“Investigating, Developing And Providing Awareness About Innovative Lesson Syllabus Implemented in Cyber Security Technologies in Information Technologies”

A1:Review and Analyze Existing European Practice for Cyber Security Education

Deliverable A1.4 Turkey Road Map

COOPERATION FOR INNOVATION AND THE EXCHANGE OF GOOD PRACTICES
Strategic Partnerships for Vocational Education and Training
Project Number:2016-1-TR01-KA202-034434
This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. Introduction and Preliminaries

It is a fact that Ciber offers opportunities such as anonymity and denial for the information systems and information / data attacks. It is difficult to determine who has been financing and organizing the advanced cyber attacks which been targeting information systems and data. This situation and characteristics reveal the asymmetric character of the risk and threats in the cyber stratum, making the struggle with the threats difficult. In fact it is no longer mentioned that absolute safety of cyber security is provided, but instead it is aimed to keep the security risks of cyber security at manageable and acceptable levels. It is recognized that being in an open and connected environment such as the Internet will bring some risks with the increased accessibility. These risks should be managed with a holistic approach involving all stakeholders and be prepared for cyber events and based on the basis of continuity with minimal damage from these events.

Considering all the previous information and in accordance with the " Decision of the Council of Ministers on the Execution, Management and Coordination of National Cyber Security Work" published in the Official newspaper dated 20/10/2012, No. 28447, and The Electronic Communication Law numbered 5809, The task of preparing and coordinating policies, strategies and action plans for the provision of national cyber security has been given to the Ministry of Transport, Maritime Affairs and Communications.

Cyber Security has been on the agenda of all developed countries since 2008, in addition to the EU (European Union), OECD (Organization for Economic Co-operation and Development), NATO (North Atlantic Alliance), during the preparation of the National Cyber Security Strategy and Action Plan of 2016-2019, in addition to the work carried out with the stakeholders, a back-to-ground resource search was conducted and cyber security strategies of many countries from America, Europe and Far East were reviewed and the scope, targets and priorities , The organizational structure, resource budgeting, R & D (research and development) coordination, public-private sector cooperation, and training, solutions were evaluated. "2016-2019 National Cyber Safety Strategy" and "2016-2019 National Cyber Safety Action Plan" were prepared as a result of the collection, examination and evaluation of the information produced within the scope of all these studies. And within the 2016-2019 period, "Awareness and Human Resource Development" was among the strategic objectives that aimed to reduce the existing risks Within the scope of this strategic action; It is planned to carry out activities aimed at providing cyber security culture to all sections of the society, from corporate administrators to computer user citizens, and to educate cyber security experts. The Turkish Cypriot Safety Roadmap, which will be developed and presented as a report within the scope of our project, has been given importance to the raising of human resources and awareness activities in the field of cyber security. Work on creating sufficient human resources and adequate number of cyber security areas is an important issue in the long and short periods. Regulations need to be made for cyber security in secondary and high education, and activities should be organized in order to inform technology developers, system administrators and all concerned about cyber security awareness and their responsibilities. In addition, a training platform for all citizens should be established to support and promote cyber security awareness, and initiatives that serve these activities should be supported.

This road map prepared in Turkey is in line with the 2013-2014 and 2016-2019 National Cyber Safety Strategy and Action Plans of Turkey. The Roadmap will also provide us with short terms and long terms goals for cyber security education development in Turkey. The short term goals will represent the needs for creation of the basis in formal and informal cyber security education. It is very important to

raise awareness among common people about cyber security. Informal education of people will raise the level of security and will prevent many of security breach that are rather deception then technical breach. Also, education will help people to recognize the security breaches and contact specialized units to combat cybercrime, which will be composed of experts from different parts of cyber security area. Mostly, cybercrime is used for frauds and money laundering on the Internet. The Roadmap will give us insight in Long term period that might be long enough for Turkey to establish integral cyber security educational system at national level. The Roadmap will also provide Plans for each Work Package activities. In that way this document is not only intended to be an overview of what should be done but also will provide detail description of steps that should be done to the end of the project to achieve the defined goals.

2. Goals of the Roadmap

Goals of the Roadmap, to improve the knowledge and skills of the vocational education instutitions in the field of cyber security and raise awareness in this field and it provides a road map for Turkey by analyzing and evaluating the European cyber security systems and comparing them with Turkey.

Within the scope of our project the 3. Cross-matching of practice in Turkey with EU standards work titled A1: Review and analysis of existing European practice for cybersecurity education, As stated in the study, there is a lack of cyber security trainings at the level of high school and undergraduate level. Cyber Security trainings, which are not given at the high school level in particular, are given at very few of universities at the undergraduate level but without any link between them. This roadmap is aimed at developing a common educational curriculum and distance education platform at the target high school and undergraduate levels between Level 2 and Level 5.

2.1. Short term goals (2016-2018)

Raise awareness about cyber security in Turkey and partners Countries:

Society needs to acquire and educate the necessary consciousness against these information thieves and attackers. So, main target should be to educate all population about possible threats over Internet and make them familiar with basic rules about using online accounts, using safe email box, cloud accounts, social media accounts, safe surfing and using online services. This project is expected to raise awareness among the vocational education schools. In order for computer users to be aware of cyber security, it is necessary to do studies to increase awareness of cyber security (seminars, brochures, non-formal education activities, awareness through distance learning and media).

Disseminating cyber security educations in middle, high schools and University degree education and non-formal education:
Adding cyber security to the curriculum of computer programming departments in Vocational Schools. Integrating cyber security subjects into the course programs which are located in IT field.

Establish sustainable strategies for trainings of workforce in cyber security:
Due to the inadequacy of cyber security training, many informatics workers and other young people can not be concerned about the subject. The increase in cyber attacks and the lack of qualified staff in sufficient numbers, the focus group is trying to learn innovative techniques and technologies. On the

other side, ICT professionals should be able to use modern technologies in order to set security system and answer on different kinds of identified attacks.

Start with collaboration and cooperation at regional and international level:
Start with collaboration and cooperation at regional and international level.
Cooperation and collaboration should be established at both, institutional and national levels, aimed on exchanging experience and knowledge, and enhancing joint forces in cyber wars. It can be realised via establishing joint regional centres for cyber security and joint participation in different project funded by EU and other international sources.

2.2. Long term goals (2016-2020)

It is our long-term goal to prioritize practices such as joint cooperation, quality assurance, curriculum reform, and restructuring of vocational and technical education for employment purposes among educational institutions. The integration of cyber security lessons into the formal and informal education system, the establishment of the cyber security areas at least at the undergraduate level in universities, the preparation of the raised human power and the activities to raise awareness of cyber events on the society are among our long-term goals.

Summary;

- Implementation of sustainable training strategy to train workforces to appropriate level;
- Establishing cost effective sustainable plans for specialised trainings;
- Integrate training on Cybercrime in regular programs at private and public
- institutions/agencies;
- Create R&D environment in the field of cyber security. R&D activities are essential: In order to prepare own forces to face a challenge on dynamic and constantly evolving and growing cyber space. To this end, PhD studies should be established with simultaneous preparation at institutional and individual (already proven researchers with expressed willingness and readiness for R&D in cyber security filed) levels to lead those activities at national and/or regional level.

Plan for WP1 (Review and Analyze Existing European Practice for Cyber Security Education)

PLAN for WP-1

PLAN

Goal

Review and analyze existing European practice for Cyber security education

Manage by;

Zonguldak Mesleki ve Teknik Anadolu Lisesi, IAT

Key Measures

Existing EU practices for cyber security

Cross-matching of practice in Turkey with EU standards

Organization of courses, workshops, presentations

Dissemination/presentation of created documents and organized events.

Team	What, Who and When
IAT and with the participation of partners	• Short partner studies for Intellectual Output O5 about Cyber Security in their countries - **IAT- *All Partners - First 3 Months*** • Cross-matching of Turkey situation with EU standards - ***ZMTAL - 3rd and 4th Months*** • Organize discussion within team to: In-Service Training, Sertificate programme, cource organisations - ***ZMTAL, BEU - Between 18th and 24th Months*** • Creation of documents related to the achievement of study program quality - ***All Partners - After 4th Months*** • Organisation of the Poster Contest about Cyber Security Public awaraness - ***BUE, ZMTAL - 5th and 6th Months*** • Organization of courses, presentations for all levels of staff, in order to increase public awareness of cyber security risks – ***All Partners - Between 20th and 24th Months*** • Organization of specialized/advanced training for specific groups of workers, staff, lecturer, teacher - ***All Partners - After 20th Months*** • Draw conclusions about future work – ***All Partners - After 3rd Month***

PLAN for WP-2

PLAN

Goal
Raise awareness about Cyber Security
Manage by;
Zonguldak Mesleki ve Teknik Anadolu Lisesi
Key Measures
Analysis of Turkey and EU Cyber Securitypublic awareness
Raising awareness of PC users about Cyber Security (posters, banners, videos and competition)
Cyber Security Magazine and Leaflets
Conferances for Dissemination and Awareness about puclic
Dissemination/presentation of created documents and organized events

Team	**What, Who and When**
With the participation of partners	• Perform analysis of existing programs on risk of online activities in EU – ***All Partners – After 3rd Month*** • Short partner studies for Intellectual Output O5 about Cyber Security in their countries - **IAT- *All Partners - First 3 Months*** • Organize discussion within team to: In-Service Training, Sertificate programme, cource organisations - ***ZMTAL, BEU - Between 18th and 24th Months*** • Organisation of the Poster Contest about Cyber Security Public awaraness - ***BUE, ZMTAL - 5th and 6th Months*** • Organization of courses, presentations for all levels of staff, in order to increase public awareness of cyber security risks – ***All Partners - Between 20th and 24th Months*** • Organization of specialized/advanced training for specific groups of workers, staff, lecturer, teacher - ***All Partners - After 20th Months*** • Organization of Dissemination for Conferances ***– IAT,BUCKS and Turkey Partners – In Last 6 Months*** • Perform Project Leaflets and Magazine– ***BEU, EPRALIMA, UDANET - After Second Term of the Project***

PLAN for WP-3

PLAN

Goal	
Increase the Human Pool of Skilled and Knowledgeable Workers About Cyber Security	
Manage by;	
Zonguldak Mesleki ve Teknik Anadolu Lisesi	
Key Measures	
Analysis of cyber security educational programs	
Training Curriculum	
Analysis distance E-elarning method	
Regulation of the certification system	
Create curriculum for VET School and HE Level program for cyber security	
Team	**What, Who and When** • Perform analysis of existing knowledge of cybersecurity in public/private organizations – ***All Partners – First 3 Months*** • Cross-matching of ME situation with EU standards – ***ZMTAL – First 4 Months of Project*** • Organize discussion within team to: decide which dissemination and educational measures will be realized; suggest courses structure; organize collaboration in courses preparation – ***All Partners – After 3rd Months*** • Organize discussions for analysing created educational plans and course material – ***All Partners – After First Meeting*** • Create curriculum for VET and HE Level program for Cyber Security – ***All Partners – After First Meeting***