EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

Gaps in European Cyber Education and Professional Training

WG5 I Education, training, awareness, cyber ranges

MARCH 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg5_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

New cyber and information security programmes are emerging at a very fast pace. This comes as no surprise to anyone who has even vaguely followed the news in recent years. Our society is fundamentally dependent on IT systems, everything is interconnected through the Internet, but vulnerabilities/hacks/breaches are occurring on a daily basis. There is clearly a lack of qualified cyber security professionals[1] and a need for a rise in the overall level of cyber awareness. The demand for cyber specialists and experts is greater than the supply and this is making society and organisations increasingly vulnerable. Governments, associated with different stakeholders, should tackle the cyber security skills gap through more education and training accredited offers.

This has become a very high priority for the European Commission, which is addressing this skills gap through several programmes, including: A New Skills Agenda for Europe: Working together to strengthen human capital, employability and competitiveness[2]. The Commission is also investing in research and innovation and industry is tackling cyber by focusing at investments based on the market needs. However, it is useless to invest in technology if we do not have the appropriate skills / experts to use it or if we don't know what technology solutions we lack. A security system operated by a person lacking required competences is not an asset, but a liability and ultimately a bad investment and just spending money on infrastructure can lead to a false feeling of security.

While investing money might not be the major obstacle anymore, today's real problems are: fast and dynamic pace of cyber security, availability of top qualified educators, and number of students interested in high-skilled jobs. It's also an issue for organisations to map and realise what are the resources, assets and competences they have and what is missing. Professional development at the workplace can partly address the skill gaps in the short run, but the long-term challenges are less likely to be solved. Secondly, highly qualified educators, trainers and coaches will be an issue for the coming years, as it is expected that they should have a formal degree, a pedagogical expertise and should be well trained on the substance (have up-to-date industry knowledge). For the academic educators, up-to-date industry knowledge is a challenge, whereas professional trainers often lack a formal degree and/or pedagogical background.

Not only education and training shall be addressed, but also the current and future carrier opportunities as the number of students could be improved for instance with more awareness on the availability and type of future jobs and by introducing cyber security topics no later than secondary school level (probably even before). This would ensure the overall rise of cyber awareness and resilience within the EU.

There is a huge growth potential in addressing the "gender issue", as women are underrepresented in cyber security professions. The cause of the disparity is mainly based on a false perception of science as a typically male field, and a lack of support for girls at all levels of education in the choice

[1] https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#485aecb55163

[2] https://ec.europa.eu/digital-single-market/en/news/digital-skills-core-new-skills-agenda-europe

of cyber security as a potential career path. In the near future, digital skills will be present in virtually every sector of the economy, thus, preventing digital exclusion of the female population is crucial not only from the social point of view, but also because of the need to support the sustainability of development of the world economy. As already mentioned, in the cyber domain, bridging the skills gap of qualified cyber security professionals by providing fully equal opportunities for women and men could contribute to the overall growth of European GDP of approximately 9 billion per year[3].

The current attitude to the overall skills shortage is to find a short-term "patch" to the problem. For example, universities have "added" a cyber security undergraduate or graduate degree to their curricula. This is often viewed as a "specialisation" or "add-on" to or just a re-branding of a Computer Science or Information Security degree. Unfortunately, many curriculum designers fail to realise the critical importance of the interdisciplinary nature of this area. Admittedly, cyber security needs professionals who are good at using keyboards. However, the challenges graduates will face in their jobs are much more complex. Cyber security requires a good understanding of law, human factors/psychology, mathematics/cryptography, social sciences, economics, security & risk management/IT audit, etc. Even within the technical domains, there is quite a difference in skills required for someone working in network/system monitoring, big data/machine learning, digital forensics for a law enforcement agency, malware reverse engineering for a security firm, and performing penetration tests, etc. Ideally, a graduate out of a cyber security programme should have a basic understanding of all those areas, plus an academic background.

This sums up the challenges curriculum designers need to face these days. It needs to be well understood that this area is fundamentally different from any of the existing curricula. Cyber security cannot be categorised as an academic discipline, but rather should be viewed as an emerging meta-discipline [1], and certainly is not an "add-on". This creates the main challenges, which are:

- Creating the foundations for a truly interdisciplinary understanding of the subject area.
- Universities need to ensure they do not lose academic values (such as critical thinking).
- Cyber security aspects shall be integrated in educational curricula (not just IT related).
- Professionals shall be able to certify their knowledge.

The second point is very important for universities, as there should be a distinct reason for attending a university. Universities should not be training for companies, but rather for society and for sustainability. At the same time, to ensure the employability of the graduates, universities need to address industry demands in their educational programmes. Certain specific cyber security skills (such as ethical hacking) can be obtained through professional training, without a formal degree, but professional training is usually focused on one specific skill and does not address the holistic nature of cyber security.

It is important to recognise that academic **education** and professional **training** address different learning needs, and to recognise opportunities for collaboration and knowledge transfer to bridge the skill gaps. Cyber education is a learning process focused on the synthesis of knowledge and skills, and applicability of these skills for solving complex issues. Training, on the other hand, tends to be targeted at the acquisition of a specific skill to a demonstrable level of competence. There is a strong case for engaging in both education and training as part of career development in cyber security.

[3] McKinsey, "Diversity Matters", February 2015

The last point is very important for the cyber security industry as currently job positions quite often traditionally require a Msc. degree both in education and industry. However, degrees and certifications are hard to compare (even if two professionals have the same certificate they might have a different level of competence) and experienced professionals might face the challenge of their experience not being recognised due to the lack of degree or certificate. Hence, many non-graduated professionals can be sought out to obtain a cyber security related degree, to benefit from the values of higher education institutions (HEI) while bridging the gap between academia and industry.

1.1 The Problem of the Higher Education Industry

Higher education institutions (HEI) need to ensure that their cyber security graduates a) have a holistic understanding of cyber security as a systemic issue and b) are ready to enter the work life (i.e. able to apply and use gained knowledge and skills). The fundamental problem, however, is to ensure the balance between the breadth and the depth of content. In order to ensure the employability of graduates, universities are more and more focusing on teaching detailed knowledge of the particular subject area. This creates a tension between skills for now (for the industry, e.g., managing a specific-vendor firewall) and skills for the longer term (e.g., how to secure the network and why this is important). The longer-term skills must include basic skills on technical details (e.g., firewall management), but need to have enough focus on systemic approaches to cyber security.

Current HEI curriculums face the issue of focusing on the IT and infosecurity aspects with some cyber security elements/modules. While infosecurity is about protecting the information itself and IT security is about protecting the IT system itself, cyber security is about securing EVERYTHING that is vulnerable through IT systems.

It is important that the following aspect is not forgotten in this argumentation: universities are supposed to be more than an accumulation of information. One of the cornerstones of academia has always been the transformation of thought, the ability to dissect scientific concepts and to think in abstract forms and structures. Those have been the values of higher education since Socrates or Plato, but they have changed in the light of large commercialisation[4]. This commercialisation is slowly leading to a decay of the quality of our graduates. Governments and universities want a return on their "investment" and charge higher fees to students. In return, students demand degrees that can ensure their employability, which means more hands-on orientation of the learning outcomes.

Another problem is related to the choice of education delivery tools and channels, while preserving the quality of education. We are now at a critical time; higher education is transforming, and this can either be a blessing or a curse. Digitalisation provides new opportunities for HEI to utilise cost-efficient technologies such as Massive Open Online Courses (MOOCs) and labs supporting education to our advantage, in addition to traditional classroom teaching methods. MOOCs and digital tools can (and probably should) replace large-scale lectures, as they are cheaper, operate at large

[4] https://popenici.com/2016/03/29/disrupteduniversities/

scale, and provide location-independent education. However, they do not adjust adequately to the learning individual, do not support team building, communication, and interpersonal skills. Those skills are vital in a globalised world and are difficult to obtain via MOOCs. So, the universities need to integrate all available teaching methods and tools to ensure we can raise the next generation of cyber security experts. “The question is whether current academic leaders have the vision, courage, and decisiveness to position their institutions to be academic leaders in the 21st century” [3].

HEIs are usually well equipped and have both technical and human resources. They are also excelling in various external funded projects (e.g. H2020) and are creating international cooperation. However, HEIs lack the true implementation of the results of such projects; their RDI facilities are doing project after project but are hardly utilising the results in their education curriculum, nor by monetising them. Also, current educational curriculums and training methodologies rarely provide proper access to real live data and networks to assess and learn from.

Finally, not only is there a shortage in the available teachers and lecturers, but many of the lecturers lack the industry experience or/and a long time has passed since they were involved in “on-field” projects. HEI can reproduce its lecturer capacity by offering lecturing positions to graduates, but those graduates most probably hardly got the experience to cope and understand real life cyber security threats and ways to manage them. As stated before, the cyber domain is changing fast, so the people involved in training/education should have current experiences from the real world.

1.2 The Problem of Professional Training Providers

Organisations offering professional trainings have a similar problem: Customers want to pay less for more value, but expenses are rising. The skills shortage makes it harder to retain inspiring teachers and the competition is fierce. Scalable solutions are needed to keep the cost at manageable levels. This is particularly important as such organisations are often fundamentally differently funded than academic institutions but are to some extent competing in the same marketplace.

For their customers, typically companies, “protections and preventions” and “detection and response” are the top priorities. Therefore, companies prefer to invest in systems rather than competences—the former seems to be an asset for the company even after employees leave. The return on investment on the cyber security spending is usually difficult to justify for the management and administration, even more the spending on the cyber security training. Far too often companies decide not to train their staff for fear they may leave once the training is over. Training can be quite expensive, depending on the type of certification, and there are indirect costs and associated disruptions of operations when members of staff attend the training courses.

Organisations often lack the clear understanding of the true level of their cyber resilience. Competing professional training providers often approach cyber security from a very different angle that results in confused stakeholders. Due to the huge offerings of different certificates and standards, organisations can hardly decide which approaches to follow and in what capabilities to invest.

Therefore, it can be more “convenient” for companies to hire graduates of higher education programmes and provide in-house training for them for further specialisation. Due to this practice, the holistic and interdisciplinary approaches are not considered on top of the pure technical and operational aspects, hence the critical thinking and the opportunities for further development are lacking.

Therefore, the community, academia and professional training providers are forced into a market niche, where providing trainings that address a specific skills gap (such as technical aspects of cyber security) is what counts, rather than approaching the problem at a holistic and interdisciplinary level.

2 Required Transformations in Cyber Security Education and Training

The key success factor in developing cyber security skills is to adapt education systems to address long-term challenges while responding to the current and future industry needs. Usually, when talking about cyber security skills gaps, we mean IT professionals. However, the skills gap is also visible among non-IT positions (such as lawyers, administrative personnel, healthcare professionals, service designers, and senior management, to name a few). Integrating cyber security courses into non-IT degrees is required. The education must cater to addressing the needs of a diverse groups of students, of different educational and work backgrounds, and of different age groups.

Current cyber (and IT/infosecurity) educational solutions address two main fields: technical and process validation. The two are hardly ever connected and tested on an organisational level (silo security solutions), yet they should be addressed and trained as they are: complementing and supporting each other. To achieve this, stakeholders should first understand the current cyber readiness of their organisation. For this, an innovative educational and exercising methodology is needed that supports the improvement of the organisational decision chain, which has a high impact on cyber resilience effectiveness and stakeholders getting familiar with their true cyber resilience capability.

Digitalisation enables required transformations of the educational system. There are unique opportunities for "flipped classroom"[5] and "Education 3.0"[6] teaching approaches to address the diversity of learners. For this, MOOCs can be an excellent enabler. Students can work at their own pace through areas where knowledge is missing, given the missing area is revealed. The quality of an online learning course (provided it is well planned and implemented) can sometimes be better than the quality of a classroom course. Finally, learning the facts or reading a book is not what needs to be done in a classroom using PowerPoint. Time can be much better spent in smaller study groups or seminar courses. In 1984, educational psychologist Benjamin Bloom described the 2-sigma problem [2], which essentially states that a student subject to 1-to-1 tuition will develop from an average student into one at the top 98% quantile of all students. So, replacing large lectures with MOOCs or other digital tools and focusing on creating a positive feedback loop and student mentoring should be a fundamental part of the teaching strategy.

Today, there is a wide choice of technology that allows us to optimise teaching, but it needs to engage the student. Technology can not only be used to reduce repetitive tasks but may also foster academic discourse. For example, blended learning [3] proposes a careful mix between asynchronous Internet technologies with face-to-face learning. It is important to appreciate the different cultural backgrounds and teach in a way that suites everyone, and this method also addresses Bloom's 2-sigma problem [2]. It's also good to integrate technology

[5] https://en.wikipedia.org/wiki/Flipped_classroom
[6] https://en.wikipedia.org/wiki/Education_3.0

in a meaningful way, but it is equally important to let inspiring teachers do what they can do best[7]. Engaging students from various cultures and gender is as equally important as encouraging quieter students to "speak-up". However, universities need to teach skills beyond "detailed knowledge". We are observing an ever-increasing gap between detailed knowledge and fundamental theory. Particularly in cybersecurity, graduates need to have a lot of technical knowledge but it's important to develop meta-cognitive processes that transform thought structures. This often goes beyond the communication of basic knowledge that is required by the curriculum. MOOCs and specific technical professional training courses can form some fundamental building blocks for a more comprehensive and interdisciplinary training approach. This interdisciplinary nature of cyber security, especially, requires novel teaching methods and strategies.

In addition to this, adaptive learning techniques can be used to assess students' capabilities and then adjust accordingly. Think of it in the following way: imagine the task given to the student is to configure a system to only allow ssh version 2[8] access to a server. Anyone with basic Linux skills will be able to do that in less than 30 seconds, while the task might take quite a long time for a student without the required background knowledge. Just measuring the time to solve such tasks could be a suitable metric to assess the skill-level and, dependent on the outcome, the system can then either adapt to go and cover more material from the Linux fundamental area or just skip the lesson completely and move to the next topic area. It is crucial to identify partners with skills in implementing and managing the cyber security platforms and systems, monitoring cyberspace events, and detecting threats and responding to anomalous situations and incidents.

Therefore, the community, academia and professional training providers are required to join forces and implement a working concept of bridging the gap between academia and industry and addressing cyber security on a conceptual level, by providing an educational and training framework that build on each other providing lifelong learning and specialisation opportunities (not just by e.g. providing specialised education on operating a certain vendor's product).

Overall, this area also has very strong synergies with ECSO's EHR4CYBER efforts to build a network among human resources experts to be able to identify and assess skills and talents in the sector. Simple metrics, a scalable way of assessing (or teaching) them, is the first step in each interview process aimed at identifying hidden talent.

2.1 The Value of Universities and Professional Trainings

So what is the value of academic education versus professional training? How do we bridge in the future the academic values and the industry technical and non-technical needs? The technical details are of critical importance to understand and solve real-world issues, but they change over time and do not form the basis of systemic thinking. Also, we shall realise that

[7] https://www.theatlantic.com/education/archive/2013/11/dont-give-up-on-the-lecture/281624/
[8] https://en.wikipedia.org/wiki/Secure_Shell#Version_2.x

cyber security is less of a technical issue than a human one and as such proper pedagogical approaches are required.

The value of university education lies in its holistic understanding of cyber security as a complex and multidisciplinary phenomenon, and in the ability to apply received knowledge and skills to solve real-life problems and development needs. Universities help develop critical thinking. However, it is also important to acknowledge differences in higher education. For traditional universities, it is important to engage students in scientific discourse whereas universities of applied sciences concentrate on real-life competences and close cooperation with the industry. In this respect, universities of applied sciences can be seen as a bridge between academic education and professional training.

The value of professional trainings is in their applied character in reaching a certain level of competence in performing a task. Professional certifications are often required by the industry for IT jobs, as they provide a certain level of accreditation of a skill. In addition, professional training is more flexible and can help security/IT professionals obtain needed skills fast (for example, GDPR training for DPO).

While there is a certain degree of overlapping between the two, it is important to realise that the value is based on fundamentally different approaches to learning. Instead of competing, education and training should form a common lifelong-learning approach to addressing cyber security skills development, which can only be achieved by creating common approaches to understanding cyber security and strong cooperation between academia and industry.

2.2 Solving the Dilemma of Cyber Security

The problem of cyber security, as illustrated above, starts with the widely recognised skills shortage and the interdisciplinarity of the field[9]. Teaching organisations need to “produce” lots of skilled people. Companies pay a lot of money for qualified experts, but many positions remain unfilled. Yet, even stakeholders at such organisations have a different understanding of addressing cyber due to the interdisciplinary nature of the field and the lack of cyber security knowledge of decision makers.

Besides this, it is also hard for universities to retain qualified teachers—as there is very little incentive to stay and teach at a university. This needs to develop towards being a shared responsibility, between higher education, professional training providers and companies.

MOOCs and adaptive learning platforms can provide a good foundation to develop cooperation between academia and industry and thus shorten the skills gap. Online courses are easily accessible and easy to scale up, and they provide fast and cost-efficient way to deliver the content. However, it is also important to remember that MOOCs and other online platforms cannot replace critical thinking and the value that one-to-one tutoring [2] brings. In addition, online platforms are the content-delivery tools, and in order to benefit from new technologies, education providers both in academia and professional training need to invest into developing a solid pedagogical framework and into producing high-quality content.

[9] https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

What can be done? The proposed solutions should have become obvious from the discussion above:

1. Invest research into teaching/knowledge transfer methods that scale in order to address the skills shortage problem. For example, ECSO SWG 5.1 "Cyber ranges and technical exercises" efforts guide towards improving skills through Cyber Security and Defence Exercises (CDX). There is a lot of potential for future research, in particular in the area of learning at such exercises [5]. Furthermore, ECSO SWG 5.3 "Awareness" is looking at raising the awareness levels through various "cyber hygiene"[10] initiatives.
2. We need to invest into novel teaching and knowledge transfer methods that sufficiently accounts for the interdisciplinary nature of a cyber security curriculum[11]. This includes a positive integration between MOOCs, CDXs and scalable professional trainings, with a more individual and academic approach. MOOCs, especially, are good at teaching the "simpler parts" of a field at highly scalable levels, where more "complex topics" require interactive discourse between teachers and students. This might require a fundamental shift in thinking on how we teach courses at HEIs as well as in cooperative settings or the context of professional trainings. This is one of the efforts in ECSO SWG 5.2 "Education & training".
3. We need to create cyber security education and research excellence centres that bring together HEIs and the industry. Integration of research and education will expand opportunities for students and educators to develop their knowledge and skills in innovative projects and will support high-quality teaching and learning. This integration should be sustainable, i.e. should not be developed on a project-by-project basis but should be based on long-term industry-university cooperation and a knowledge transfer approach. ECSO serves as an enabler of such cooperation but more actions needs to be done among ECSO academic and industrial members towards developing common approaches to education and training.
4. HEIs organisational structures shall address the cyber security domain as a holistic approach. Cyber security shall be embedded in all educational curriculum not just in the specific IT/cyber related ones. R&D and living labs shall be available for industry cooperation and HEIs shall focus more on utilising available resources and results in current educational curriculums.
5. A cyber security educational framework shall be developed, aimed at delivering an integrated, multidisciplinary approach to cyber security training, exercising and certification, allowing different expertise in the organisation to understand how they shall cooperate to be prepared and defend the organisation. This integrated framework and methodology shall provide an integration of academia and training industry know-how and the technical capabilities and resources available to deliver and validate the knowledge.
6. Cyber security related trainings, educations and certifications shall be comparable and also the gained knowledge shall be validated. HEIs and the training industry shall focus on non-graduated professionals offering courses specialised for them (with certification or graduation possibilities), while industry can offer train-the-trainer courses specialised for HEI lecturers providing up-to-date knowledge for them.

[10] https://www.enisa.europa.eu/publications/cyber-hygiene
[11] See for example: https://maennel.net/research-course.html

Through close cooperation between academia and industry, both parties can benefit and strengthen each other. Industry can help utilise and monetise HEI's project results, while HEIs can offer their resources to assess real-life projects (for research and educational purposes).

Ultimately, cyber security education needs to start in schools to get young people interested in technology, IT and cyber security topics. For now, we have to address the massive skills gap. The cyber security domain can be considered unpopular due to it having a bad culture, high burnout rate, and somewhat limited career perspectives[12].

We also need to shift towards a gender balanced culture [6]. Women already active in the ICT market suffer from additional pressures and negative stereotypes. According to Eurostat statistics in 2014, women employed in the ICT sector vary from 12% in Cyprus to 32% in Bulgaria[13]. Women are still held back by stereotyped thinking; most girls drop out of studies after secondary education. This can be attributed partly to lack of support from role models, persistent stereotyped views that the sector is better suited to men, a lack of understanding about what cyber security jobs entail, and in some cases, how easy or difficult they find the subject. Most girls generally enjoy ICT studies and are competent users of computers and computer operating systems [7], but this enjoyment does not transmit into careers. Female role models generally exert strong influence on girls making decisions about further study/careers. These role models are not always 'tech-savvy'. The support of parents and teachers has a crucial influence on girls during the development of their interests in science, technology, engineering and mathematics [7]. Schools that engage and counteract stereotypes can strengthen and shape girls towards developing an interest in science – including the area of ICT. Similarly, in the case of parents, their awareness of the huge importance of digital competences and knowledge of how they can use acquired skills can translate into support for a child to develop interests in this direction.

[12] https://venturebeat.com/2017/11/11/why-cybersecurity-workers-are-some-of-the-hardest-to-retain/
[13] http://ec.europa.eu/eurostat/statistics-explained/index.php

3 Conclusion

The field of education itself is changing fast. It can be expected that the commercialisation of higher education, including the rising cost of education and growing number of students, will soon lose the students to affordable and widely accessible MOOCs, unless those are effectively incorporated into the university teaching repertoire. The online courses scale better and can sometimes offer the same level of knowledge at a cheaper price. However, institutions that stick to strong academic values will find themselves equipped with a rich learning environment for graduates of the information-age. Those institutions can discover the transformative potential of modern technology, but the high quality of the institution will always have to come from inspired teachers. We need to find ways of retaining those teachers and strengthen research excellence courses.

With regards to cyber security, we are already in a crisis for not producing enough skilled experts that the industry is desperately looking for and stakeholders also lack the knowledge to understand the nature of the cyber domain. We urgently need a "constructive transformation of higher education", but we need it to rapidly react to such needs for high growth. **It is important that we do not compete but strengthen the synergies between higher education and professional trainings**.

To satisfy the growing demand for skilled cyber security professionals, we need to expand educational opportunities at all levels; increase the number of qualified educators; create synergies between educational paths and training possibilities at a workplace; reach the skilled unemployed and displaced workers (workers who are not happy with their current profession); and create the fundamentals of lifelong learning in cyber security. We also need to ensure gender diversity and inclusiveness of cyber security education and training, to inform and encourage girls and women to engage into cyber security careers. To achieve this, a working cooperation is needed between academia and industry which utilises and combines their available resources to ultimately strengthen the cyber domain together.

References

[1] J. Collier and A. Martin, “Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand,” draft, 2017.

[2] D. Garrison and H. Kanuka, “Blended learning: Uncovering its transformative potential in higher education,” The Internet and Higher Education, vol. 7, no. 2, pp. 95 – 105, 2004.

[3] B. S. Bloom, “The 2-sigma problem: The search for methods of group instruction as effective as one-to-one tutoring,” Educational Researcher, vol. 13, no. 6, pp. 4–16, 1984

[4] D. E. Stephen, P. O’Connell, and M. Hall, “‘Going the extra miler’, ‘fire- fighting’, or laissez-faire? Re-evaluating personal tutoring relationships within mass higher education,” Teaching in Higher Education, vol. 13, no. 4, pp. 449– 460, 2008.

[5] K. Maennel, “Improving and Measuring Learning Effectiveness at Cyber Defence Exercises,” Thesis, University of Tartu, Estonia, 2017. http://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=58410&year=2017.

[6] T. Wheeler, “Women in Tech: Take Your Career to the Next Level with Practical Advice and Inspiring Stories”. New York: Sasquatch Books, 2017.

[7] A. Gras-Velazquez, A. Joyce & M. Debry, “Women and ICT - Why are girls still not attracted to ICT studies and careers?”. European Schoolnet, June 2009.