EaP-Connect + CyberEDU workshop, 10-11.2.2022

International cooperation in Cybersecurity
(Horizen Europe and NATO SPS options)

Jacek Gajewski
NCBJ International Projects
Coordinator

NARODOWE CENTRUM BADAŃ JĄDROWYCH ŚWIERK

Outline

➢ NCBJ and its CyberLAB

➢ Cybersecurity and International Cooperation

➢ Programmes and Projects (funding options)

➢ International Organizations

➢ International initiatives

- Largest research institute in PL: 1118 FTE, 59 prof., 151 PhD, own PhD School, Hirsh index 141;

- International collaborations with largest laboratories (CERN, DESY, Grenoble, JParc, FAIR, Julich, ESS, JINR, etc), and many universities around the world;

- In 2020: 180 projects including 14 (H2020), eg. 15MEuro TEAMING; 10 (eg. IAEA, NATO);

- Two specialized Project support units, high success rate

CyberLAB created by IAEA CRP project

NCBJ Results/Discoveries

➤ **Found vulnerabilities:**

▪ IPV4 zero-day in S7-1500 Siemens PLC - reported via Responsible Disclosure Procedure (CVE-2018-13805);

▪ New OPC-UA vulnerability S7-1500 PLC (also found by Siemens CERT);

▪ Zero-day vulnerability in TM241CE24U PLC reported to Schneider Electric;

▪ NPP Simulator Asherah (result of the whole IAEA CRP collaboration)

▪ Simulations of cyberattacks on CIs

▪ Cyberattack detection methods (traffic analysis, honeypots)

➤ **Jacek Gajewski:**

▪ 1993-2010 CEENet Secretary General, NATO Consultant for Caucasus;

▪ 2016-2021 PL-CRP Project Leader, CyberLAB Principal Investigator;

NARODOWE
CENTRUM
BADAŃ
JĄDROWYCH
ŚWIERK

Cybersecurity and International Cooperation

➢ **Sophistication** of modern cyberattacks (many of **them cross-border** and/or politically motivated) & global interconnection created **the need for international cooperation**.

➢ Computer security incident response **teams (CSIRTs/CERTs)** are **key actors** to help the community prevent and respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training.

➢ Various international projects, organizations and initiatives have been suggested and implemented to foster the international cooperation of local CSIRT/CERT teams.

Example: Cyberattack on Georgia
(Courtesy: David Tabatadze, GRENA)

➢ **In end-July 2008 CERT international training in Tbilisi;**

➢ From Aug 9th, 2008 Georgia under heavy cyberattack;

➢ Approx. 90% of all gov.ge domain addresses and significant fraction of .ge domain addresses were affected by DDos attacks (e.g. president.gov.ge, mfa.gov.ge, government.gov.ge, www.parliament.ge);

➢ CERT-Georgia (part of GRENA) undertook obligation to operate as national CERT and made heroic effort to defend their country;

➢ **CERT-GE contacted CERT-Polska, which offered its help in preventing and filtering attacks; as a quick action they distributed information on attacks to more than 180 CERT teams and other security related bodies all over the world, which analysed the data. In particular, CERT-Estonia provided crucial help by sending their experts to Georgia.**

CI Cybersecurity – an important issue for EaP

➢ The most vulnerable facilities are **industrial systems**, designed with little thought to security.

➢ Critical Infrastructures (CI), often have the option for **remote access**, which can be possibly seized by an intruder creating a significant risk.

➢ As the EaP countries embark on modernization projects and the r**elations** with some neighbours are **tense,** their Critical Infrastructures (eg. Baku-Tbilisi-Ceyhan pipeline) were and are **likely to be be cyberattacked**.

➢ Building a modern **cybesecurity (c-s) education** and fostering **international cooperation** are key factors to increase the ability of EaP countries to protect their CI infrastructure.

➢ CI cybersecurity is now widely recognized as a topic for education and research.

➢ On international level CI c-s is handled by the same organizations as IT c-s.

Programmes, Projects, Funding opportunities

➢ NATO Science for Peace and Security (SPS) programme;

➢ EU Programmes;

➢ Other international cybersecurity funding agencies.

The NATO Science for Peace and Security (SPS) Programme

➢ Establish and promote <u>collaboration</u> (dialogue, practical cooperation) between **NATO and Partner** countries;

➢ Mobilize and enhance **R & D** capabilities in topics related to **NATO priorities** - includes: Cyber-Security (prevention, reaction, awareness in IT and OT systems, CI protection);

➢ SPS offers **funding and support** to **civil** security activities.

SPS Characteristics

➢ Applications are short and not complicated

➢ Rapid grant approval (when call is open).

➢ Low bureaucracy, easy reporting

➢ Four mechanisms available

➢ **Look around for project ideas and apply!**

Jacek Gajewski

NARODOWE
CENTRUM
BADAŃ
JĄDROWYCH
ŚWIERK

Support Mechanisms

ADVANCED RESEARCH WORKSHOPS

(ARW)

➢ Grants to organise **expert** workshops where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for **future actions** (e.g. MYP)

➢ 2-5 days, 20-50 participants, <40 000 Euro

Support Mechanisms

ADVANCED STUDY INSTITUTES (ASI)

ADVANCED TRAINING COURSE (ATC)

➢ Grants to organise high-level tutorials of latest developments in a given subject to an advanced-level audience;

➢ ASI: inviting professor with a series of lectures, summer schools, etc.;

➢ ATC: interactive, expert networking;

➢ Typically: 5-7 days, 20-50 pax, <60 000 EURO.

Support Mechanisms

SCIENCE FOR PEACE PROJECTS (MYP)

Grants to collaborate on multi-year applied R&D and Capacity building projects

➤ Duration: 2 to 3 years;

➤ Multicountry projects and the participation of young scientists are encouraged;

➤ Budget ~150-350 kEuro: covers equipment, computers, software, travels and trainings;

EU (HE) Programmes: Digital Europe (7500 Meuro)

Available document: Cybersecurity Work Programme 2021-2022

➢ Focus on needs of businesses, citizens and public administration

➢ Cybersecurity is one of 5 pillars of DE, with following objectives:

- **Developmen**t of advanced cybersecurity **equipment, tools and data infrastructures**

- **Spreading knowledge** and best practices, building capacity and skills

- **Deployment** of effective cybersecurity **solutions**

- Capabilities in support of the NIS Directive;

- **Building resilience**, risk-awareness, basics levels of cybersecurity;

- **Enhancing synergies** & coordination between the c-s **civilian** and **defense** sphere.

In Construction:

Cybersecurity Industrial, Technology and Research Competence Centre in Bucharest

Jacek Gajewski

EU Programme - Connecting Europe Facility (CEF)

3 CEF sectors: Energy, Telecom, Transport

Each of those sectors publishes „call for proposals"

Example of relevant call:

A Digitised, Resource-Efficient and Resilient Industry 2022

In most of the calls there are 1 or 2 cybersecurity topics

Jacek Gajewski

EU Programmes for non-EU countries

➢ Instrument contributing to Stability and Peace (IcSP), includes cybersecurity and combatting cybercrime

➢ European Neighbourhood Instrument (ENI), to help EaP countries to define strategic priorities related to the fight against cybercrime

➢ HE Widening Participation programme (high chances for success)

➢ Talk to your EUD: Technical Assistance projects possible through EuropAid -> International Partnerships mechanism.

Example: Az-RDI project (2018-2020)

NARODOWE
CENTRUM
BADAŃ
JĄDROWYCH
ŚWIERK

Cybersecurity programmes by other donors

- ➢ US National Cyber security Center (NCCIC)

- ➢ Regional Internet Registries: RIPE, APNIC,…

- ➢ OECD, IAEA, ISOC, IEEE, ITU

- ➢ G8 24/7 Cybercrime Network

- ➢ World Bank Global Cybersecurity Capacity Program

- ➢ External aid agencies (USAID, SI, …)

Cybesecurity-relevant International Organizations

➢ Inventory

➢ FIRST

➢ TF-CSIRT (Trusted Introducer, TI)

➢ ENISA

Inventory of C-S-relevant International Organizations

➢ Gov-level: UN: IGF, ITU, NATO/CCDCOE, ENISA, EDA, OECD, ASEAN, INTERPOL;

➢ Industry: Messsaging/Malware/Mobile/AntiAbuse WG, Network Operators Groups (NOGs);

➢ Community: FIRST, TF-CSIRT, AP-CERT, Internet Registries (e.g. Ripe), ICANN, G8 24/7 Cybercrime Network, Internet Society (ISOC);

➢ USA: National Cyber security and Communications Integration Center (NCCIC), US Technology Training Institute (USTTI).

FIRST
Forum of Incident Response and Security Teams

VISION:

➢ Bring together CSIRT/CERT 602 teams from 99 countries;

➢ Work together to limit the damage of security incidents;

➢ Build high level of trust among members.

MISSION:

➢ Global coordination (also with non-technical stakeholders);

➢ Provides platforms, means and tools for incident responders;

➢ Find the right partner to collaborate efficiently;

➢ Trainings how to react in a fast and efficient manner;

➢ Data transfer, machine-to-machine communication.

TF-CSIRT
Trusted Introducer

TF-CSIRT offers Public and Accredited Members' Services:

➢ Public: basic information about all teams registered by the TI (Points of contact, cryptographic keys, etc – no policies)

➢ Accredited (introduced) Members: in-depth operational data

➢ Secure chat, mailing lists

➢ Meetings and trainings

➢ **Incident Response coordination (with CERT Center)**

➢ Certification of teams and activities

➢ Technical: Public Key Infrastructure, PGP keys, Compendium

ENISA
European Cybersecurity(!) Agency

ENISA goal: **a high common level of cybersecurity in Europe Activities:**

➤ contributes to EU cyber policy (NIS directive)

➤ develops cybersecurity certification schemes,

➤ Prepares Europe for cyber challenges of tomorrow through:

➤ knowledge sharing – very useful documentation

➤ capacity building/trainings & awareness raising events,

➤ protection against cybercrime, especially in area e-commerce, e-payment, e-health;

➤ ENISA CSIRTs Network of Gov CSIRTs and CERT-EU: ENISA provides the secretariat and incident coordination.

Inventory of C-S-relevant International Initiatives

➤ EU initiatives: European Defence Fund, PESCO, ENISA CSIRT Network, EU Cyber Challenge;

➤ NATO initiative: Atlantic Council Staff Games;

➤ UN-ITU initiatives: National-CIRT support programmes;

➤ USA initiatives: US–ICS-CERT – ICS specific CSIRT;

➤ Good example of regional cooperation is APCERT;

➤ SIM3 – a model of cybersecurity readiness assessment;

➤ International games (maneuvres) Capture-the-flag, Cyber-EXE, Cyber-Fortress to train c-s Staff.

NARODOWE
CENTRUM
BADAŃ
JADROWYCH
ŚWIERK

Open CSIRT Foundation (OCF)

➢ The OCF fulfills the role of "Head Trainer" for TRANSITS trainings organised by GEANT.

➢ 4gh is a new type of Security Conference – small scale, for "hardcore security experts" (~highly trusted participants).

➢ Organizes „Certified SIM3 Auditor" trainings.

SIM3 Model
Security Incident Management Maturity Model

➤ CSIRT Maturity SIM3 Model is an indication of how well a CSIRT team governs, documents, performs and measures their function;

➤ Used by TF-CSIRT/TI for Certification of members;

➤ Used by ENISA for development of Gov-CSIRTs;

➤ 40 Maturity Parameters, in 4 quadrants (O-Organisation, H–Human, T–Tools, P–Processes), quantified maturity levels of 0-4.

NARODOWE
CENTRUM
BADAŃ
JĄDROWYCH
ŚWIERK

Conclusions

➢ Cybersecurity does not recognise borders and by its very nature needs international cooperatiion. This is very true for Caucasian region.

➢ CERTs/CSIRTs are essential tools to secure cybesecurity for a given domain or community.

➢ Cybersecurity is interesting research area and important topic for education, as the needs for experts sharply grows.

➢ There is plenty of international organizations and initiatives, which foster international cooperation in cybersecurity.

➢ ***Think about possible projects and educational programmes !***

Funded by Swedish Institute

CyberEDU project
2021-2022

Stockholm U., NCBJ, **ASOIU, BHOS**, Georgia U, GRENA, KhAI

Goals: - establish a network of cybersecurity experts

➢ Increase awareness, knowledge and practices in cybersecurity programmes

Activities 2021: - Explore current state of cybersecurity education

➢ Identify the needs of industry

➢ Actively participate in NATO ARW

Activities 2022: - Raise awareness for the protection of national CI and ICSs

➢ Enhance cybersecurity education with expectations of students and industry

➢ Create and run an online course module, "Cybersecurity of critical infrastructures"

➢ Organize CERT-staff training

➢ Define follow-up project(s)

CyberEDU

CyberEDU project
2021-2022

Stockholm U., NCBJ, **ASOIU, BHOS**, Georgia U, GRENA, KhAI

Message from the Coordinator, prof. Oliver Popov:

The overarching spirit of the CyberEDU project is internationalization, which advocates learning through friendly collaboration, complementary needs and competence, and different inter-cultural perspectives.

Thank you for your attention!

In case of interest and concrete project ideas, you may contact:
CyberLAB@ncbj.gov.pl

or me personally:
Jacek.Gajewski@ncbj.gov.pl

NARODOWE CENTRUM BADAŃ JĄDROWYCH ŚWIERK

www.ncbj.gov.pl