Roadmap for new Cyber security Education in ME

Table of content

1. Introduction and preliminaries

According to actual state recorded in Montenegro, regarding cyber security education Roadmap for new Cyber security Education in Montenegro is created. At a moment there is no formal education in cyber security in Montenegro that can educate students at graduated and post graduated level. One of the reason for this situation is that, at the moment, there are no adopted politics and strategies in cyber security education. Also the Government bodies have not created full and effective legal basis for dealing with cybercriminal. It is important to mention that cyber security is very sensitive area that is both technical and legal issue. Having in mind importance of education of technical staff in the area it very important to keep in mind the legal part of education. As a multidisciplinary and very complex area, that directly impact life of people, it is impossible to create expert that can cover all parts of cyber security. Mostly at the mentioning of cyber security people think about computer engineering and specialist, and thanks to popular media they imagine them as almighty hackers that poses greater knowledge about ICT. In practice, it is very important to know legal restriction about using computer software and network. All actions that exceed legal norms can be considered as a type of cybercriminal. As it is in real life, in cybercriminal there are different types of criminal acts. So first step in cyber security is to recognize criminal acts. This is the reason why there have to be experts in law in cyber space that can recognize criminal acts. Because of great differences between law and engineering it is expected to have separate experts for these parts of cyber security area. The aim of the Roadmap is, based on previous research, to show proper steps needed to be taken for proper education of needed profile of experts. The Roadmap will give us insight in profile of needed experts, firstly is it technical or law expert and in a second level it will show us what exact area of cyber security will be covered by education that is needed in Montenegro. The Roadmap will provide us with short terms and long terms goals of cyber security education development in Montenegro. Short terms goals will represent needs for creation of basis for formal and informal cyber security education. It is very important to raise awareness of common people about cyber security. Informal education of people will raise level of security and will prevent many of security breach that are rather deception then technical breach. Also that education will help people to recognize security breaches and to contact specialized units to combat cybercrime, which will be composed from expert of different parts of cyber security area. Mostly, cybercriminal is used for frauds and money laundering on the Internet. The Roadmap will give us insight in Long terms period that might be long enough for Montenegro to establish integral cyber security educational system at national level. The Roadmap will also provide Plan - Do – Check - Act (PDCA) for each plan activity. 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 a project to achieve defined goals.

2. Goals of the Roadmap

The fight against cybercrime includes different areas and therefore defined priorities and measures to be taken, such as follows:

1. Politics and strategies in cyber security
2. Full and effective legal basis for the operation of the criminal justice system
3. Specialized units to combat cyber crime
4. Financial investigations and preventing and combating fraud and money laundering on the Internet
5. Cooperation between law enforcement and internet service providers
6. Effective regional and international cooperation

All these areas and activities have one common requirement and pre-condition: trained and educated staff capable to respond on all challenges issued in modern cyber space. As already shown in DEV 1.3, Montenegro has lack of integral cyber educational system and thus, the Roadmap is aimed on defining strategic priorities in educational system at national level in the fight against cybercrime.

Following sub-sections define strategic priorities needed to be achieved in order to develop effective educational system aimed on strengthening national capacities of the whole nation, as well as highly specialised workforce in both, public and private sectors.

2.1 Short term goals (2014-2016)

For short term period (which is for this Roadmap limited on two years, 2014-2016), the following priorities are defined:

- **Raise awareness about cyber security over Montenegrin population in general.** Target should be to educate all population about possible threats over Internet and make them familiar with basic rules about using online accounts, safe surfing and using online services.
- **Establish sustainable strategies for trainings of workforce in specific fields and areas of action, such as: law enforcement, training judiciary, ICT sectors, etc.** Target should be to ensure that law enforcement agencies have the skills and competencies necessary to investigate cybercrime, provide electronic evidence, conduct computer forensic analysis in criminal proceedings, to help others bodies and contribute to network security. 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.
- **Create core elements of formal educational system in cyber security (graduate and post-graduate studies).** In order to ensure sustainable education in cyber security, educational system should be established, including both, formal and informal education. In accordance with the above priorities, its core elements should include literacy of cyber security at lowest levels in educational system and specialised HE such as post-graduate and master studies. All other elements of educational system may be established later in full coherence with those core elements.

- **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 (such as regional CERT, regional joint studies in cyber security, etc.) and/or joint participation in different project funded by EU and other international sources.

2.2 Long term goals (2014-2020)

Long terms period (which is for this Roadmap planned on six years, 2014-2020), might be long enough for Montenegro to establish integral cyber security educational system at national level, and thus the following priorities are defined:

- **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.

General idea of this TEMPUS project is to provide core elements essential for achievement of defined short term goals with sustainable plans focused on long term goals and their realisation.

3. Plan - Do – Check - Act (PDCA)

3.1 PDCA for WP2 (Raise awareness about the risk of online activities)

<table>
<tr><th colspan="3">WP2
Plan – Do – Check – Act (PDCA)</th></tr>
<tr><td rowspan="2"><b>PLAN</b></td><td colspan="2"><b>Goal:</b>
Raise awareness about the risk of online activities
<b>Task is managed by:</b>
Buckinghamshire New University (BUCKS)</td></tr>
<tr><td><b>Key Measures:</b>
• Cross-matching of current EU standards with all levels of current awareness on risk of online activities.
• Creation of documents for Content, contact and conduct- a framework for digital skills
• Dissemination/presentation of created documents and organized events</td><td><b><u>What-Who-When:</u></b>
1. Perform analysis of existing programs on risk of online activities in EU and world – As soon as possible
2. Cross-matching of current EU standards with all levels of activities on risk of online activities – EU partners – soon and when needed
3. Organize open discussion with academic, government and non-governmental organizations about current risk of online activities –
4. Arrange virtual discussion within team to: suggest risk of online activities and proposal for minimise risk ;
5. Creation of documents related to the risk of online activities – All team – soon
6. Organization of workshops, virtual seminars and promotions for citizens and all levels of academic staff, in order to increase public awareness of</td></tr>
</table>

	Team: Representative of Buckinghamshire New University, educational and governmental institutions from Montenegro, with the participation of academic EU partners.	risks on online activities– All team – soon

DO	• Analysis and discussion of the existing standards on online activities in EU – • Identify the key factors on risk of online activities ◦ Identify online courses and distance educational systems ◦ Identify risk on all other online activities • Organization of informational workshops, virtual presentations and improving citizens' knowledge about online risk and inform population about future/ongoing awareness campaign • Development of problem solving strategies, planning, reflecting the online activity risk. **Preparing documents:** • Prepare initial versions of educational material documents. **Working:** • Interactive working in teams, using shared repository (Dropbox)	**Created documents:** • Here should be listed created documents

CHECK	• Report and conclusions about existing knowledge of risk of online activities in EU organizations • Developing tailored strategies to solve potential problematic situations online • Analysing documents/reports: • Organize virtual workshops	**Conclusions:** • Draw conclusions about effectiveness and impact of created documents and presentations.

ACT	**Check if created documents/reports are sufficiently satisfying with respect to the goals set**	
	Yes – Adopt & Adapt • Identify possible improvements • Prepare improved versions of documents and presentations • Prepare printed versions of documents	**No – Abandon & Predict New Change** • Determine most relevant strategies • Determine what material is completely unsatisfying • Prepare printed or virtual version of documents

3.2 PDCA for WP3 (Develop and maintain an unrivalled, globally competitive cyber security workforce)

<table>
<tr><th colspan="3">WP3
Plan – Do – Check – Act (PDCA)</th></tr>
<tr><td rowspan="2"><b>PLAN</b></td><td colspan="2"><b>Goal:</b>
Develop and maintain an unrivalled, globally competitive cyber security workforce
<b>Task is managed by:</b>
University of Roma Tre (UR3)</td></tr>
<tr><td><b>Key Measures:</b>
• Cross-matching of public/private organizations with EU standards
• Creation of processes and documents for standardization/improvement/enrichment of study programs and instructions for their implementation
• Organization of courses, workshops, presentations and promotions for citizens and all levels of staff
• Dissemination/presentation of created documents and organized events</td><td><b><u>What-Who-When:</u></b>
7. Perform analysis of existing knowledge of cybersecurity in public/private organizations – ME partners – As soon as possible
8. Cross-matching of ME situation with EU standards – EU partners – As soon as 1. is done
9. Organize open discussion with governmental and non-governmental organizations about current and future cybersecurity risks and vulnerabilities – As soon as 2. is done
10. Organize discussion within team to: decide which dissemination and educational measures will be realized; suggest courses structure; organize collaboration in courses preparation – All team – As soon as 3. is done
11. Creation of documents related to the achievement of study programs quality – All team – As soon as 4. is done</td></tr>
</table>

	Team: Representative of educational and governmental institutions from Montenegro, with the participation of academic EU partners.	12. Organization of courses, extensive workshops, presentations and promotions for citizens and all levels of staff, in order to increase public awareness of cyber security risks – All team – As soon as 5. is done 13. Organization of specialized/advanced training for specific groups of workers, related to their range of responsibilities and jurisdictions – All team – As soon as 5. is done 14. Organize discussions for analysing created educational plans and course material. Panels' conclusions should be used as measure quality – All team – As soon as 6. and 7. are done 15. Draw conclusions about future work – All team – As soon as 8. is done

DO	• Analysis and discussion of the existing level of cyber security awareness in ME – common citizens and public/private organizations staff • Proposal of a roadmap for the implementation and management of Cyber security Education in ME ◦ Identify course and dissemination material that should be prepared ◦ Development of a draft framework implementing cyber security methodology • Organization of informational open days, on-line presentations and internet marketing for improving citizens' knowledge about online risk and inform population about future/ongoing awareness campaign • Publishing of (previously created – see WP1) Handbook defining roles, procedures, methodologies and evaluation of cyber security resources for citizens • Development of a usable cyber security competency framework (Human Resources & Curriculum focus)	**Created documents:** • Here should be listed created documents

	Preparing documents: • Prepare initial versions of educational material documents. **Working:** • Interactive working in teams, using shared repository (Dropbox)	

CHECK	• Report about organized informational open days, on-line presentations and internet marketing activities: ◦ Number of participants ◦ Number of hard copies of Handbook supplied to all interested parts ◦ Feedback from participants • Report and conclusions about existing knowledge of cyber security within ME organizations • Report about organized specialized trainings: ◦ Number of participants ◦ Number of public and private institutions which representatives participated at organized trainings ◦ Feedback from participants (possibly through final examinations) **Analysing documents/reports:** • Organize workshop in Rome for analysing documents and reports • Organize presentation of project and created documents to professors and	**Conclusions:** • Draw conclusions about effectiveness and impact of created documents/courses and course material.

	assistants at ME partners	

	Check if created documents/reports are sufficiently satisfying with respect to the goals set	
ACT	**Yes – Adopt & Adapt** • Identify possible improvements • Prepare improved versions of documents and course/dissemination material and plans • Prepare printed versions of documents • Present material and documents to national authorities	**No – Abandon & Predict New Change** • Determine most relevant problems • Determine what material is completely unsatisfying • Identify responsibilities to adjust new team organizations • Define who will make changes • Start new PDCA cycle

3.3 PDCA for WP4 (Broaden the pool of skilled workers capable of supporting a cyber-secure nation)

<table>
<tr><th colspan="3">WP4
Plan – Do – Check – Act (PDCA)</th></tr>
<tr><td rowspan="3"><b>PLAN</b></td><td colspan="2"><b>Goal:</b>
Create multidisciplinary curriculum for master study program for cyber security
<b>Task is managed by:</b>
Tallinn University of Technology</td></tr>
<tr><td><b>Key Measures:</b>
• Accredited multidisciplinary master program in specific areas of cyber security.</td><td rowspan="2"><b>Key Measures:</b>
• Accredited multidisciplinary master program in specific areas of cyber security.
<b>Team:</b>
Working team consisted of representative of the universities of Montenegro, EU partners and other interested partners.</td></tr>
<tr><td><b>Team:</b>
Working team consisted of representative of the universities of Montenegro, EU partners and other interested partners.</td></tr>
</table>

DO	• Carry out the actions in the plan **Preparing documents:** • Prepare initial versions of documents, review and publish the final version **Working:** • Interactive working in teams, using shared repository (Dropbox)	16. Carry out the actions in the plan **Preparing documents:** 17. Prepare initial versions of documents, review and publish the final version **Working:** 18. Interactive working in teams, using shared repository (Dropbox)

CHECK	**Analysing documents:** **When - Where** • Creation and quality of the documents • Meetings and workshops to discuss the results	**Analysing documents:** **When - Where** • Creation and quality of the documents • Meetings and workshops to discuss the results

	Check if created documents correspond to the goals set	
ACT	**Yes – Adopt & Adapt** • Identify possible improvements • Prepare improved versions of documents and course/dissemination material and plans • Prepare printed versions of documents • Present material and documents to national authorities	**Yes – Adopt & Adapt** • Identify possible improvements • Prepare improved versions of documents and course/dissemination material and plans • Prepare printed versions of documents • Present material and documents to national authorities