NATIONAL CYBERSECURITY QUALIFICATIONS FRAMEWORK

JUDR. PAVEL LOUTOCKÝ, PH.D., BA (HONS)

BASIC AIM OF THE PROJECT

- The main target of the project is research aimed at creating a universal and holistic qualification framework in the Czech Republic in the field of cybersecurity
- The framework will classify the individual qualifications and professional roles of cybersecurity personnel
- It should describe their required education, skills and will serve as a single basis for the development of capacities in this area in the Czech Republic

DIFFERENT AVAILABLE SCHEMES

- Not all of them are purely focused on qualification frameworks
- Overlapping with existing educational schemes

- What do we have now?
  - 1) NICE (NIST)
  - 2) ENISA (more focused on education than positions)
  - 3) Cybersecurity Curricular Guideline by ACM (educational and scientific computing society, uniting educators, researchers and professionals)

1) NICE (NIST)

- **National Initiative for Cybersecurity Education lead by National Institute of Standards and Technology**
- **Detailed material and the describtion of knowledge base of each area of cysec employee**
- **Detailed structure from general to specific**

- **Starting with general categories (7) moving to more detailed describtions:**
  - NICE Framework Workforce Categories
  - NICE Framework Specialty Areas
  - NICE Framework Work Roles
  - NICE Framework Tasks
  - NICE Framework Knowledge Descriptions
  - NICE Framework Skills Descriptions
  - NICE Framework Ability Descriptions

1) NICE (NIST)

Table 1 - NICE Framework Workforce Categories

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

1) NICE (NIST)

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf

P. 20 et seq.

2) ENISA

- European Union Agency for Network and Information Security
- *Roadmap for NIS education programmes in Europe*
- Not focused on qualifications so far
- Offering roadmap for education (2014)
- Other materials, but not always important for the project

2) ENISA

- **Roadmap for NIS education programmes in Europe**
  - Mapping available courses, programes
  - Mapping available materials, databases, educational information

  - Identyfiing gaps in education
    - Teachers (mainly basic, high schools)
    - Healthcare Scenarion
    - Data protection officers
    - SME scenario
    - Digital Forensics

https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe

3) ACM CYBERSECURITY CURRICULAR GUIDELINE

- **Very detailed material on personal aspects and areas (qualification)**
- **Many described curricular guidences are interconnected in more fields below (all is related to all)**
- CSEC2017 v1.0 manual was developed through the leadership of the Joint Task Force on Cybersecurity Education and the contributions of educators, industry professionals, and government representatives from around the globe.
- It includes 4 components:
  1. an overview of the cybersecurity discipline to frame the curricular model,
  2. a presentation of the curricular framework and outline of the recommended curricular content,
  3. a highlight of industry perspectives on cybersecurity, and
  4. a discussion of issues related to the educational practice, suggestion for a process to develop roadmaps that link the curricular model to workforce frameworks, and references that highlight how global institutions could implement the curricular guidelines.

3) ACM CYBERSECURITY CU RRICULAR GUIDELINE

- **Positions devided into 8 groups**
  1. **Data Security** (e.g. legal issues, digital forensics, evidence secure design, authentication)
  2. **Software Security** (e.g. modularity, security features, testing, patching, SW documentation)
  3. **Component Security** (e.g. components integrated in larger systems, supplies, software reverse engineering)
  4. **Connection Security** (e.g. sharing of data, standards, hardwarem, network monitoring)
  5. **System Security** (e.g. policy models, insider threat, identity, recovery, attacs)
  6. **Human Security** (e.g. identity services, social engineering attacs, psychological level of employees, systém misuse, cyber hygien, social aspects,)
  7. **Organizational Security** (e.g. risk management, privacy, ethics, security governance, cloud administration)
  8. **Societal Securtity** (e.g. cyber law – personal data, privacy, digital evidence, contracting; dilpomacy, breaches connected to legal aspects)

3) ACM CYBERSECURITY CU RRICULAR GUIDELINE

https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

P. 24 et seq.

BASIC CORNERSTONES OF OUR PROJECT

1. **Creating a taxonomy of qualifications** - analysis of existing solutions and research results abroad, investigation of needs within the security forces in the Czech Republic and identification of the character and structure of relevant entities in the Czech Republic. The necessary qualifications in both technical and non-technical fields at the level of both private organizations and the state will be offered in a structured manner.
2. **Design of Competency Model -** professional competencies will be assigned to the individual roles / qualifications – those should be concerned as prerequisite for performing the appropriate role in cybersecurity.
3. **Cybersecurity Qualifications Framework** - the Qualifications Framework will include proposed taxonomy and competencies of individual qualifications, extended in the manner to identify the required training capacities based on the existing demand for qualifications.

BASIC CORNERSTONES OF OUR PROJECT

4. **Analysis of available education in the Czech Republic** - based on surveys and questionnaires, the current offer of available educational programs, courses and exercises in the field of cybersecurity will be identified, which can be used to build the necessary capacities described in the framework.
5. **GAP analysis** - the training requirements described in the framework with the existing offer will be compared. Based on this comparison quantitative and qualitative gaps in terms of available cybersecurity education should be identified.
6. **Action plan on building educational capacities** - in order to effectively implement the results of the project, the aim will also be to develop an action plan to inform users and target groups about the practical application of research results at the level of support and development of cybersecurity training, recruitment and evaluation.
7. **Interactive Software for Qualifications Framework** - in order to effectively implement the Qualifications Framework, an interactive software tool will be created to provide knowledge databasis.

4 PHASES

1. initial research will be conducted to identify the available approaches to the taxonomy of roles / qualifications in cybersecurity.
2. individual qualifications will be described by the general information on the role and will be shared between qualifications to ensure the substitutability of individual roles.
3. then it will focus on putting previous results into practice. To this end, an action plan will be developed which will propose systematic actions that can be taken at the level of the state, private organizations and research institutions to support the development and application of the available cybersecurity workforce.
4. an information system will be developed to work with the taxonomy and qualifications framework. The proposed software will allow the expert public to access, systematically search and use the qualification database to achieve the objectives specified in their project. It will also allow to manage, maintain, add more qualifications to this system.

FURTHER PLANS

1. Language mutations (CZ and ENG)
2. Database of qualifications
3. Inspiration for education…
4. … and more

Inspiration in other shcemes:

https://www.sans.org/cyber-security-skills-roadmap

Thank you for your attention

Questions?