# European Crime Prevention Award (ECPA)

# Annex I

### Approved by the EUCPN Management Board in 2017

**Please complete the template in English in compliance with the ECPA criteria contained in the Rules and procedures for awarding and presenting the European Crime Prevention Award (Par.2 §3).**

## General information

1. Please specify your country.

Estonia

2. Is this your country's ECPA entry or an additional project?

Country's ECPA entry project

3. What is the title of the project?

The cyber defence field of study at Põltsamaa Coeducational Gymnasium

4. Who is responsible for the project? Contact details.

Tiia Mikson
Põltsamaa Coeducational Gymnasium
Head Teacher
Veski 5, Põltsamaa 48106 Estonia
Mob: +372 5063741
Tel: +372 77 51 500
tiia.mikson@poltsamaa.edu.ee

Kertu Liebert (enquiries in English)
Põltsamaa Coeducational Gymnasium
Project manager
Veski 5, Põltsamaa 48106 Estonia
Mob: +372 59191445
Tel: +372 77 52 525
kertu.liebert@poltsamaa.edu.ee

5. Start date of the project (dd/mm/yyyy)? Is the project still running (Yes/No)? If not, please provide the end date of the project.

The project is ongoing.

Preparation period: January 2015 – August 2015.

First stage: 01.09.2015 – 31.05.2018 (The first cohort completes the 10th, 11th and 12th grade)

Second stage: 1.01.2016 – 31.05.2019 (the second cohort)

Third stage: 01.09.2017 – 31.05.2020

End of project: cannot be predicted at the moment

As of September 1, 2017, 55 students are enrolled in the cyber defence programme.

6. Where can we find more information about the project? Please provide links to the project's website or online reports or publications (preferably in English).

**In English:**

http://in.reuters.com/article/us-estonia-cybersecurity/with-an-eye-on-russia-estonia-seeks-security-in-computing-cloud-idINKBN0TN1BT20151204 – A Reuters story on cyber security in Estonia for background. Clips filmed at Põltsamaa Coeducational Gymnasium were used in the footage.

https://www.youtube.com/watch?v=YT8g_uU4ew0 – Ukraine Today's story on Põltsamaa Coeducational Gymnasium

http://www.zdnet.com/article/cyber-security-for-kids-the-earlier-we-teach-this-the-better-specialists-well-have/ – ZDNET article on the school's efforts

https://vp2006-2016.president.ee/en/president/ieva-ilves/ieva-ilves-in-the-media/12039-2016-02-20-13-05-28/index.html – school visited by the head of Latvian cyber security initiatives.

**In Estonian:**

http://reporter.postimees.ee/3558793/poltsamaa-uhisgumnaasiumis-opetatakse-kuberkaitset – overview of the programme by an Estonian news show.

https://tv3play.tv3.ee/sisu/seitsmesed-uudised-2016/772512?autostart=true – another overview.

https://koolielu.ee/uudiskiri/readnews/520039/milleks-gumnasistile-kuberkaitse – an article on a popular education website.

http://www.kaitseliit.ee/et/poltsamaa-uhisgumnaasiumi-opilased-opivad-kuberkaitset – press release on cooperation by the Estonian Defence League

http://www.err.ee/554785/ieva-ilves-raakis-poltsamaa-uhisgumnaasiumi-opilastele-kuberkaitsest – school visited by the head of Latvian cyber security initiatives.

http://etv.err.ee/v/kultuurisaated/saated/d04d5e83-185f-46f9-a41d-80915bc549e8/aasta-opetaja-gala-eestimaa-opib-ja-tanab – Põltsamaa Coeducational Gymnasium also won “Accomplishment of the Year in Education” for starting the programme.

7. Please give a **one page** description of the project (**Max. 600 words)**

Põltsamaa Coeducational Gymnasium has opened a cyber defence field of study (3-year upper secondary school programme). The project, which is ongoing, started with initiative from Põltsamaa Coeducational Gymnasium and has evolved with the help of several key partners, who supported it (listed in the "partners" section).

On November 9, 2015, the key partners signed a cooperation agreement at the school. Thus, we became probably the first high school in the world to open this specific field of study at the upper secondary school level.

The cyber defence curriculum of Põltsamaa Coeducational Gymnasium has 4 cyber defence courses (35h each):

1) Information society. Key topics: defence strategy; data and social media; gathering and use of data; the EU digital market; e-Estonia and its components; the culture of a digital society; device security; the legal basis of (cyber)security; contemporary threats (including cyber warfare, hybrid warfare).

http://www.poltsamaa.edu.ee/public/files/Ainepassid/Kyber_infoyhiskond.pdf

2) Information technology: the basics of safe networking. Key topics: the basic principles of physical and IT-related network security; common mistakes in creating safe networks: detection and prevention; overview of critical IT infrastructure (at a service provider in the field in Estonia).

http://www.poltsamaa.edu.ee/public/files/Ainepassid/Kyber_turvaline_vorgundus.pdf

3) Digital security and cryptography. Key topics: the principles of a digital lifestyle in Estonia; the history of cryptography; modern cryptographic solutions; institutions that ensure the operation of a digital lifestyle; e-Estonia: structure and operation; responsible and informed use of social media.

http://www.poltsamaa.edu.ee/public/files/Ainepassid/Kyber_turvalisus_kryptograafia.pdf

4) Introduction to mechatronics. Key topics: the history, trends and scope of use of mechatronics; the functioning of various sensors, microprocessors, controllers, actuators and software; tools and materials in mechatronics; safety and safety equipment; UAV types; UAVs (DJI F550) – construction and operation/flying (FrSky Taranis X9D); the theoretical methods of deploying UAVs in warfare

http://www.poltsamaa.edu.ee/public/files/Ainepassid/Kyber_mehhatroonika_UAV.pdf

The 3-year programme has the following structure:

During the first trimester of Year 1, students learn national defence (3h a week, 35-hour course). In the second and third trimester, the focus is on Information technology (35 h) and mechatronics (35h) (robotics and UAVs). Both theoretical and practical learning is used. A technical drawing course (35h) supports these courses. During Year 1, students usually have the training visits at the NATO Cooperative Cyber Defence Centre of Excellence, e-Estonia Showroom and Estonian Information System Authority.

During Year 2, students learn via an integrated syllabus (2h a week, 70 h in total) of safe networking, cyber security, cryptography and mechatronics (UAVs). The additional courses are 3D modelling (35h) and programming (35h). During Year 2, students have training visits at Santa Monica Networks and The Estonian Foreign Ministry.

In Year 3, the course Basics of safe networking continues based on the Mikrotik programme (35h) and students take an exam to obtain an MTCNA certificate.
https://www.mikrotik.com/download/pdf/MTCNA_Outline.pdf

In total, students pass 10 courses (350h) in the cyber defence field of study, which are complemented by three training visits and practical programming at the University of Tartu Computer Science Institute. All added together, this makes 400h of study.

Various learning methods are used: seminars; Skype-lectures; watching relevant film (for example, *CyberWar Threat* by PBS NOVA); practical projects; training visits etc. Lectors include specialists from the Estonian Information System Authority, the National Cyber Defence League, and the Center for Communication and Information Security Research and Development. Here are some examples of practical assignments:

1) analysing a case study of information manipulation – the sides, root and motivation in the conflict
2) virus detection with virustotal.com
3) compiling network schematics
4) IP address detection and operations
5) security audit on a device; scanning a file for threats; setting up firewalls
6) analysis of standard contracts
7) case study with the emphasis of finding the applicable law.

## I. The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.

8. How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

By giving students knowledge and practical experiences in the cyber security field, including cyber hygiene, we are shaping legally informed and responsible behaviour in young people.

As students do case studies on information manipulation, they understand that conflicts have sides and motives. This also instils the knowledge that no one will remain anonymous and every activity leaves a trace – every perpetrator is identifiable. This is something that young people often lack an awareness of.

Through immersing themselves in practical activities like compiling network schematics, analysing one's IP address or setting up a firewall, students gain personal cyber-crime prevention skills, which are crucial, but also rare nowadays.

Being aware of the threats that lurk in cyber space and having the know-how to prevent them, students evolve into informed cyber space users and as carriers of their knowledge, become cyber-crime preventers themselves. Most importantly, they acquire the principles of ethical behaviour in the modern digital society.  Fears can be alleviated when students know that the law protects and they know how to recognise a cyber threat and where to turn. Therefore, they can also alleviate the fears of family members and friends. In addition, society as a whole would feel safer if there was general knowledge that there are enough cyber security experts to govern the field and protect people with a more limited knowledge. This is one of our goals – to feed more eager learners into higher education in this field.

When students learn about UAVs, they also learn about the criminal activities that can be perpetrated with the help of these easily accessible devices. For example, a person's private room is breached, a drone can be flown over private land in preparation for theft; a drone can be used to gather illegal information both in public and private places. All these fields are covered by legislation, but few drone-owners, especially young people are aware of the legal implications. This is a double threat – citizens are likely to both become victims and perpetrators without knowing the laws and regulations affecting this field. Therefore, at Põltsamaa Coeducational Gymnasium, cyber defence students learn about both the practical skills and the laws and ethical implications of all the topics that they cover.

9. How is the project contributing to raising citizens' awareness of crime prevention? (**Max. 150 words**)

Students in the cyber defence programme of Põltsamaa Coeducation Gymnasium will have the basic necessary skills to prevent becoming the victim of a cyber-crime. They know how digital services are set up and what their weaknesses are. They know how to distinguish between the legal and illegal, the ethical and unethical. They know the damage that cyber-crime can cause. They know the value of privacy and identity. They know their rights and responsibilities as citizens soon to be at the forefront of the security of our digital society.

All of this knowledge, the students take home to their communities and with them to new communities at the university or other institution of further education after they graduate. In that sense, they are "carriers" of cyber defence awareness. The more students acquire up-to-date and relevant knowledge, the bigger the number of informed and socially responsible people.

## II. **The project shall have been evaluated and have achieved most or all of its objectives.**[1]

10. What was the reason for setting up the project? What problem(s) did it aim to tackle?

The continuing rapid development of information and communication technologies, globalisation, the drastic increase in data volumes, and the growing number of different devices connected to data communication networks all have an impact on everyday life, the economy and the functioning of a country. This kind of ICT development brings with it better accessibility, increased user-friendliness, improved transparency and functioning of the state, and reduces expenses in both the private and public sectors.

The growing importance of technology also comes with the high dependency of the society, the economy and the state on these solutions. It is expected that the e-solutions work safely and smoothly. However, as we all know, these increases in digital services have also led to an increased risk – there are countless more attack vectors and the attacks themselves have become a lot more complex.

From the student's perspective, the internet has also become very accessible, but the aforementioned threats have made them targets as well. We at Põltsamaa Coeducational Gymnasium set up the cyber defence programme,

[1] For more information on evaluation, see Guidelines on the evaluation of crime prevention initiatives (EUCPN Toolbox No.3): http://www.eucpn.org/library/results.asp?category=32&pubdate

because we want students to keep control of these processes and protect themselves while using ICT responsibly and effectively. Our mission also derived from the constant worries at state level (and globally) about the lack of good IT and cyber security specialists.

Therefore, the idea to start earlier, already at the upper secondary school level with this education seemed the best way to contribute to keeping us all safe. Although the importance of IT had been growing in our education system, no one had implemented an in depth cyber defence programme. This topic was not included in the Estonian National Curriculum, so our school decided to take on this challenge and try to be the trailblazers if needed.  We now see that this idea seems to resonate with many others, as our school has received lots of requests for assisting in setting up a cyber defence elective course (no other full programmes yet) across Estonia. All this interest and feedback shows that we have hit on something truly significant.

Ultimately, our expectation is that through in-depth knowledge of the ethics of cyber space, cyber hygiene and threats, many future cyber incidents can be prevented and the world will gain more competent specialists in this field.

11. Was the context analysed **before** the project was initiated? How, and by whom? Which data were used? (**Max. 150 words**)

Our everyday experiences were enough to show that students spend more and more time in cyber space, but do not understand the possible consequences or impact of their activities. There were no specific learning activities in the national curriculum that would deal with cybersecurity. In addition, we saw that cyber hygiene is a crucial skill after our school and a government agency suffered a cyber attack by a 9th grade student, which rendered our school webpage and internet inoperable for several days. This also demonstrated that cyber defence topics are obviously not too difficult for upper secondary school students. This is the context from which we started the project in 2015.

12. What were the objective(s) of the project? Please, if applicable, distinguish between main and secondary objectives. (**Max. 150 words**)

The goal of the project "Cyber defence field of studies in Põltsamaa Coeducational Gymnasium" is for students to acquire the principles of a contemporary digital lifestyle and act lawfully and ethically in cyber space:

1) Students know how a digital lifestyle works and the institutions that uphold it.
2) Students know the basics of cyber defence and have basic knowledge in cyber security.

3) Students have the skills and habits to act lawfully and safely in cyberspace.
4) Students use practical activities to enforce theoretical knowledge.
5) Students use social media and other digital tools and opportunities safely, responsibly and in an informed way.

6) Students know the principles and sphere of influence of networking and communications techonology and act socially responsibly when dealing with this technology.

7) Students have the skills and readiness to inform their community on basic cyber security.
8) Successful students continue studies in higher education in the IT and cyber security fields.

13. Did you build in internal goals to measure the performance of the project? If so, please describe at what stage of the project and how you measured whether the project was moving in the planned direction. (**Max. 150 words**)

When planning the project, we considered measuring the outcomes extremely important.

1. Firstly, it was crucial that after the end of every course, the cyber defence teachers and the school heads should meet to discuss how the project is working and how the actual learning and course content is matching expectations.

2. As there was no previous experience in teaching cyber defence and the courses had to be compiled from zero, it was decided to continuously improve the courses as the programme progresses.

3. It was also crucial to analyse the resources needed for learning activities

1) teachers, their professional training and additional training

2) study kits and teaching aids, training visits

3) the learning environment

3. At the end of the year, there is a feedback questionnaire, which is included in improving the courses for the next cohorts.

14. Has there been a process evaluation? Who conducted the evaluation (internally or externally?) and what where the main results? (**max. 300 words) -** *for more information on process evaluation, see EUCPN Toolbox No.3, p.9-10 & part 2 - section 2A*

1. Assessing the project happened at the end of each course.
2. More generally, discussions, student feedback questionnaires and lesson observations are used for assessment.
3. At the end of the first year of the programme, the school reached the following conclusions when analysing the progress of the students with the teachers and school leader.
   1) Teaching cannot rely on guest lecturers as had at first been planned. Therefore, the decision was made to send the school's IT head and IT specialist to training courses in order to acquire the necessary knowledge, skills and certificates to teach. In addition, they were encouraged to participate in cyber defence conferences and seminars, which they did.
   2) The UAV (practical mechatronics) course was planned as a semi-extracurricular activity: as a school-organised "interest" course after the lessons. However, this did not work as students were too tired for another 2-3 hours of work after the end of the school day.
   3) In practise, the planned practical learning justified itself. In order to continue high quality practical learning, for example, to buy UAVs and organise transport for training visits, it was decided to seek additional resources from different support measures.
   4) We have done a student feedback questionnaire both in 2016 and 2017.

The second year of the programme confirmed that the school had made the correct decision when restructuring. In addition, it was apparent that students need more time for achieving certain learning outcomes, which is why the MTCNA certificate exam was moved to Year 3.

During this year, (the third year) the school has started renewing and enhancing all the courses based on analysis and feedback. Both the goals and learning outcomes will be specified even more to improve students' understanding of what is required of them. Some changes in structure are also being discussed to make the learning even more effective.

More informally, we have also monitored students' online behaviour and we have seen a decrease in unethical or risky behaviour, for example, accidentally leaving accounts logged in after the end of the lesson.

Finally, we have assessed the reception of the programme outside our school and have found that this is indeed a topic that resonates with both the Ministry of Education and Research, other schools and both governmental and non-governmental institutions. With our help and based on our curriculum, the state has developed an elective cyber defence course that could be used in all schools, not only those who want to teach cyber defence in depth. The Ministry has also asked the school to share its experience as an innovative and important one from the perspective of national defence. A cooperation network has been created with other schools interested in teaching cyber defence, this includes Jõhvi Gymnasium, Elva Gymnasium, Rocca al Mare School, Tartu Tamme Gymnasium, Tartu Jaan Poska Gymnasium, Keila Coeducational Gymnasium.

15. Has there been an outcome or impact evaluation? Who conducted the evaluation (internally or externally?), which data and evaluation method where used and what were the main results? (**Max. 300 words**) *- for more information on outcome or impact evaluation, see EUCPN Toolbox No.3, p.7-9 & part 2 - section 2A*

Assessment of results and impact is done accroding to the following criteria:

1) 95% of the students graduate the cyber defence programme
2) At least 30% of the graduates get the MTCNA certificate
3) The percentage of students who enrol in the cyber defence programme outside Põltsamaa Codeducational Gymnasium
4) The general number of students wanting to study cyber defence increases year by year.
5) At least 90% of students are satisfied with the programme and the way their learning is organised.
6) Every year, at least 3 outside specialists/lectors give seminars. There are at least 2 training visits per year.

By September 2017, the school has the following data:

1) The drop-out rate is nearly zero. Only one student from the 18 in the first cohort has left due to moving to another city. All students were satisfied with the content and how learning was organised. They like the practical approach, training visits and interesting outside lectors. They did not enjoy continuously filling in their lecture notes portfolio.

3) Out of the second cohort, which started in 2016, all 15 students are continuing their studies in the 11th grade. All students were satisfied with the content and how learning was organised. Their likes were identical to the first cohort, but one additional negative aspect was mentioned – double lessons at the end of a school day.

4) In 2017, 23 students enrolled in the third cohort, whereas 20% of them are from outside Põltsamaa.

5) There has been no issues raised by parents of the cyber defence students, the parents are satisfied and supportive (based on classroom meetings).

6) As a result of the analysis, the Information society course was optimised and an integrated syllabus was compiled for fours specific courses, where theretical learning alternates with practical assignments. To improve the safe networking course, a new training visit partner – Santa Monica Networks – was gained.

7) We have instructed all students on the digital footprint and cyber ethics. There has been a noticeable decrease in cyber bullying and intentional or unintentional misuse of computers at school.

## III. The project shall, as far as possible, be innovative, involving new methods or new approaches.

16. How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

This project is innovation at its purest form. In 2015, no other Estonian or European comprehensive school taught cyber defence. It is possible that no other such programme existed in the world. We built the curriculum from the ground up together with our partners.

Several schools in Estonia have contacted Põltsamaa Coeducational Gymnasium to get advice and form partnerships in improving their own IT education. The curriculum was the basis of developing a 35-hour national cyber defence elective course for other schools to include in their elective subjects.

The Ministry of Education and Research awarded the “Deed of the Year in Education” prize to the school in 2016.

## IV. The project shall be based on cooperation between partners, where possible.

18. Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

Estonian Atlantic Treaty Association, Krista Mulenok – key partner, information and training seminars

Estonian Information System Authority, Anto Veldre – lectures and practical seminars

NATO Cooperative Cyber Defence Centre of Excellence, Sven Sakkov, Siim Alatalu – lectures

National Cyber Defense League, Andrus Padar, Kristjan Kaskmann – compiling the syllabi, lectures

The e-Estonia Showroom- training visits

Thor-Sten Vertmann, team member of A. Ansip at the European Commission – Skype lecture on the European digital market.

Erki Kert, CEO at Big Data Scoring - Skype lecture on Big Data

Kristjan Krips, Institute of Information Sciences at the University of Tartu - syllabi consultant, practical programming sessions

National Defence League Jõgeva Unit – purchased the UAV sets (drones) needed for the first cohort.

Rein Põdra, CEO, Center for Communication and Informationsecurity Research and Development – syllabi development; training seminars for teachers; MikroTik Academy license for the school.

Santa Monica Networks – practical learning during the safe networking course

The Ministry of Education and Research - support and encouragement

## V. The project shall be capable of replication in other Member States.

19. How and by whom is the project funded? (**Max. 150 words**)

It is impossible to set up and operate a cyber defence programme without outside help. We have asked many sponsors and partners for help, and have received enough support to start the programme.

Current funding:

The School's budget (see item 20)

Rein Põdra, CEO, Center for Communication and Informationsecurity Research and Development – 2301 € (training seminars for teachers; Mikrotik routers).

National Defence League Jõgeva Unit - 2500 € (for UAV sets for the first cohort).

Sotsiaaldemokraatlik Erakond (The Social Democratic Party of Estonia) - 5000 € (for UAV sets).

Keskerakond (The Central Party of Estonia) - 4000 € (for laptops in the technology classroom).

Kaitseressurisside Amet (Defence Resources Agency) – 9003.36 € (training visits, camps, teaching aides 2016-2017).

European Regional Development Fund and The Republic of Estonia. Project: “Practical technological skills from the Põltsamaa Coeducational Gymnasium mechatronics club” - 19302.58 € (pay for the instructor, teaching aides – UAVs, model airplanes, additional equipment). This sum is for 2017-2020 and we have received 5505.26 € of this.

20. What were the costs of the project in terms of finances, material and human resources? (**Max. 150 words**)

Cost articles covered by the school budget in the first stage (first three years 2015-2018), unless stated differently:

Wages: 4615 € (10th-12th grade in three school years. Altogether 11 courses, 11x355 €, at the moment, the first cohort has had 8. courses, the second cohort has had 4 courses and the third cohort has had 1 course, altogether 13 courses).

Teacher training - 640 € MUM conference in Italy, 300 € MikroTik training seminar, 549 € MTCNA and MTCRE training seminars.

Teaching aides: 5500 € UAVs, 890 € Arduino basic sets, 2175 € Ardunio Robi

“Practical technological skills from the Põltsamaa Coeducational Gymnasium mechatronics club” - cost sharing 3406.34 € (pay for the instructor, teaching aides – UAVs, model airplanes, additional equipment), This sum is for 2017-2020, out of which we have used 971.51 €.

Transport - 3160 € (preparations, cooperation with other education facilities, conferences, training visits)

21. Has a cost-benefit analysis been carried out? If so, describe the analysis, including how and by whom it was carried out and list the main findings of the analysis. (**Max. 150 words**)

Cost analysis done by the school has shown that due to the nature of teaching cyber defence well, the school cannot organise the provision of education in the cyber defence field of study from the school’s own budget. Additional resources are needed for organising training visits for the students, for purchasing teaching aids and study kits, for participating in camps and competitions and for training teachers. Students cannot carry these costs themselves and this has hindered participation in events held outside the school and development of the programme. Teaching cyber defence is a crucial preventative measure of cyber crimes and should be funded at the state level.

22. Are there adjustments to be made to the project to ensure a successful replication in another Member State?

The foundation of the programme is universal – the issues and technology discussed is part of the global digital society.

If another Member State wanted to replicate our cyber defence field of studies at the upper secondary school level, the only major adjustments would be to replace Estonia-specific tasks with what is relevant in their country (the laws, major service providers etc). Some countries may not have as many e-solutions as Estonia, for example. In addition, students may or may not need additional IT courses if the lower levels of education do not provide enough of these.

The other side to consider is partnership with other stakeholders – the state, universities, companies offering their expertise etc.

Securing financing is a key issue as both the material and human resources tend to be more expensive than average in this field.

23. How is the project relevant for other Member States? Please explain the European dimension of your project.

The goal of improving cyber security starting from young people and teaching the next great experts in this field should be common to us all.

In the digital age, issues of online security are crucial for all Member States. Recent developments have shown that the next major threats might be cyber threats in nature. A young person, who feels like "a true professional" in the computer world must know how to function without endangering themselves or others.

Real life shows that cyber defence and behaviour in cyber space as a school subject should be included in all European school curricula as fast as possible. Cyber crime has been on the rise and many of the perpetrators and victims are young people. Socially responsible and lawful behaviour has to be acquired already at the primary level so that they would be ready for more in depth knowledge later in their school years.

What Põltsamaa Coeducational Gymnasium can teach other schools in Europe is to make the teaching of cyber defence and other IT topics as lifelike and practical as possible.

As can be seen form our list of partners, we gained a national and even international dimension very quickly. This kind of project is unthinkable without this type of support.

As said before – we are all facing the threats that our project aims to curtail. As all Member States are connected through both the strengths and weaknesses of giant data communication networks, it is in everyone's best interest to have the best basic knowledge and experts possible.

Please provide a short general description of the project (abstract for inclusion in the conference booklet – **max. 150 words**).

In 2015, Põltsamaa Coeducational Gymnasium, a general education school in Põltsamaa, Estonia, became the first known school in Europe to implement a cyber defence field of studies in the upper secondary school curriculum. The school sees this as a vital innovation in the field of cybersecurity, which has been increasing in importance at an unstoppable rate in the past decades. Estonia and Europe will need both an informed digital society and more and more cybersecurity experts in the future. The aim of the project is to provide students with a more in depth education in cyber hygiene, ethics, relevant hardware and software, national defence and personal protection. In the Estonian cyber security expert career path, the programme is a new stepping stone - one that comes early rather than late. The first stages of the project have shown that the students are ready to take up this challenge. Are the policy-makers?