Information & Security

P. Varbanov
vol. 53, no. 2 (2022): 177-190
https://doi.org/10.11610/isij.5312

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Perspectives in the Design of a Modern Cybersecurity Training Programme: The ECHO Approach

Pavel Varbanov [1, 2] (✉)

[1] *European Software Institute – Center Eastern Europe, https://esicenter.bg/*

[2] *Institute of Information Technology and Communication-Bulgarian Academy of Science, Sofia, Bulgaria, https://iict.bas.bg/*

ABSTRACT:

The paper leverages the training and education-related research outputs developed under the ECHO project. They are compared to the progress of the workgroups in ENISA (European Union Agency for Cybersecurity) and ECSO (European Cybersecurity Organization) that classify, structure and define the competencies, skills, and knowledge and risk factors. The approach digested by the ECHO project explores the methods for achieving a more vital balance between the market demands and talent supply. The scope of the research activities covers four main and interconnected components – i) Contextualization; ii) Competences; iii) Generic Curriculum; iv) Assessment methodology. The proposed approach explores and gradually builds upon the generic definitions of the skills and knowledge toward specific requirements on what an ICT or cybersecurity professional must know and be able to do in order to implement initial and further cyber-incident response actions. The paper considers mainly the design methods for building cybersecurity training programs for professionals. Still, it could be applied in academic settings as well, enriching the academic programs with practical learning experiences. Several examples are provided to demonstrate the relevance and applicability of the proposed methods.

ARTICLE INFO:

RECEIVED: 24 JUNE 2022
REVISED: 25 AUG 2022
ONLINE: 22 SEP 2022

KEYWORDS:

cybersecurity skills, competencies, training program, framework, design

✉ Corresponding Author: E-mail: pavel@esicenter.bg

Introduction

Human capital is at the heart of strong and resilient cybersecurity practices. Regardless of the professional background of employees, the rapidly-expanding digitalization in all sectors of society and economy implies the need for a well-structured, practical and yet research-informed approach to providing individuals, organizations and entire sectors with the instruments necessary to develop cybersecurity knowledge, skills, and competences. The ECHO project proposes analytical and cyber-risk informed tools to identify the existing gaps in the preparedness of the personnel to perform cyber-defence related tasks and practical learning tools to fill those gaps.

The European Cybersecurity Organization (ECSO) explores the gaps in the training/education programme design[1] from two perspectives – the challenges in the formal education (HEIs mainly) and those faced by the professional training providers. Although the HEIs and professional training providers serve two different types of needs – acquiring detailed fundamental knowledge in a particular subject and application of the acquired knowledge for solving specific problems – the services that they both provide to the market need to address the balance between the ability to perform specific operational and technical tasks and the attitude to approach the problems in a systematic and holistic manner. Moreover, due to the high competitive environment, the formal education institutions and training providers offer, usually, generic, standard-based programs rather than searching and exploiting flexible and adaptable learning methods and tools. Thus, the multidisciplinary character and the essential importance of the cybersecurity domain as horizontal challenge should be considered in all socio-economic fields. The HEIs and professional training providers are required to work in collaboration for providing a product that meets the market demand and save to the customer additional investments in training and education. More extensive knowledge and related toolsets for acquiring this knowledge should be created for the professionals in all industries to equip them with tools for effective reaction of cyber-incidents taking into account their roles in the incident response lifecycle together with the security operations centers and emergency response teams.

The ECHO Cyberskills Framework (henceforth mentioned also as “E-CSF”, “ECHO Cybersecurity Skills Framework” or “the Cyberskills Framework”) address the gap between the market expectations and the results of training products, both within the framework of the ECHO project, as well as within the scope of relevant EU initiatives. ECHO proposes a more profound reference model for design of programs for capacity building. The leveraged modular approach fulfilled with the other solutions developed under the project (the platform for information sharing and threat intelligence ECHO-Early Warning System, its plugins, the sectoral and inter-sectoral prototypes and cyber ranges), used as training tools, allows the stakeholders to achieve flexibility in the design of the training products, as well as to find a good balance between theoretical and

practical learning experience. The ECHO's experience demonstrates the collaboration between academy, industry and life-long learning providers in building training products that meet the needs and capabilities of the stakeholders.

George Hatzivasilis et al.[2] approaches the multidisciplinary nature of the cybersecurity domain in the design of adaptive to various training needs tools and procedures through combination of pedagogical methods for building knowledge and cyber modelling (cyber-ranges) for continuous acquiring the skills required for performing the cybersecurity functions. Although, the authors focus on the constant evaluation of the learning progress for provision of a gradual learning experience, many common features with the ECHO approach could be found. The attitude towards ensuring deeper overview, including human, organization and technical aspects, on the existing cyber-risks, the need of providing training to different type of job roles for responding better the cyber-threats, combination of knowledge-building and skills-development training methods, exploitation of different delivery tools etc. fully match the ECHO principles. However, the ECHO training results and methods are enabled and inspired by the common and specific sectoral and transversal cybersecurity challenges and opportunities. Also, the ECHO's emphasis is on the significant importance of the identification and prioritization of the training needs through mapping the existing competence descriptors and knowledge areas with risk and threat related categories such as assets, vulnerabilities, threats, impact, attack vectors, and security controls, i.e., the mapping method is used not only for the training design but also for the identification of the demand. And last but not least, ECHO proposes an ontology model for better informing the decision-making and training-building processes.

The next section presents the methods used in the classification of the domain of cybersecurity knowledge and skills as well as the intersection with other categories that could support the adequate evaluation of the training needs. The following chapters inform about the structure and leverage of the E-CSF, explaining the classification principles adopted by the ECHO project, the components of the Cyberskills Framework, and how those components are applied in the creation of a pool with instruments for educators and program designers to address the sectorial, multidisciplinary and essential challenges of the cybersecurity knowledge and capacity building.

Methods and Principles in the Identification of and Addressing the Training Needs

The methods and principles selected for the building of the E-CSF supports two main challenges ahead for the training designer – i) to improve the identification and prioritization of the training needs and ii) to propose the most effective tools for addressing these needs. To achieve the first goal, the ECHO consortium performed three major tasks: 1) *grouping the existing competence standards* and frameworks around three dimensions - *narrower Cybersecurity-Focused Frameworks,* which are the most fragmented frameworks where the users could find the most detailed descriptors of the cybersecurity skills, knowledge

and competences (NICE-NIST,[3] SPARTA's Cybersecurity skills framework,[4] CyberSec4Europe's Education and Professional Framework[5]); *mid-range frameworks* which cover broader domain, e.g. ICT or computing, where the user still could extract more generic cybersecurity related descriptors and where the correlations and dependencies with the broader area could be found (e-CF,[6] Info-Comm Technology[7]); and *broader frameworks* (ESCO)[8] where specific cybersecurity descriptors of skills and knowledge are assigned to professional profiles from the entire spectrum of the occupations in Europe. This step explores the question which cybersecurity challenges can influence the critical operations in the other professional domains and which are the essential knowledge and skills that the professionals in those domains need to possess for protection of their organizational assets, e.g. identity management, data security and privacy protection for database administrators in hospitals, distributed systems security for system administrators in energy supplying companies and maritime transportation etc.

The second task is **the analysis of the risk management and risk assessment categories**. A pre-developed set of use-cases and scenarios enables the training designers in proper identification and prioritization of common, interdependent and unique for each sector or organization *assets, vulnerabilities, threats, incidents and countermeasures*. This step enhances a very precise targeting of the training needs and development of interconnected training services that address these needs. The identified categories could be further classified and aligned with the existing taxonomies (Technical Guideline on Threats and Assets,[9] JRC Cybersecurity Taxonomy[10]) that contributes to the establishment of a common understanding in the domain.

The third and last activity is **mapping** (1) the tasks, skills and knowledge descriptors to (2) the risk assessment categories. This effort enriches the existing generic skill and knowledge descriptors with the critical assets that need to be protected or recovered, their inherent vulnerabilities, and the threats that can be exploited. In addition, this mapping allows extraction of specific learning objectives that cover specific knowledge areas and topics to structure target-oriented training programs and to develop the essential content and tools.

For the addressing the second challenge of the training designer, the ECHO's training toolkit contains theoretical modules implemented as **e-learning activities** within a moodle environment, **cyber range exercises** implemented in a simulated environment deployed by industrial partners or independent training providers, and **tabletop exercises** on threat hunting, threat intelligence and cybersecurity information management implemented with the leverage of the ECHO-Early Warning System. All these tools, taken together or as independent components, depending on the expert evaluation of the training designer, can build a complex personalized learning experience that addresses the current cybersecurity challenges in front of an industry or an organization.

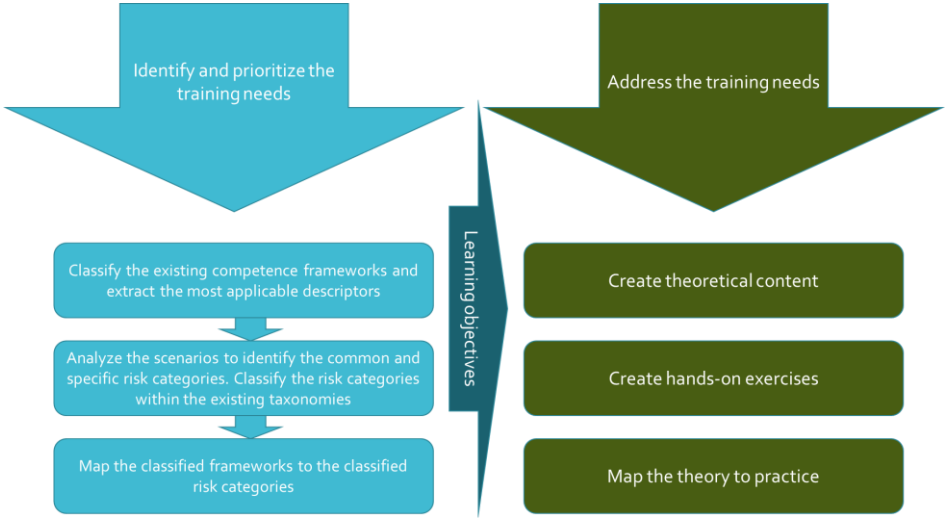

Figure 1: Risk-informed approach for the identification, prioritization of, and addressing the training needs.

The main principles followed by the ECHO consortium in building the framework and based on its curricula are in line with the identified challenges. The leading perceptions of the ECHO training and education efforts are oriented mainly towards accounting for the different industrial and organizational settings and enriching the approaches taken by the existing competence frameworks.

Addressing the limitations of small and medium-sized organizations that could not afford to maintain their own security operation centres and cybersecurity professionals requires involving as many professionals as possible in capacity building activities. Thus, the stakeholders will be prepared to actively contribute to their capacity-building actions and strengthen the national cyber-defence forces.

Semantic and expertise-based mapping of generic competency concepts to specific contexts, systems, and organizational structures aims to provide the professionals who are responsible for the protection of ICT and operational assets with the necessary capacity and capabilities to design, develop and establish adequate security controls as well as to react properly to cyber incidents and events.

Building **an overarching reference scheme for cybersecurity competences** that maps the skill definitions to the sector-related risks allows constant enrichment and update of the training products. Thus, the relations between competence descriptors and risk categories reveal interdependencies between the sectors and categories as well as the granularity of the skill definitions.

The ECHO Cyberskills Framework *builds upon the results of the EU initiatives for creating a shared understanding* of the development and application of the cybersecurity domain with a proposal for a vertical approach to the generic taxonomies and models.

In the delivery of the ECHO Training programs, the ECHO consortium considers the simulation-based hands-on exercises as the most powerful instrument for enhancing the learning experience that completes the knowledge building. It is a well-known approach in medical, engineering, and military studies to the instruction of domain-specific skills, knowledge, and abilities, along with 21st-century skills, such as problem-solving skills, creativity, and critical thinking.[11] Through simulation-based learning, the participants are offered a controlled, fault-tolerant, and scaffolding-offering environment, where learners could practice pre-existing knowledge and concepts along with learning the implementation of its principles and the consequences of their application.

The structure of E-CSF

The ECHO approach in collecting and structuring learning outcomes focuses on the analysis of commonalities, specifics and transversal aspects within 3 industries – energy, healthcare and maritime transportation. The scenario exploration provides context to the existing generic multi-purpose knowledge and skills definitions. It is the foundation of the ECHO training model.

The E-CSF consists of 4 main components: 1) **the contextualisation model** that leverages the ECHO Use Cases and ECHO Multisector Assessment Framework, 2) **learning outcomes** that are based on the descriptors (examples) in the existing competence models, mapped with the categories from the contextualization model, 3) **a generic curriculum** that includes sector-specific, but still, general training scenarios and 4) **an assessment methodology** that evaluates the results of training programmes from a learner's perspective and an organisational perspective.

The first component, the context, involves:

Identification of sector-specific **assets**, e.g. for the energy sector they could include:

Operational technology in Energy/ Water supply companies – PLCs, SCADA systems - this instance is compatible with *Operational support systems* and *Buildings and physical security systems* from the ENISA's Guideline.[9]

Energy monitoring, security and safety systems - this instance is compatible with *Operational support systems* and *Buildings and physical security systems* from the ENISA's Guideline.[9]

(Shared) **ICT infrastructure** - this instance is compatible with *Interconnection points*, *Operational support systems,* and *Buildings and physical security systems* from the ENISA's Guideline.[9]

The organizational assets in focus for the ECHO Cyberskills Framework are the ICT assets in a company (operational technology and information technology) and the professionals (job profiles) responsible for operating those assets.

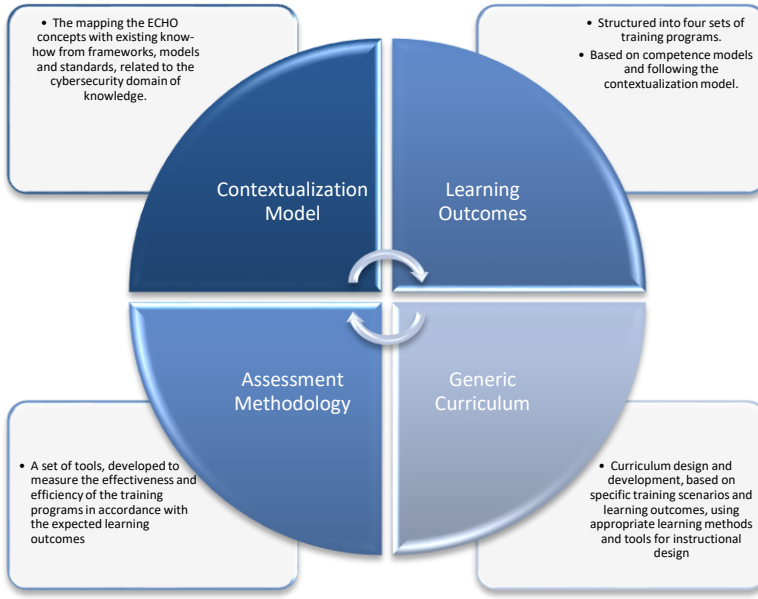

Figure 2: Main Components of the E-CSF.

The next step is identification of the **vulnerabilities** that could be exploited by a threat actor in the use-cases and scenarios. The technology-related vulnerabilities in the healthcare sector, considered in the ECHO use cases and scenarios with a potential to threaten human life or patient privacy can affect, for example, implantable medical devices. They are vulnerable to *off-the-shelf software vulnerabilities, remote access* and *use of old and unpatched software.* The asset related failures that could affect hospital or healthcare organization's operations are the medical/ clinical and enterprise networked systems. The reasons for successful hacker attacks could be *the lack of network segmentation, lack of encryption of data and information, use of old and unpatched software and operating systems, slow or absent security patching cycles and security misconfigurations, reliance on unsecured medical protocols and design deficiencies.*

Identification of the most common **attack vectors**, leveraged by the malicious actors for gaining access to the targeted system is one of the following steps in the analysis but from this point on the analyst could consider them in a different sequence. Among the attacking techniques are: social engineering, phishing campaigns, ransomware campaigns, spoofing a web system, eavesdropping etc.

Identification and prioritization of **threats and impacts** present other aspect from the contextualization of the learning objectives. Different assessment frameworks and practices can be used for the risk calculation and prioritization. The ECHO consortium considers the treat intelligence and information sharing platforms as an integral part of this process. The correct prioritization of the

risks and the appetite of the organization for taking these risks are critical for planning the resources for avoiding and mitigating the related risks.

When the cyber-analyst identifies the risks and determines the risk appetite of the organization, the planning of **countermeasures and security controls** comes at the end. Valuable input in this phase of the risk assessment was provided by the ECHO team that developed the multi-sector assessment framework.

The identification and prioritization activities are followed by mapping of their result to the generic competence descriptors. Within this phase the risk components and countermeasures should be connected with the cybersecurity knowledge and skills required from a professional to implement the countermeasures or security controls. The final goal is to create a training program or training pathway that satisfies the identified needs/ gaps and provide potential learners with stable knowledge and skills to protect the organizational assets or mitigate related risks. The mapping is performed based on expert evaluation of collected information, semantic principles, or upon stakeholders' guidelines and recommendations.

The table below includes the identified risk components in a scenario of an attack against the navigation system on a ship.

Then the educator can propose several appropriate knowledge and skills needed for the active implementation of the security controls in an operational environment (in our case they are extracted from NICE-NIST Framework):

K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.

K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

K0004 Knowledge of cybersecurity and privacy principles.

K0005 Knowledge of cyber threats and vulnerabilities.

K0006 Knowledge of specific operational impacts of cybersecurity lapses.

K0007 Knowledge of authentication, authorization, and access control methods.

K0620 Knowledge of continuous monitoring technologies and tools

K0041 Knowledge of incident categories, incident responses, and timelines for responses

K0133 Knowledge of types of digital forensics data and how to recognize them

S0340 Skill to monitor target or threat situation and environmental factors

S0371 Skill to respond and take local actions in response to threat-sharing alerts from service providers

Table 1. Extraction of risk components from an attack scenario.

Asset	Vulnerability	Threat	Impact	Countermeasures
ECDIS console	Network topology	Change of configuration file	Ship navigation and safe floating	Events Analysis Malicious Code Detected Event Information Sharing Response Plans Forensic Analysis
Media server	Network topology	-	Ship navigation and safe floating	Network monitoring Penetration Tests
Service server	Network topology	Unauthorized access	Ship navigation and safe floating	Network monitoring Penetration Tests
Internal Gateway	Network topology	Bypassing security controls	Ship navigation and safe floating	Network monitoring Penetration Tests
External Gateway	Network topology	Bypassing security controls	Ship navigation and safe floating	Network monitoring Penetration Tests

Starting from the identification of high-level generic descriptors that proved their efficiency in a variety of contexts, the educators need to enrich them to specific requirements and objectives that could be achieved with a short (3 to 5 days) course consulted with cyber domain experts and the experts who work with the specific systems in other domains.

Thus, the "*K0001 Knowledge of computer networking concepts and protocols, and network security methodologies"* from the NICE-NIST Framework could be formulated as "*To understand in details the network topology and network protocols deployed on a ship as well as the security controls that could be established and implemented"* or "*To be able to describe the network topology deployed on a ship and identify potential configuration gaps"* leveraging the Blooms Taxonomy verbs.

After the definition of the learning objectives the training designers and domain experts structure the learning experience that could be provided to the learners. At this point, the educators are able to evaluate their capacity to deliver the specific training service to satisfy the customer needs. The identified risk components during the first phase address the development of the requirements for hands-on exercises (identified assets deployed within a cyber-range

exercise or the threats as a basis for the development of injects for a tabletop exercise).

Within the ECHO project more than 50 use-cases and scenarios were explored which enabled the development of an extended analysis of common and specific risk components in the energy, healthcare and maritime domain. The results were structured in four **generic training curricula** – three specific programs that concern the unique and some common risk factors in each sector and one transversal program in information security for project managers. Those curricula could be defined as the generic base for the development and implementation of a pool with learning objective-oriented tools (e-learning content, cyber range scenarios, tabletop exercise scenarios and injects, laboratory demonstrations) scaffolded as training modules that fit to the five functions in NIST Cybersecurity Framework (IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER).

Leverage of the E-CSF for training program design

The E-CSF is built around the concept of modularity. The training modules built upon the framework ensures its flexibility, reusability, and adaptability of the content and tools to the different training needs. These building blocks are compiled and connected with a set of learning outcomes and learning experiences focused on real-world offensive and defensive scenarios. Thus, the educators are enabled to maintain the consistency and continuity of the training process starting with the generic or sector-specific modules (Introduction in cybersecurity, privacy and information security principles and concepts, Cybersecurity implications in the maritime sector) and framing the program with scenario or function-based modules (Detection of ransomware in hospital settings, Intelligence and analysis of Indicators of compromise in a network part of which is a SCADA system using Squert).

The instructional designers and educators can use the developed, content, instruments and methods within the modules to design new training programs or update their existing training services by selecting from the existing pool to meet specific use-case-driven demands. As an important element for the analysis of the achievements and learning experience are the assessment techniques. They serve to measure the quality of the provided service from the user experience point of view at individual, team, and organisational levels.

This figure visualises the work process in creation of a training course and the content of each separate component of the E-CSF.

The combination of methodological tools, theoretical and practical learning content meet several customer demands:

- adequate addressing the training needs in an organization/ team;
- effective learning and capacity building for the staff in an organization;
- development, establishment and testing policies and procedures in an organization.

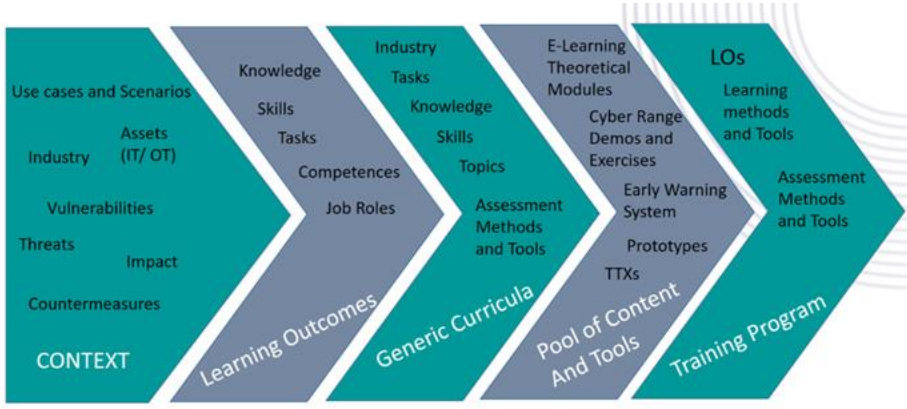

Figure 3: Detailed workflow and content of the components of the E-CSF.

After building the ECHO-Cyberskills Framework and its content components, the service design process follows. The activities included inside follow the chronological order:

- the identification of the relevant scenario or use case applicable to a particular customer or industry;
- defining the learning objectives that answer the following questions:
  - what the responsible experts should know and be able to do to avoid the scenario or mitigate the consequences of the considered incident,
  - how the responsible experts can acquire the related knowledge and skills and what are their constraints in terms of pre-requisite knowledge, time, job role, etc.
  - how the knowledge acquisition can be measured.
- selecting the respective content and delivery tools that address the defined objectives.

The development of the ECHO training programs for testing the Cyberskills Framework was carried out according to the good practices in the fields of instructional design and leveraged some of the most popular tools in the domain – simulation and modelling of specific environments and scenarios for cyber range exercises, tabletop exercises, and collaborative testing incident response procedures.

In general, the presented aggregation of the processes follows the plan-do-check-act cycle:

Plan – this phase includes the activities: i) Identify scenarios in terms of industry, assets (IT/OT + experts), vulnerabilities-threats- impacts (risks). ii) Create a toolset for each industry.

Do – this phase includes the activities: i) Build respective training program selecting the tools and content, ii) Verify the selected tools and content with the domain experts and service providers

Check - this phase includes the activities: i) Implement the training program with the target groups, ii) Evaluate the effect.

Act – Improve the training program and enrich the toolset by leveraging the lessons learned and repeating the above steps.

In conclusion, the ECHO consortium proposes a practical (the most severe risks for the operations in an organisation/ industry and dealing with them with the available expertize), structured (the training needs of the different teams for avoiding or mitigating those risks) and modular (the instruments that can be leveraged to provide the respective targeted knowledge and skills) approach for the design and delivery of a training service that meets the market demand.

Conclusions

For an organization whose operations and business continuity are dependent on the cybersecurity, there is a well-staffed Security Operations Centre (SOC) with very specific expert tasks assigned. Still, for the smaller organizations, in most of the cases, the security policy and strategy assumes an ad hoc assembled incident response capacity with the existing (ICT) staff members who are expected to cover a broad range of incident response and forensics-related skills. Providing all size and type of organizations with practical tools for assessment of their training needs and expert participation in the design and development of the services that meet those needs is essential for building a capacity for effective cyber-defence.

The ECHO consortium considered the ontology and semantic technologies as tools for building a common understanding of the competences needed for development and adaptation of professionals to the security strategies and procedures in the private and public sector. The E-CSF Ontology improves the visualizations of relationships between the cyber-risk and learning concepts. The visual tools enhance the analysis and mapping, while furthermore, it currently serves as a database for educators where all the relevant information is kept and can be constantly updated. The development of the ontology as AI-supporting mechanism for finding hidden dependencies, correlations and causal links is critical factor for more targeted trainings in detection and response actions for front-line defenders.

Within the ECHO project, the task group started a research on using semantic technologies for identification of training needs in the three ECHO industries. The results and visualizations are achieved through queries using the SPARQL querying language. Currently, in this work the tool Protégé was leveraged[1]. However, as a future goal can be considered the enrichment and query-based

[1] An open-source tool for knowledge management developed and maintained by Stanford University, https://protege.stanford.edu/

further development of the E-CSF Ontology. This will allow the further exploration of the usability and quality of collected and analyzed information and data.

The work on a GUI will allow users to interact easier with the ontology and make queries without being specialists in query languages and syntax. Achieving of those goals will empower organizations from industry, academia, and government to include more people in the design and delivery of their cyber-defence courses, by providing them with a tool to identify the people, suitable for these tasks and the gaps in their skills, knowledge.

Acknowledgements

This work is funded by the ECHO project, financed by the European Union's Horizon 2020 research and innovation programme under grant agreement no. 830943. The author gratefully acknowledges the work and support of the instructional designers Christina Todorova (ESI CEE) and George Petrisor (SIMAVI), the evaluation experts Mascia Toussaint and Veronica Rosa (ENQUIRIA), Sten Mäses (Tallinn University of Technology), the content creators Ioannis Chalkias, Cagatay Yucel and Vasilis Katos (Bournemouth University), Georgios Iosifidis (RHEA), Marco Dri (FIN), Marco Pappalardo and Gian Paolo Donnarumma (CIRM), Marco Quartullo and Andrea Guarino (ACEA).

References

[1] European Cyber Security Organisation (ECSO), *Gaps in European Cyber Education and Professional Training,* March, 2018, https://www.ecs-org.eu/documents/publications/5ad725df6d33d.pdf.

[2] George Hatzivasilis, Sotiris Ioannidis, Michail Smyrlis, George Spanoudakis, Fulvio Frati, Ludger Goeke, Torsten Hildebrandt, George Tsakirakis, Fotis Oikonomou, George Leftheriotis, and Hristo Koshutanski, "Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees," *Applied Sciences Journal* 10, no. 16 (August, 2020): 5702, DOI: 10.3390/app10165702.

[3] National Initiative for Cybersecurity Education, accessed June 12, 2022, https://www.nist.gov/itl/applied-cybersecurity/nice.

[4] "D9.1. Cybersecurity skills framework," Strategic programs for advanced research and technology in Europe (SPARTA), January 2020, https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf.

[5] "D6.3. Design of Education and Professional Framework," Cyber Security for Europe, 2021, https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf.

[6] "The e-CF Explorer," IT Professionalism, 2022, https://ecfexplorer.itprofessionalism.org/.

[7] Infocomm Media Cyber Security, accessed June, 2022, https://www.imda.gov.sg/regulations-and-licensing-listing/infocomm-media-cyber-security.

[8] ESCO - European Skills, Competences, Qualifications and Occupations, accessed June, 2022, https://esco.ec.europa.eu/en.

[9] "Technical Guideline on Threats and Assets," ENISA, 2022, https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets.

[10] Joint Research Centre Cybersecurity Taxonomy, accessed June, 2022, https://data.jrc.ec.europa.eu/dataset/d2f56334-a0df-485b-8dc8-2c0039d31122.

[11] Jerry Dale Jones, Catherine Elise, Barret, "Simulation as a classroom teaching method," *i-manager's Journal on School Educational Technology* 12, no. 4, (March - May 2017).

About the Author

Pavel Varbanov is a project coordinator and researcher at the European Software Institute - Center Eastern Europe and at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences. The main focus of his work revolves around the design, development, and management of projects in the field of training and education, digital innovation, and cybersecurity. His scientific interests are in innovative educational methods, competence frameworks and taxonomies, and solutions for overcoming the digital divide. His most recent research activity is directed towards the adaptation of cyber-defence training content to the specific needs of the industry and professionals from other domains, cybersecurity certification, and security of new technologies. https://orcid.org/0000-0002-1868-8638