CYBER SECURITY EDUCATION IN MONTENEGRO: CURRENT TRENDS, CHALLENGES AND OPEN PERSPECTIVES

Ramo Šendelj, Ivana Ognjanović
University of Donja Gorica, Montenegro

Abstract

Cyber-security threats evolve as rapidly as the Internet expands, and staying protected against cyber-security threats requires all users, ranging from children and their parents to the most sophisticated users, their risk awareness and improvement of security practices on an ongoing basis. However, cyber educational system with all educational levels, including elementary education, higher education, universities and lifelong education, present core carriers for education and encouragement of cyber-security competence across the nation.

Recently, Montenegro (ME) has recognized the importance of modern cyber security society development, by taking the following steps: (i) Government has adopted strategic documents in 2012 (Strategy for development of Information Society in ME 2012-2016), with goals and tasks of establishing quality level of cyber security; (ii) National ME Computer Emergency Readiness Team (CERT) is established in 2012, and (iii) CERT already took actions of assistance to government agencies for both, reducing the risks of computer security incidents and responding to such incidents when they occur. Finally, the issues of cyber-security vulnerabilities, national security, public safety, and critical infrastructure were discussed on Explanatory session between EU and ME (2012) during the Screening chapter 10 – "Information society". In this report, EU highlighted the necessity of initiating activities focused on cyber-security awareness, education, trainings, and professional development, all coordinated and systematically organized at national level. Motivated by recent trends in cyber security education and as well as growing challenges of fighting against cyber treats and attacks at global level, ME universities in cooperation with relevant ministries and other institutions at national level, initiated national project titled 'Enhancement of cyber educational system of ME', which is accepted for funding by last TEMPUS call (544088-1-2013-1-SI-TEMPUS-JPHES). The project is aimed on enhancing the overall ME cyber-security educational system and accelerating the availability of educational and training resources designed to improve the overall cyber security society in ME. Project specific objectives are: (i) increase public awareness of cyber-security risks, responsible use of the Internet, and cyber-security as a career path; (ii) raise the competency and capability of information security professionals and practitioners through education, training, employment, and certification; and (iii) develop the next generation of cyber-security workers by establishing Master study in Cyber security.

In this paper we present results of comprehensive analyses of current level of cyber educational system of ME with measuring indicators (e.g. organizational capacities, number of cyber security and general ICT courses, number of departments and study programs addressing some of cyber security issues, number of organized trainings and workshops, etc.) on which bases, innovative model with short-term and long-term goals are defined with respect to specificity of ME society (may be seen in small population, differences in regional development and prosperity, etc.). Implementation of proposed model represent challenging issues for ME society in order to achieve advanced national prosperity and security in the 21st century through innovative cyber-security education, and thus, specific indicators are proposed for measuring progress level.

Keywords: Cyber security, educational system, Montenegro, EU standards

1 INTRODUCTION

The Internet allows users to gather, store, process, and transfer vast amounts of data, including proprietary and sensitive business, transactional, and personal data. Cyber-security threats evolve as rapidly as the Internet expands, and the associated risks are becoming increasingly global. Staying protected against cyber-security threats requires all users, ranging from children and their parents to the most sophisticated users, to be aware of the risks and improve their security practices on an ongoing basis. In order to motivate all parties involved in Internet traffic and economy, technical and public policy measures requires carefully balancing to heighten cyber-security without creating barriers

to innovation, by using widely used ICTs for development, implementation and management of safety instruments.

Over the last forty years, and especially since the year 2000, governments and businesses have embraced the internet, and ICT's potential to generate income and employment, provide access to business and information, enable e-learning, and facilitate government activities. The potentials of ICTs for supporting of highly secured usage of themselves are highlighted by the *Digital Agenda for Europe*[1] (DAE), adopted in May 2010. The DAE emphasizes the need for all stakeholders to join their forces in a holistic effort to ensure the security and resilience of ICT infrastructures, by focusing on: (i) prevention, preparedness and risk awareness; and (ii) development of effective and coordinated mechanisms for responding to new and increasingly sophisticated forms of cyber-attacks and cyber-crime.

To this end, the European Network and Information Security Agency (ENISA) is established in March 2004, by Regulation No 460/2004 of the European Parliament (EP) and of the Council. ENISA with the EU-institutions and the Member States seeks to develop a culture of network and information security for the benefit of citizens, consumers, business and public sector organizations in the EU [1]. Strategy for a Secure Information Society in Europe, established by the Council in March 2007, defines that network, information security knowledge and skills must also become integral part of everyday life of each individual and stakeholder in the society. Thereby, the EP invited member states to give support to training programs and raise general awareness of network and information security issues [11].

More recently, the European Commission established 'Cyber security Strategy of the EU: An Open, Safe and Secure Cyberspace' [10] in 2013, which outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment more safety. The EU vision presented in this strategy is articulated in five strategic priorities, such as: (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy; (iv) develop the industrial and technological resources for cyber security; and (v) establish a coherent international cyberspace policy for the EU and promote core EU values.

It is particularly emphasized that a high level of security can only be ensured if all in the value (e.g. equipment manufacturers, software developers, information society services providers) make security a priority. By fostering R&D investments and innovation it should be filled the technology gaps in ICT security, prepared for the next generation of security challenges [6], taking into account the constant evolution of user needs and reap the benefits of dual use technologies.

Montenegro has also recognized the importance of modern cyber security society development. During 2012, the Government has adopted Strategy for development of Information Society in Montenegro 2012-2016 which clearly define the goals and tasks of establishing quality level of cyber security [12]. Also, the National Montenegrin Computer Emergency Readiness Team (CERT) is established in 2012, with mission to coordinate and assist government agencies in implementing proactive services for reducing risks of computer security incidents as well as responding to such incidents when they occur. Since 2012, Montenegrin CERT is a member of ENISA, and since January 2013 a member of the Forum for Incident Response and Security Team (FIRST), an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

The issues of cyber-security vulnerabilities, national security, public safety, economic prosperity and critical infrastructure were discussed on Explanatory session between EU and Montenegro (December 2012) during the Screening chapter 10 – "Information society". EU has highlighted for Montenegro to begin with coordinated national initiative focused on cyber-security awareness, education, trainings, and professional development. The Government and higher education (HE) institutions must encourage cyber-security competence across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats.

TEMPUS project 'Enhancement of cyber educational system of ME' (544088-1-2013-1-SI-TEMPUS-JPHES is aimed on enhancing the overall cyber-security posture of the Montenegro and accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population. The project will help to secure Montenegrin digital

[1] http://ec.europa.eu/digital-agenda/

nation capable of advancing national economic prosperity and security in the 21st century through innovative cyber-security education (with different levels, ranging from promotions, specialized trainings to master studies), and awareness on a grand scale. Special focus within this project is put on developing comprehensive educational system in cyber security by taking into account characteristics of existing national educational system, as well as current trends and best practice at EU and global levels.

2 CYBER SECURITY EDUCATION

Academic institutions are taking different approaches to cyber security education. Some believe in specializing early and focus more on the application of cyber security, making it a part of mainstream undergraduate education. Others aren't advocates of specialized undergraduate degrees and think it is more important to have a strong grounding in the fundamentals of computer science first [7]. Existing cyber security educational programs, has some kind of limitations in focus and lack unity of efforts. In order to effectively ensure continued technical advantage and future cyber security challenges, education in cyber security should be developed over a technologically-skilled and cyber workforce and effective skills of the future experts.

Current cyber security education can be divided into formal and informal approaches and other trainings. Formal approach could be conducted through the elementary education, high school education and university education (Bachelor, Master, PhD, etc.). Cyber security Bachelor programs are at the university level of studying, mostly within the discipline of Computer Security or Computing, with honour for cyber security. This study programs includes broad scale from courses in fundamental computer science principles to more specialized courses covering all aspects of information systems security. Programs on Master degrees include all aspects of defence of possible attacks that can be conduct through the network or directly to computer [2]. Basically, these programs provide studying through the courses in the following areas: intrusion analysis and response, critical infrastructure and control system security, electronic evidence and presentations, information assurance and security, principles of communications networks, cyber security risks, secure software design, malware, cryptography, legal aspects of cyber security, etc. Some of the important characteristics of the formal educational Bachelor and Master programs in cyber security are [13]:

- Interdisciplinary programs that cuts across different, but related fields – especially computer science, engineering and management;
- Curriculum addresses both technical and theoretical issues in cyber security;
- Both undergraduate and graduate degree programs are offered;
- Faculty composed of leading practitioners and researchers in the field of cyber security and information assurance;
- Hands-on learning environment where students and faculty work together on projects that address real life cyber security threats;
- Emphasis on learning outcomes as well as career and professional advancement;
- Courses on management, information security policy and other related topics essential to the effective governance of secure information systems;
- Graduates of programs are placed in private and public sector positions.

The analysis focuses on cyber security education practice worldwide. The most developed programs are in the USA, where many Bachelor and Master Programs exist. Programs are drafted with special attention to different cyber security areas [3]. On the other hand, some countries still don't have formal education at the university level for the cyber security, even if they are aware of the importance of developing educational capacities for cyber security.

It is obvious that any academic program cannot on its own address the full range of trends, challenges, issues and differing perspectives. This is the aim of the leading cyber security education and practice to promote a collaborative approach and a long-term focus.

Bachelor study programs in cyber security usually last for three or four years, whereas the first three years focus on core studying and the fourth year is for specialization in specific areas. Master study programs in cyber security last for one year, ending with the Master thesis.

Enrolment conditions for Master Studies request an appropriate previous education within the IT area and sometimes there are prerequisites such as specific courses that should be passed before enrolment.

Approaches to formal education opportunities for students are critical to help building and shaping future cyber security capacities. This applies to students at all levels including colleges, undergraduate, graduate, and post-graduate students. The aim is to make such educational opportunities available to every student.

Another, important approach to cyber security education is through the cyber competitions or participation in projects. Cyber competitions are interactive, scenario-based that help participants develop cyber security skills and increase interest in cyber security careers [4]. Cyber competitions foster talent in potential cyber security professionals who might otherwise be unidentifiable through traditional academic means, and encourage mentor-led environment where participants can practice and hone their cyber security skills in a controlled, real-world environment.

Cyber security projects for university level students consist from a set of activities and programs tailored to prepare scientists and engineers to extend their focus beyond the laboratory. While the knowledge gained from project based research frequently advances a particular field of science. Such results may be translated into technologies with near-term benefits for the economy and society. Combining experience and guidance from established entrepreneurs with a targeted curriculum, the project could be a public-private partnership program that teaches grantees to identify valuable product opportunities that can emerge from academic research, and offers entrepreneurship training to student participants.

Business and government could encourage and improve cyber expertise by funding scholarships to help students afford graduate-level courses in cyber security.

One more widely popular approach is Open-online-courses (OOC) aimed at large-scale interactive participation and open access over the Internet. Anyone with an Internet connection could access OOCs teaching mathematics, computer science, technology, history and many other fields from top universities [5]. OOCs are another resource that internet users can utilize to begin their career in cyber security. To become a cyber security professional, basic math, engineering and computer science skills need to be acquired.

Recommendations for the general approaches and principles to cyber security education are [9]: (1) Cyber security should evolve into a formal discipline in the curriculum similar to other existing disciplines; (2) Programs must teach a combination of theory and practice, and to have a holistic approach; (3) Cyber security should be taught in an integrated fashion, with all students learning basic principles and respect principle of the interdisciplinary; (4) Government and industry collaboration is extremely important; (5) Collaborative approach and long-term focus.

3 ANALYSIS OF CYBER SECURITY LITERACY AND AWARENESS IN MONTENEGRO

In order to make comprehensive analyses of current level of cyber security education in Montenegro, we applied two different approaches: estimation of indicators measuring ICT literacy at national level and summarizing existing elements/parts of educational system in Montenegro aimed on multidisciplinary cyber security issues. Detailed analysis is given in [14], while in respect to space limitation of this paper, we briefly present major highlights.

3.1 ICT literacy in Montenegro

The Statistical Office of Montenegro conducted a survey on ICT usage in the period from 1 to 15 April 2014. The survey refers to the ICT usage in households, by individuals, and in enterprises. The ICT usage survey which was conducted in households, according to the EUROSTAT methodology, includes households with at least one member aged between 16 and 74 years old, and individuals of the same age. 1 200 households, with 1200 individuals, were interviewed face-to-face. The ICT usage survey which is conducted in enterprises covers 578 enterprises with 10 or more employees from 10 business sectors according to NACE Rev. 2; who were interviewed by telephone.

In Montenegro, there is a very small number of ICT professionals who are experts in the field of cyber security. The University of Montenegro does not provide an academic program in cyber security. The percentage of persons with no security software (antivirus, anti spam, firewall,…) installed and running in their computers is 25%.All these facts demonstrate that the cyber security awareness is not at an appropriate level in Montenegro.

Summarized data shows that (MONTSAT. 2014):

- Percentage of households that have access to computers is 53.7%.
- Percentage of households with Internet access at home is 63.6%.
- Percentage of households with TV set access (in house) is 99.2%.
- Percentage of households with mobile phone is 93.6%.

Furthermore, access to cyber space is characterized with the following data:

- Access to the Internet via a PC achieves 75.1% of households that have Internet access.
- Access to the Internet via a laptop achieves 57.6% of households that have Internet access.
- Access to the Internet via a mobile phone achieves 38.5% of households that have Internet access.

It is interesting to consider the reasons for having no access to the Internet, since 33.2% said that they have a lack of ICT literacy in using it (see Table 1).

Table 1. Reasons for having to access to the Internet [17]

Reasons	Percentage (%)		Reasons	Percentage (%)
I do not want to have Internet access	36,8		Physical disability	9,5
I have lack of ICT literacy	33,2		I access to Interent at some another place	7,5
Internet access is too expensive	29,9		Broadband connections are diabled	5,8
Equipment is too expensive	27,8		Other reasons	19,6

Furthermore, use of Internet by individuals is represented with Table 2 where data are divided over age categories of all citizens.

Table 2. Use of Internet by individuals – age categories

Age categories		**16-24**	**25-34**	**35-54**	**55-64**	**65-74**
Montenegro Population	459.892	77.846	90.288	169.077	75.419	47.262
Frequency of internet use	**Country**	**16-24**	**25-34**	**35-54**	**55-64**	**65-74**
Every day or almost every day	Montenegro	89.9%	85.7%	83.0%	72.3%	68.7%

The frequency of Internet use is of 79.92% (every day or almost every day) considering the average of all the age clusters from 16-74 years old. It means that it will be not a plus to introduce people in “how to use Internet” Internet because the majority of them already surf on web. This implies that there is a very good diffusion of the instrument they already know how to go on Internet but we still don’t know if they surf on it safely.

Furthermore, kinds of activities that users of Internet in last 3 months have used are presented on Figure 1, while Figure 2 gives more information regarding for which kind of activities users are aware and capable to use.

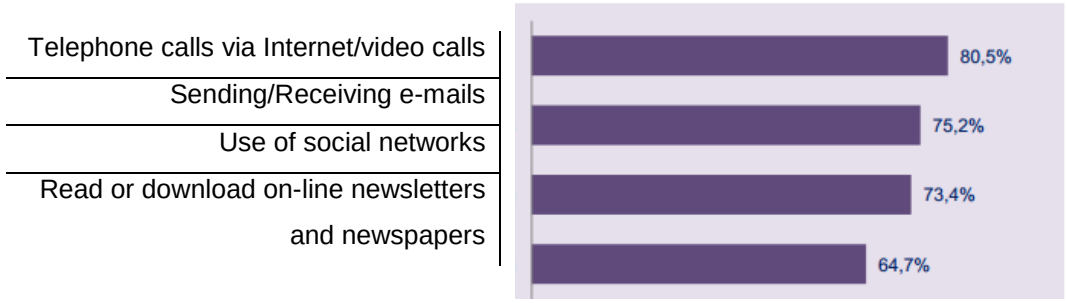

Figure 1. Kinds of activities that users performed via Internet in last 3 months (this question is with multiple choices)

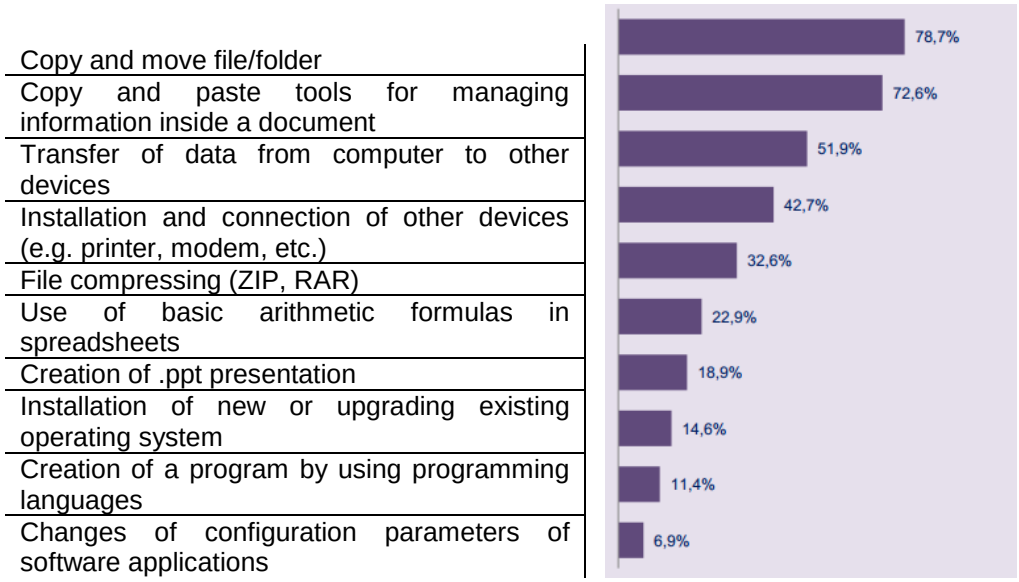

Figure 2. Kinds of activities that users are aware and capable to use.

Thus, in order to enhance overall cyber security awareness in Montenegro, the following approach is proposed to be used in [15]: the total target has already told before it will be of 519.109 people: **82%** circa of Montenegro population. The total target will be split in the specific paragraph on "target population".

- **Internet and computer skills:** the average level of Internet and computer skills is not very high. For that reason, the preparation of the communication materials should consider a language close to a basic level of knowledge in order to reach the maximum target available.
- **Activities on Internet:** The Consortium selected the main 23 activities on Internet presented by EUROSTAT in information society statistics. The activities have been matched with 4 main cyber security domain (topic) for basic users.

Thus, campaigns and different kinds of trainings are planned to be organized targeting the population, while lack of ICT knowledge and unavailability to Internet connections still remains to be addressed at national level.

The following section briefly described educational system in Montenegro from the aspect of multidisciplinary issues of cyber security.

3.2 Existing educational programs in cyber security in Montenegro

Detailed analysis of existing educational system in Montenegro is given in [15], while Table 3 summarizes results and gives overall analysis at all level of education, formal (from elementary to HEI with Master and Doctoral programs) and informal.

4 ROADMAP FOR CYBER SECURITY EDUCATION IN MONTENEGRO

According to the actual state of cyber security education in Montenegro the Roadmap for new Cyber security Education in Montenegro is being created. At the moment in Montenegro there is no formal education in cyber security that can educate students at graduate and post graduate level. One of the reasons for this situation is the lack of policies and strategies in cyber security education. Also the Government bodies did not create full and effective legal basis for dealing with cybercrime. It is important to mention that cyber security is a very sensitive area including both technical and legal issues. Having in mind the importance of technical education in cyber security, is very important not to underestimate the importance of the Law component of education. As a multidisciplinary and very complex area that directly impact life of people, it is impossible to create experts that can cover all parts of cyber security. When mention about cyber security, most people would think about computer engineering and imagine the people behind as hackers that possess great knowledge about ICT [16].

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.

4.1 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 among 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.

Table 3. Educational system in Montenegro in the field of cyber secuirty

Formal education in the field of cyber security	
Elementary and secondary education	Curricula at elementary and secondary levels of education contains one (two) mandatory ICT courses, while the field of cyber security is not included in their contents. Also, there is no elective course aimed on cyber security issues.
Bachelor study programs	In Montenegro, there is no Bachelor study program in cyber security. Although, EU practice and experience show that it is not necessary to include the whole study program at Bachelor level, in cases where existing study programs contain courses about multidisciplinary aspects on cyber security. However, only few courses exist at Montenegrin HEIs aimed on cyber security issues and they are included only for students at technical faculties, which thus cover only issues of technical cyber security of computing systems; and also at faculties of legal sciences aimed on legal aspects of cyber security.
Master study programs	Only one HEI, University of Donja Gorica has established Master study programs in cyber security, giving multidisciplinary approach for different groups of future experts in this area. They established the following Master study programs: - *Cyber security* master program at Humanistic studies - *Data protections and information systems security* – graduate and master study programs at Faculty of information systems and technologies
PhD study programs	There does not exist any PhD program in cyber security. EU practice and experience show that it is not necessary to include the whole study program at PhD level, in cases where existing study programs contain courses about multidisciplinary aspects on cyber security.
Informal education in the field of cyber security	
Professional development	There are a number of initiatives or general professional training at the institutional (usually organized by banks, telecommunication providers, etc.) and national level are organized for a wide range of ICT personnel. There is no information on whether some private companies engaged in the provision of professional training in this area, as well as how many are available and spread other side programs.
Training of employees	In Montenegro, the companies, especially small and medium enterprises do not organise training in the field of cyber protection for their employees. Lately, there is a growing trend of organizing these training by large companies (typically banks, ICT companies, telecom providers, etc.).
Education of general public in cyber education	
Raising awareness campaigns	An effective campaign to raise awareness of the general public do not exist. The Ministry for Information Society and Telecommunications plans to organize training for the general public, where special attention will be paid to children and young people, and the continuous introduction of new programs in the field of cyber security at all levels of education. But concrete actions are not recorded.
Informative cyber security campaigns	Effective campaigns for the general public do not exist except for elementary and secondary schools (organized by Ministry of Education in cooperation with Telenor Montenegro) where students are informed about the conscientious use of ICT and the Internet, in terms of security. It is necessary to organize initiatives between universities, private companies and schools.

4.2 Long term goals (2016-2020)

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.

5 CONLUSIONS

In developed Western countries (e.g. USA, Canada, UK, Australia), the most widely used type of education in cyber security is formal education which could be met at all levels of university education (i.e. Bachelor, Master and PhD studies). Very important fact of cyber security education is that it is linked with military and security institutions, especially in USA. Also, there are different sublevels of cyber security education within the levels of university education (Bachelor, Master and PhD studies), with different outcomes and from which emerges the approaches in choosing subjects for studying. At most universities that have cyber security programs, there are determined criteria for enrolment. Cyber security education is still at the early stage of development both in formal and informal education. There is still huge gap between practical needs and educational outcomes. In many countries cyber security is not recognized as a study program at the universities and education is mostly informal1.

The notices and recommendations are focusing on increasing and improving openness and collaboration, along with addressing both immediate priorities and longer-term strategies. Programs must strive to balance the near-term requirements of industry and government while educating future faculty members and researchers, developing more internships and fellowships, and continuing investments in research [7, 8]. These are the key initiatives of prime importance in the development of cyber security education.

1. Increase awareness and expertise – improve resources on work to raise the level of awareness across the academic community. Cyber security is no longer a hidden area embedded in computer science or engineering disciplines. Programs need to graduate more computer scientists and engineers with hands-on training and the ability to design and develop secure systems from the start.

2. Treat security education as a global issue cyber security issues are not relegated to a single country. They know no boundaries. Institutions need to share and collaborate with other programs around the world. Academics from more mature countries should increase their formal collaboration with those in emerging countries to help address the skills gap. Such initiatives could include distance learning programs and the sharing of curriculum and best practices among educators.

3. Approach security comprehensively, linking technical to non-technical fields –adopt a curriculum that has a holistic and interdisciplinary approach. Security education should cover infrastructure, people, data, applications, ethics, policy and legal issues. Business and public policy schools should focus on creating better security policy and governance and training future information security leaders, such as Chief Information Security Officers.

4. Seek innovative ways to fund labs and pursue real-world projects – Resources will always be tough to come by. Industry, government and academia must come up with novel ways to give students practical experience. More internships and design contests are one way to overcome this challenge. Other alter-natives include cloud-based or virtualized ranges, simulators and test beds.

5. Advance a “science of security” – more emphasis on the creation of a discipline of security science with fundamental concepts and a common vocabulary. This new science should focus on anticipating security problems, not just reacting to attacks. It must include scientific methodologies and incorporate reproducibility and proofs in the design of security systems.

We believe that these recommendations offer ways to make cybersecurity education more effective in the short and the long term. By breaking down barriers and working in concert, it is possible to better address current and emerging challenges.

Acknowledgements. Research presented in this paper is conducted within the TEMPUS project ‘Enhancement of Cyber Educational System in Montenegro (ECESM)’, project no. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

REFERENCES

[1] ENISA. (2014). Threats Landscape 2013. Brussels

[2] Baykal, N. (2013). Hands-on Cyber Defence Training Course for System / Network Administrators. Lecture Notes. Ankara, Turkey: Institute of Informatics

[3] European Union for Network and Information Security. (May 2012). Report on National Cyber Security Strategies: Setting the course for National Efforts to Strengthen Security in Cyberspace. Heraklion, Greece

[4] Goodman, S., Lin, H. (2007). Toward a Safer and More Secure Cyberspace. Washington DC: National Academies Press

[5] Miklaucic, M., Brewer, J. (Eds.) (2013). Convergence – Illicit Networks and National Security in the Age of Globalization. Washington DC:NDU Press

[6] Phahlamohlaka, J. (2008). Globalisation and National Security Issues for the State: Implications for National ICT policies. Social Dimensions Of Information And Communication Technology Policy. IFIP International Federation for Information Processing . Volume 282, 2008. pp 95-107

[7] Seymour, E. G., Herbert, S. L. (Eds). (2007).Toward a Safer and More Secure Cyberspace. Washington DC:NDU Press

[8] Stevens, T. (2012). A Cyber war of Ideas: Deterrence and Norms in Cyberspace, Contemporary Security Policy. Volume 33 (Issue 1)

[9] Svete, U. (2012). European E-readiness? Cyber dimension of national security policies. The Journal of comparative politics. ISBN 1338 1385, Vol 5 Number 1, January 2012

[10] European Commission. (2013). Cyber security Strategy of the European Union. Brussels, Belgium

[11] European Council (2008). Report on the Implementation of the European Security Strategy - Providing Security in a Changing World

[12] Government of Montenegro (2013). National Cyber Security Strategy of Montenegro

[13] ECESM Dev 1.2. (2014) EU practice for cyber security education, available online: http://ecesm.net/sites/default/files/Dev%201.2.-v1.4-FINAL.pdf

[14] ECESM Dev 1.3. (2014) Cross-matching of practice in ME with EU standards, available online: http://ecesm.net/sites/default/files/Dev%201.3-v4-FINAL.pdf

[15] ECESM Dev 2.1. (2015) Analysis of the ME cyber security public awareness, available online: http://ecesm.net/sites/default/files/Dev2.1%20-%20v1.pdf

[16] ECESM Dev 1.4. (2014) Roadmap for new Cyber security Education in ME, available online: http://ecesm.net/sites/default/files/Dev%201.4-v4-FINAL.pdf

[17] EC (2014) Assessment report for Montenegro 2014 Compliance Monitoring Round (for reference year 2013) - Version 1