline February 20, 2022, based on the comments from two-hour presentation and discussions.
- The **needs of the industry surveyed**, a draft of the analysis presented in the beginning of January 2022. The deadline is March 15, 2022 for the final review.
- The **current results** posit and firmly **reassert** both the need for cybersecurity on every level of **education**, with a strong **presence** and diffusion of the **research dimension.**

# Synergies, mutual drivers, initiatives



- *SI for EaP*
- *NATO SPS*
- *Horizon EU*

# *Programme of the NATO SPS ARW Baku, AZ 27-29 Oct 2021*

- *Cybersecurity of critical infrastructures (CIs)*
- *Cybersecurity research and education – programmes, projects, and labs*
- *ICS/PLC/SCADA testbeds and research facilities*
- *Vulnerability analysis, testing, and risk management*
- *Intrusion detection, mitigation, and prevention*
- *Digital and cyber forensics for CI*
- *Both NATO ARW and the CyberEDU confirmed the need of academic course on CS of CI*

CyberEDU

# *Thank you so very much*

- *For your attention and interest*
- *To all our partners for their contribution and the pleasure of working together*
- *To Si for their support.*

SI. Funded by Swedish Institute

Web site of the project: https://cyberedu.ncbj.gov.pl/home

An article about the project on GEANT connect: https://connect.geant.org/2021/10/20/cyberedu-project-a-strong-partnership-to-improve-the-education-of-cybersecurity-professionals

# NATO ARW->ATC->MYP

- During ARW in Baku,  NATO senior officials encouraged us to continue work on (education of) Cybersecurity of Critical Infratructures

- A possible scenario is to organize:

  (a) Workshop to design the concept of a full academic course (including laboratories) on CS of CI (preferred format NATO SPS ATC)

  (b) project to create, implement and test the course (preferred format NATO MYP)

# NATO ATC *(reserve: IEEE)*

- One week w/shop in Tbilisi, late 2022
- ~13 renowned scholars from NATO countries
- ~40 participants from EaP countries (incl. Country Rapporteurs)
- Plenaries + parallel sessions in 3 WGs:

*(1) State of the art in the cybersecurity laboratories, research and education; Possible set of courses for cybersecurity of critical infrastructure and their scope, form, delivery methods, language*

*(2) Needs of economies and societies for cybersecurity experts; Possible capacity building concepts: at University level: separate Master, addition to other Master programs, postgraduate/tertiary courses and at business level: external training companies and on-site trainings of CI staff*

*(3) Requirements from accreditation and qualification framework;*

*Possible funding mechanisms, programmes and projects.*

- Formation of Task Forces to implement the created concept

# *NATO MYP (reserve: Erasmus)*

General idea (to be modified by Task Forces):

- Three year project:  2023-2025
- Realized by wide consortium of universities from EaP Countries
- Each of the university should create 1-2 modules of a joint course
- After necessary harmonization the whole course it will be test-run in few universities with good laboratories
- Final (basic) course will be given to all consortium members for possible localization and modernization of their laboratories
- The improved course and the laboratory design will be available to all universities in EaP

# *Thank you for your attention!*

*In case of your interest, please contact:*

*Jacek Gajewski* ***jacek.gajewski@ncbj.gov.pl***

*Ramaz Kvatadze* ***ramaz@grena.ge***