EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

Gaps in European Cyber Education and Professional Training

WG5 I Education, training, awareness, cyber ranges

NOVEMBER 2017

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 programs 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 daily basis. There is clearly a lack of qualified cyber security professionals[1]. The demand for cyber specialists and experts is greater than the supply. This is making us increasingly vulnerable. Governments, associated with different stakeholders, should tackle this problem of cyber security skills gap through more education and training accredited offers.

This has become a very high priority to the European Commission, which is addressing this skill gap through several programs, 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. 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 that. A security system operated by a person lacking required competences is not an asset, but a liability and ultimately a bad investment.

While investing money might not be the major obstacle any more, today's real problems are: time, availability of top qualified teachers and number of students interested in high-skilled jobs. Time is not compressible, and it will remain an issue. Secondly, highly qualified teachers will be an issue for the coming years, as "decision makers" are not sufficiently investing in their salary—the industry is paying much more and leaving universities with the problem of retaining their teaching staff. Number of students could be improved for instance with more awareness on availability and kind of future jobs and intruding cyber security topics not later than secondary school level (probably even before). Also, we have to find a solution to the "gender issue", as we are losing almost 50% of chances to get more qualified experts, because women are not aware of opportunities in cyber security. The cause of a disparity is mainly based on a false perception of science as a field of typically male, and lack of support for girls at all levels of education in the choice 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 sustainability of development of the world economy. Bridging the skill gap of qualified cyber security professional by 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 skill shortage is to find a short-term "patch" the problem. For example, universities have "added" a Cyber Security undergraduate or graduate degree to their curricula. This is often viewed as a "specialization" or "add-on" to a Computer Science degree.

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

Unfortunately, many curriculum designers fail to realize 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 program 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 loose academic values (such as critical thinking).

The last 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. Decay of academic degrees[4] have been reported manifold. Without an academic degree it is very hard to get a job, but as more and more students obtain such degrees there is also no distinctive advantage anymore for graduates. In fact, industry asks more and more for specific skills to be covered in university programs. In the area of cyber security, most of those skills can actually be obtained through vocational education or profession trainings—a university degree is not required. Especially, now most employers rank hands-on experience and professional certifications above a degree as the best two ways to acquire cyber security skills.

1.1 The Problem of the Higher Education Industry

Accredited certificates that universities issue are challenging to compare internationally. In order to ensure employability of graduates, universities are more and more focusing on teaching detailed knowledge of the particular subject area. The danger is 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 have to include basic skills on technical details (e.g., firewall management), but need to have enough focus on broader concepts.

It is important that the following aspect will not be forgotten in this argumentation: universities are supposed to be more than an accumulation of information. One of the academia's cornerstones was always the transformation of thought, the ability to dissect scientific concepts and to think in abstract forms and structures. Those are values of higher education since Socrates or Plato, but

[4] http://content.time.com/time/business/article/0,8599,1946088,00.html

they have changed in the light of large commercialization[5]. This commercialization is slowly leading to a decay of the quality of our graduates. Governments and universities want a return on their "investment" and charge high fees to students.

We are now at a critical time; higher education is transforming, and this can either be a blessing or a curse. We are looking at a growing budget in cyber security, but we need to make sure the budget is wisely invested. Universities should have to deal with 20% of very high skilled education that nobody else could offer (provided Universities can retain the appropriate teachers). They should not try to compete with other "professional training providers", which will likely provide the education / training for the remaining 80% of "skilled jobs". However, students and employers are expecting that university graduates receive an education that equals a professional training. In order to make the university graduates employable, we can now use the technology, such as Massive Open Online Courses (MOOCs), to our advantage in addition to traditional classroom teaching methods. MOOCs can (and probably should) replace large-scale lectures, as they are cheaper, operate at large 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 globalized world and difficult to obtain via MOOCs. So, the universities need to integrate all available training methods 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].

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 raising. The skill 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 in particularly important, as such organisations are often fundamentally differently funded from academic institutions, but 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 in- vest 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 the staff for fear they may leave once the training is over. Training can be quite expensive, depending on the type of certification, and the indirect costs & associated disruption of operations when members of staff attend the training courses.

Therefore, it can be more "convenient" for companies to hire graduates of higher education programs. But there is a shortage of the cyber security programmes offered by the academia, that fulfil the need and requirement of industry. Universities do not focus on what is needed by the industry, as the cost of including professional certifications to the curriculum means higher tuition fees for

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

the students and all the issues such increase would bring along. Universities too have challenges in sourcing for staff capable of delivering the hands-on experience and certifications sought after by the industry. In fact, universities can hardly compete with the industry where a suitable professional can command much higher compensation. Universities have a slow accreditation process—it takes time for a new programme of study to be developed and validated to be lectured. If academia wants to ad- dress to the cyber security skills gap, it needs to incorporate practical learning and professional certifications into the academic programs.

Therefore, the community, academia and professional training providers are forced into a market niche, where providing trainings that address a specific skill 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

We should be aware that students will enter with a different background. The education has to cater for this, including for people that join later on than just 18-year olds. To illustrate the challenges and opportunities that the interdisciplinary nature of cyber security image a MSc-level course on “hardening operating systems”, and also imagine one student with 10 years of system administration experience (yes, there are such students) attending this course, and another student being a graduate from an IT-Law program (without much “traditional computer science” background knowledge). Clearly both students are among the target audience.

However, with traditional teaching methods it is nearly impossible to teach such a course: the experienced system administrator will be fundamentally bored, while the law graduate would be lost right after the first set of lectures. And while informal feedback from students typically confirms that they enjoy the breath different backgrounds of their colleagues, it poses unique challenges on the teaching methodology.

However, here are the unique opportunities for “flipped classroom”[6] and “Education 3.0”[7] teaching approaches. The student from our example with 10 years of system administration experience, might have to learn about the difference be- tween criminal and civil law; while the lawyer will have to understand what a bash shell is. For this MOOCs can be an excellent enabler. Students can work in their own pace through areas where knowledge is missing. The quality of an online learning course is often also much better than the quality of a random unmotivated and overworked lecturer. 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 and focusing on creating a positive feedback loop should be a fundamental part of the teaching strategy.

The overall mix of students with different backgrounds and future dreams will then create an inspiring atmosphere, to delve into a discourse and create an understanding for the interdisciplinary problems we are facing. This forms the basis for a constructive transformation of higher education, which integrates disruptive learning and teaching techniques instead of competing with them over the same market-share.

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

[6] https://en.wikipedia.org/wiki/Flipped_classroom
[7] https://en.wikipedia.org/wiki/Education_3.0
[8] https://en.wikipedia.org/wiki/Secure_Shell#Version_2.x

the time to solve such tasks could be a suitable metric to assess the skill-level and, dependent on the outcome, the system 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, detecting threats and responding to anomalous situations and incidents.

Overall, this area has also 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 that aims at identifying hidden talent.

2.1 The Value of Universities and Professional Trainings

One big question remains unanswered. How do we bridge in the future the academic values into a curriculum already filled with technical details? 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 academic thinking.

For universities it will be important to engage students in scientific discourse. Today there is a wide choice of technology that allows us to optimize 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 careful mix between asynchronous Internet technologies with face-to-face learning. It is important to appreciate the different cultural back- grounds 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 in a meaningful way, but it is equally important to let inspiring teachers what they can do best[9]. Engage students from various cultures, genders is 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. In particular, in cyber security our graduates need to have a lot of technical knowledge, but it's important to develop meta-cognitive processes that transforms 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. Especially, this interdisciplinary nature of cyber security requires novel teaching methods and strategies.

2.2 Solving the Dilemma of Cyber Security

The problem of cyber security, as illustrated above, starts with the widely recognised skill shortage and the interdisciplinarity of the field[10]. Teaching organisations need to "produce"

[9] https://www.theatlantic.com/education/archive/2013/11/dont-give-up-on-the-lecture/281624/
[10] https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

lots of skilled people. Companies pay a lot of money for qualified experts, and many positions remain unfilled despite the fact that companies pay horrendous salaries. This in turn means that 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 large scale Cyber Defence Exercises (CDXs)[11] will be the only feasible answer to the skill shortage problem. Therefore, research into adaptive learning platforms are the way forward to train the required large number of students—and there is nothing wrong with this method. The number of teachers is low, the number of students high, and that leads to a situation where the teachers are overloaded. Regardless of how qualified or good they are, the output that is produced lacks quality and the amount of time that can be spent with each individual student is low. The vicious cycle continues, as the students will realise what value they get from a university and what value they get from professional trainings (or MOOCs). The point to understand is, that if MOOCs (including automated CDXs and so on) would be sufficient to train the next generation work-force, there would simply be no need for tier-2 or tier-3 universities anymore (at least in the context of cyber security education).

Note that this applies only to tier-2 and tier-3 "thinking" universities, as one will easily realise that the described vicious cycle is exactly the opposite to Bloom's 2- sigma-problem. MOOCs and CDXs cannot replace critical thinking and the value that one-to-one tutoring [2] brings. For example, Stephen et al. (2008) [4] discusses the need to breaks the barrier of "accessibility" or "approachability". If we take, for example, the idea behind colleges at top-tier universities, such as Kings College at Cambridge University, where students and academic staff are typically living together. There is an academic discourse from different disciplines conducted during joint dinners. The barriers a broken down in a very subtle and gentle way: academic fellows and students are joined together in social activities. A joint dinner cannot really be perceived as "taking up tutor's time"—the tutor has to eat anyway. From there a discussion unfolds, and then the tutor is not seen any more as this unapproachable person, but as a human being. Furthermore, every so-called fellow of the College has mandatory tutoring time with students. That is significant one-to-one time giving students of the college the 2-sigma-advantage [2].

No surprise that top-university graduates are doing that well. What can be done? The proposed solution should have become obvious from the discussion above:

1. Invest research into teaching-methods that scale in order to address the skill- shortage problem. For example, ECSO SWG 5.1 efforts guide towards improving skills through Cyber Defence Exercises. 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 is looking at raising the awareness levels through various "cyber hygiene"[12] initiatives.
2. We need to invest into novel teaching methods that sufficiently accounts for the interdisciplinary nature of a Cyber Security curriculum[13]. This includes a positive integration between MOOCs, CDXs and scalable professional trainings, with more individual and academic approach. Especially, MOOCs are good at teaching the "simpler

[11] https://ccdcoe.org/locked-shields-2017.html
[12] https://www.enisa.europa.eu/publications/cyber-hygiene
[13] See for example: https://maennel.net/research-course.html

parts" of a field at highly scalable-levels, where more "complex topics" requires interactive discourse between teachers and students. This might require a fundamental shift in thinking on how we teach courses at higher education institutions as well as in cooperative set- tings or the context of professional trainings. This is one of the efforts in ECSO SWG 5.2.

3. Invest into more academic cyber security research excellence courses that bring students, which have the ability and interest, to the next level and help them to go beyond learning today's skill-set. This will preserve an academic atmosphere and create a culture that will hopefully also spark to a larger community.

Ultimately, cyber security education needs to start in schools and get young people interesting in technology, IT and cyber security topics. We also need to change towards a gender balanced culture [6]. For now, we have to address a massive skill gap. Important to train and retain good people. The cyber security domain is unpopular due to having a bad culture, high burnout rate, and somewhat limited career perspectives[14].

Finally, we need to address the gender-balance. In 2013 in the United States only 18% women graduated from information technology studies. This is despite the fact that it is very easy to find a job (72% of girls in high schools in 2015). Women, already active in 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[15]. 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 'tech-savvy'. The support of parents and teachers has crucial influence on girls during the development of their interests in science, technology, engineering and mathematics [7]. Respectively school that is engaging and counteracting stereotypes can strengthen and shape girls towards developing interests 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 used acquired skills can translate into support for a child to develop interests in this direction.

[14] https://venturebeat.com/2017/11/11/why-cybersecurity-workers-are-some-of-the-hardest-to-retain/

[15] 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 commercialization of higher education (including raising cost of education, raising numbers of students) will soon lose the students to affordable and widely accessible MOOCs, unless those are effectively incorporated into university teaching repertoire. The online courses scale better and can 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 industry is desperately looking for. 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.

The higher education cyber security courses must not just become professional accreditation schemes. Those are better taught by the professional training providers. However, if the private industry takes over the university courses and largely steers the direction of courses, then other areas (such as privacy, digital rights, human factors, etc.) would be neglected.

There is a big challenge in front of schools, teachers, politicians to fight against the stereotypical assumptions about the roles of women in the ICT. Educational institutions should play a significant role as main communication channels to inform and encourage interested girls to participate in ICT trainings, faculties as well as job fairs.

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

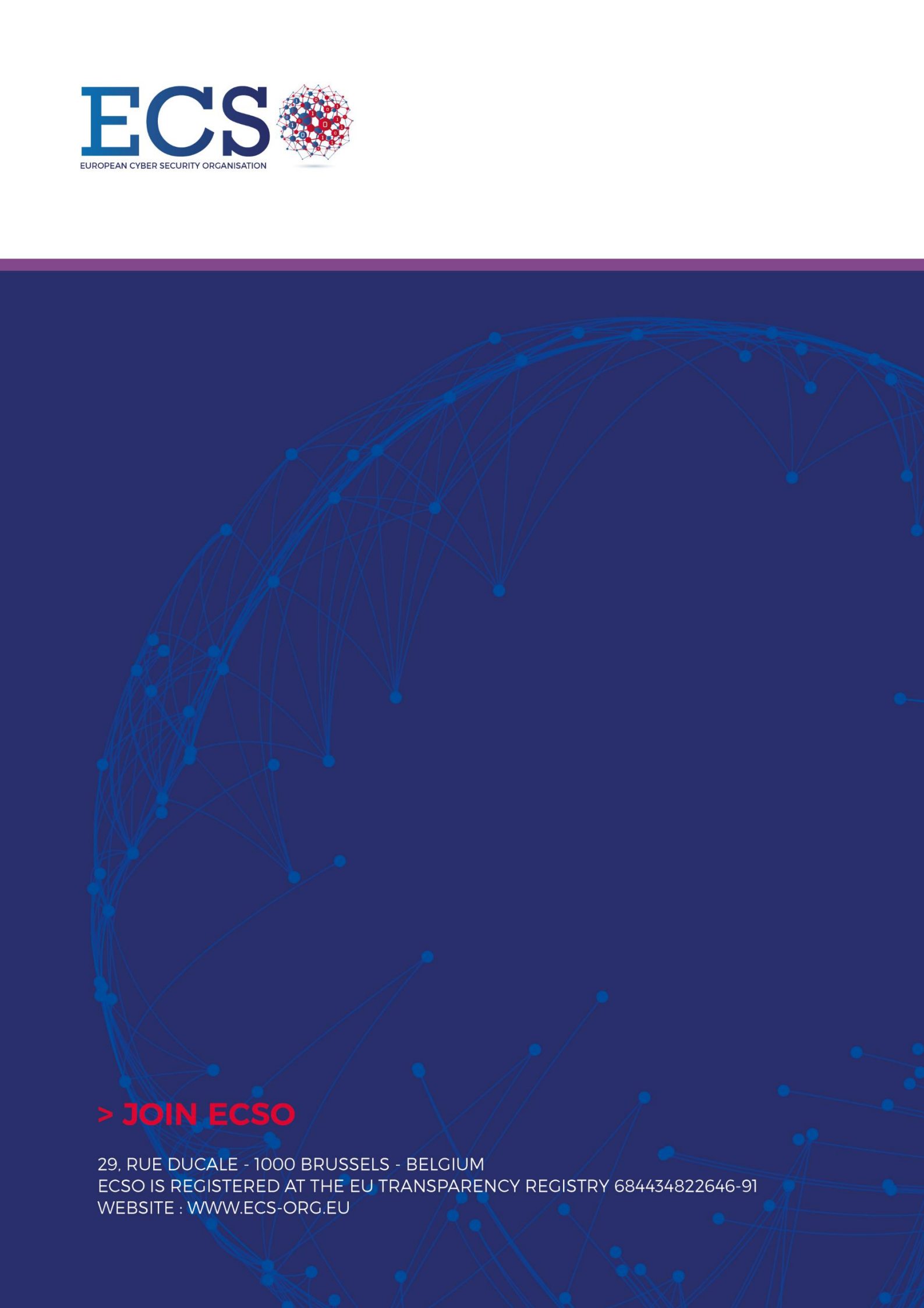
[4] D. E. Stephen, P. O’Connell, and M. Hall, “‘Going the extra miler’, ‘fire- fighting’, or laissez-faire? Re-evaluating personal tutoring relationships within mass higher education,” Teaching in Higher Education, vol. 13, no. 4, pp. 449– 460, 2008.

[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.

ECS
EUROPEAN CYBER SECURITY ORGANISATION



> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU