European Union
European Social Fund

Investing in your future

praxis
think tank

Labour force and skills needs in cyber security in Estonia. Main conclusions.

Kirsti Melesk, Eve Mägi, Kaupo Koppel, Aleksandr Michelson

The rapid development of information and communication technologies (ICT) has increased dependence on the cyber space among individuals as well as economies and governments more widely. Public services are increasingly dependent on the cyber space, including vital services like rescue, electricity and water supply, phone and data communication, currency circulation, payment services or personal identity management.

These developments raise the need for skills and knowledge on cyber security, to prevent and adequately react to security incidents in the cyber space. **The aim of this research is to map the labour force need in cyber security in the next five-year perspective in public and the private sector**. To achieve this, the Estonian cyber security sector is mapped for the first time together with cyber security main competences required in the sector. The focus is on companies offering cyber security products and services, cyber security in the public sector and on companies offering vital services (emergency care, electricity supply, banking and phone and data communication). The analysis includes an overview of the education and training opportunities and needs in cyber security in Estonia.

By 2023, Estonian cyber security sector needs additional 270-870 specialists with skills and knowledge in the field. Compared to 2017, this is an increase of 32-86% in labour force.

According to the most conservative scenario, there is a need for additional 270 specialists with cyber security skills and knowledge. The scenario foresees a context, where there are no leaps in sector development (number of new companies is low) and the growth pace of cyber security companies is low. The companies themselves foresee a labour force growth rate of around 10% per year, which means there is a need for an additional 800 cyber security specialists after five years' time. It also needs to be considered that the need for cyber security skills is spans into other sectors as well that are not covered in the current research. This raises the labour force need even further. Thus, it is important to ensure the availability of qualified cyber security specialists in Estonia to support the growth of the sector in Estonia.

To cover the labour force need, varied career paths need to be reinforced in cyber security. This is built on a pyramid of skills development, where talent growth is supported by a wide base of cyber security skills, which spans across sectors. This also reinforces implementation of cyber security skills in fields outside of ICT. The specific and in-depth cyber security skills rely on a wider base knowledge that is acquired relatively early in the education system. The research outlines four key areas for the growth of qualified cyber security specialists to meet the labour force needs.

Training of people with no ICT background in cyber security

- The main path into cyber security is from ICT backgrounds – a sector that suffers from heavy labour shortage in Estonia. Hence, the question is whether to put the burden of covering labour demand in cyber security only on the ICT sector or whether to widen the potential pool of labour force with varied skills backgrounds
- Almost sixth of cyber security specialists have their background in other fields than ICT, including law, financial management, history or international relations. These skills are represented in different tasks, including analysts and cyber security management.
- Companies indicate that the presence of formal cyber security training is not primary upon recruitment. The main focus is on ICT knowledge and openness to continued learning.
- The main obstacle on recruitment outside of ICT is the relative difficulty and technicality of the cyber security field. Hence, there are limitations to the tasks or functions that can be filled with no prior or basic technological skills.
- Inclusion of people outside ICT has become part of the skills development strategies in many countries. For instance, Singapore aims at increasing the number of cyber security specialists through training for specialists in areas related to cyber security.

Priority action: widening of cyber security career paths. Cyber security tends to be viewed as a closed circle requiring high level of very specific skills. This reinforces entry barriers – recruitment focuses on very specific fields and people outside of ICT do not recognise cyber security as a potential career option. Hence, it is necessary to increase knowledge about the potential career paths in cyber security and its necessity outside of ICT.

This is supported by the following roles:

- The success stories of cyber security companies recruiting outside of ICT is a positive role model for other companies, offering examples of more varied recruitment patterns.
- Widening national defence courses from upper secondary schools to the basic school level might increase an interest towards the cyber defence service in the armed forces.
- Universities and vocational schools can introduce courses on cyber security, such as risk management, secure programming etc. This can give the basic level of knowledge to people with no prior ICT training.
- Cyber security component is also necessary in teacher training (including initial training and additional training), together with elementary digital skills and risk management in cyber space.
- The opportunity to acquire basic level of knowledge in cyber security could be provided by attractive learning materials like video lectures or computer games. These could be developed in cooperation by policy managers (in education, cyber security and defence), schools and companies. These skills should be certified in order to make them visible to potential employers.

Supporting the development of cyber security skills among youth across education levels

- Cyber security skills are mainly acquired outside of formal education, through hobby groups or self-learning. Primary skills and attitudes, which are important for raising interest towards cyber security, develop in young school age. To support interest towards of cyber security and raise knowledge of the potential career path among youth, more systematic guidance of interests in formal education is necessary.
- Currently there are some elective courses on cyber security in upper secondary level, one school has implemented a specialised field of study in cyber security, which are supported by cyber security contests and exercises for students. However, these activities are not coordinated and access is random rather than systematic.
- Development of cyber security skills among youth need to be integrated into ICT and teacher training. In higher education, cyber security skills are necessary for study fields in health care and law.
- Currently a small group of students have access to cyber security training at upper secondary level (one school offers specialised training) while for most students, basic skills level is acquired in higher education or additional training. Many experts stress the need to provide basic cyber security skills in general education, which enables to focus on more specialised training at higher education level.

Priority action: Development of a system, which is able to notice, support and guide the cyber security interest of students relatively early. This requires increasing the knowledge among people able to fill this role and building a network to support their activities. It will also be necessary to break the stereotypes of cyber security being a military and male-dominated field.

This is supported by the following roles:

- Goal setting, involving various fields in policy development (education, cyber security, defence) to identify the main aim for cyber security skills in formal education, set out the necessary action plan together with the resources necessary to achieve the goal. This supports the transfer from project-based activities to systematic development of cyber security skills among youth.
- Central role is on ICT teachers and education technologists, who can notice interest, provide basic skills and knowledge, organise cyber security events in schools, guide students towards cyber security contests or groups and guide talented students towards more in-depth training. They can also provide basic skills for other teachers and involve students into digital training of teachers.
- Cyber security and digital competences need to be part of teacher training to support the growth of qualified ICT teachers and education technologists. In addition, cyber security topics could be integrated in various subjects, including writing essays on these topics, integrating with mathematics and English subjects.
- The Estonian Information Technology Foundation for Education (HITSA) could provide basic and additional training for teachers, involving cyber security experts, trainers in companies, public sector and potentially also talented students. HITSA can also support the development

of a support network for teachers, education technologists and science schools for more interested students.

- Teachers in science schools support ICT teachers in noticing and developing cyber security interest and talent by providing information on specialised events, assignments for more interested students and creating networks of interested students. It is also necessary to further develop and test the methodology for teaching cyber security in schools to know which methodologies provide the best results.
- Parents can support cyber security interests among their children. Parents need knowledge on cyber security, guidance from teachers or basic courses on the topic. This involves recognising the role of computer games, which are often the source for cyber security interest.
- It is necessary to ensure on a national level that access to cyber security contests and training is provided despite the geographical location or socioeconomic background. This requires organising cyber security contests or work groups outside the two largest cities of Tallinn and Tartu and open these to younger students as well.
- Career counsellors need additional information (or training) on cyber security career prospects, with the focus on breaking the main stereotypes of military oriented or a male dominated field. This widens the career options in cyber security and supports the involvement of girls in cyber security training.

Integrating cyber security skills in ICT training

- ICT training is the most common pathway into cyber security. The most popular fields of training in cyber security are related to ICT, including informatics and IT system administration.
- Specific cyber security skills are mostly acquired through self-learning or taking part in training courses. There are some cyber security courses in ICT higher education. However, the topics covered are not systematic across all ICT programmes and these are often offered as elective courses.
- Integration of cyber security in ICT programmes have two potential effects: (A) support the training of IT specialists knowledgeable in cyber security and (B) guiding interested ICT students towards cyber security careers.
- From the cyber security perspective, the most important ICT fields are systems administration, systems architecture, informatics and programming. Cyber security is competing for these skills together with the whole ICT sector more widely.
- Employers stress that instead of very specialised people, there is a need for a wide base of knowledge and skills in ICT, to understand the needs of different roles in the production process.

Priority action: Integrating cyber security in ICT programmes in higher and vocational education. The aim is to implement the security by design principle already from the first stages of building hardware of software. Cyber security courses should be available to current students as well as ICT specialists already working as additional training.

This is supported by the following roles:

- Involving the policy developers in the field (cyber security, defence, education), a framework needs to be developed to introduce the options to pilot security by design principle in ICT programmes, collecting and introducing good practices and development or adjustment of respective methodologies.
- ICT programme development in universities can introduce additional cyber security courses in programmes or integrate this in existing courses, involving employers and organisations in the field of cyber security. Experts have highlighted as priority topics in cyber security: risk management, secure programming, cyber security standards (for processes and products) and related legislation (local as well as international). The skills acquired in ICT should include analysis, recognising the integrity of a information system, identifying security issues and assessing its priority level, understanding the process of building security protocols.
- Cyber security companies and organisations could be involved in teaching cyber security courses and providing additional training, also providing opportunities for traineeship in cyber security.
- ICT programmes could be complemented with experience learning, i.e. learning by experiencing real security issues and consequences of weak security protocols. This is supported by developing the necessary methodological materials with cyber security experts and companies. This requires access to information on cyber security incidents for learning purposes.
- Cyber security students can be involved in training of ICT students, including supervising practical seminars.
- ICT students with cyber security skills could be further involved in teaching and supervising students as well as teachers in general education, including preparation of courses and teacher education.

Cyber security talent attraction and retention in the global labour market

- ➢ Cyber security labour market is global – the talent search of companies spans across boarders. This enables widening the search for very specific skills that are in shortage in the local labour market or are not available at all. Companies find that involving foreign employees also support their export activities.
- ➢ There are not many foreign employees in Estonian cyber security companies. Foreign employees are mostly involved in specific projects and in large companies. In international companies, experts move flexibly between the different units across countries. Hence, local units can use the skills and knowledge available in other country units of the international company.
- ➢ There are some important limitations for the recruitment of foreign specialists in cyber security, particularly in relation to cyber defence and limitation of access to sensitive information. Another obstacle is in language barriers – the local standards and legislation are in Estonian, making it difficult for foreign employees. Finally, there are additional obstacles for recruitment of foreign employees, common to all sectors, including the difficulties in supporting adjustment with the local community, difficulties with formalities, language barriers etc.

Priority action: Development of national support for the recruitment of foreign talents. The aim is to create an environment that supports companies in recruitment of foreign specialists and introduce Estonian cyber security companies in international markets.

This is supported by the following roles:

- Ministry of Finance, with the support of a political decision, can develop measures for (temporary) reduction in tax burden for employers hiring foreign employees. For instance, it has been suggested to reduce the social tax by component dedicated to the first pillar of the pension system.
- Ministry of Interior can support companies in performing additional background checks on potential employees. This means companies can request for confirmation on the fulfilment of the security requirements for people from third countries (outside European Union) from the Police and Board Guard Board. This requires the support of the Ministry of Justice to develop the legislative framework for this type of background checks and define the standards required in the cyber security sector.
- With the cooperation of Ministry of Economic Affairs and Communications, Ministry of Foreign Affairs, Estonian embassies and high-level government representatives related to cyber security, Estonian cyber security companies could be introduced more actively in the foreign markets. This includes making use of current programmes for supporting the export of Estonian companies and adding cyber security element where necessary.
- Introducing the local language and culture for foreign students and foreign employees, relying on the current programmes (e.g. Work in Estonia, programme for the adjustment of foreigners), developing additional activities (integrating Estonian language in courses where possible) and involving them in the local cyber security community through events and networking opportunities.