Annex I

Pre-defined project

Project title:	*Open Cyber Range (OCR)*[1]
Project Promoter:	*Estonian Ministry of Defence*
Project Partner(s):	*Tallinn University of Technology (TalTech), Foundation CR14 (CR14)*
Donor project partner(s):	*Norwegian University of Science and Technology*
Total maximum eligible project cost:	*3 331 765€*
Project grant rate:	*100%*
Project grant amount:	*3 331 765€*
Estimated duration:	*36 months*

Open Cyber Range is a virtual environment that is used for cybersecurity training and cybertechnology development. It provides tools that help strengthen the stability, security and performance of cyberinfrastructures and IT systems leading to secure and trustworthy products and well-educated personnel.

Cyber Ranges function like shooting or kinetic ranges, facilitating training and exercises. Thus, IT professionals employed by various organizations train, develop and test Cyber Range technologies to ensure consistent operations and readiness for real world threats.

Main objectives of this project are to create a platform for (new) cybersecurity companies to develop, test and validate their innovative products, create a launch pad for new products to emerge to the market, promote security thinking in private sector and educate better workforce for the private companies.

The platform will include tools and products that are not part of standard cloud service (automation tools, simulations, red and blue team tools, situational awareness, hybrid systems etc.), thus there is added value to SME-s to develop and test the products in OCR – faster setup of testing and validation environment, reduced initial cost for the environment, community support from academia and government, mentors and test-clients from other SME-s, government and academia etc.

Challenges in the cybersecurity education and training and introducing new technologies:

Challenge 1: Security of ICT products starts from the design of the product, the education of cybersecurity is already incorporated to curricula of computer sciences via different courses like

[1] Refer to the terms and acronyms sections at the end of the document

“Secure Programming Techniques”. However, OCR supports cybersecurity education and training by enabling creation of interactive courses and exercises, where the skill of students can be tested in live environments with monitoring and scoring when needed.

For this OCR solution library will contain learning materials, pre-built environments and ethical hacking tools for both defensive and offensive activities to simulate real life situations. All this can be implemented in a course or a training to provide imminent feedback for the students of their progress, work effectiveness and overall competence in cybersecurity.

This measure will support educating a smarter and security-minded workforce that will contribute to creating sustainable, secure and quality solutions for the industry. Companies and start-ups are encouraged to develop and introduce new content to the education and training curriculum to promote their services for wider audience.

Development of new product and services are not supported by the programme, rather a facility will be provided to SME-s to create, develop, test and validate their products and services.

Target group: industry, universities and other academic institutions.

Challenge 2: Most sophisticated cyberattacks in the world are being conducted against critical information infrastructure (Stuxnet, Energetic Bear etc.), these attacks might cause widespread blackouts, interruptions in water supply, heating and other services that modern world depends on.

Under the OCR project capabilities will be developed to simulate wide range of networks and environments where experts can model and apply different security measures (prepare and prevent), allow red teams (also known as white hat hackers) to penetrate their simulated environments (detect and response) and rehearse their cybersecurity procedures (mitigate, recover and cooperate) to provide comprehensive critical information infrastructure protection. Enterprise own networks can be virtualized and simulated to create more realistic environment.

Concepts like IoT and Industry 4.0 are covered by this challenge, OCR will provide tools and measures to support new technology and companies to emerge that support creating secure and innovative solutions for billions of interconnected devices and production lines.

Target group: critical information infrastructure companies, start-ups

Challenge 3: Academic and industry researchers create vast amount of tools, applications and other pieces of software (artefacts) that need to be experimented, validated and tested throughout their development cycle. OCR will provide a solution library of simulated networks and environments that can be used for these purposes. Also these same artefacts can be later, when they reach enough maturity, added to the solution library for other OCR participants to use and develop.

Organizations can provide expertise of students, researchers, developers and testers through OCR for industry to experiment, validate and test new technologies. Using the new technologies for educational means will give additional feedback to the producer and rises the quality of ICT products.

Also industry partners that provide stress-testing, pen-testing and red team services can be used for assuring security of the newly created technologies. Developing these types of services listed is not part of the project, however using these services on OCR will enable higher efficiency on making sure the products and services developed are better and more secure than their competitors.

Target group: industry, start-ups and academic institutions

Challenge 4: Academic organizations and industry will be able to introduce ready to deploy software and technologies to the OCR solution library that will allow them to rapidly create enterprise environments to pilot and demonstrate the capabilities of their products.

This measure differentiates from the measure 2 as these products will be ready for deployment in production systems and are considered to be mature enough to deploy in activities where the product itself assures the quality of activity, for example the product is used for educational purposes and measuring the skill of a student.

For this measure the OCR participant will build (part of) their enterprise on OCR to evaluate if the product will meet their needs in an enterprise-like environment, e.g. the product is scaling up for the use, is compliant with industry standards or other enterprise specific elements, conditions and requirements.

To achieve this template environments and commonly used artefacts (virtual machines, scripts, scenarios, etc.) will be developed in the project and provided to the OCR users. This enables to rapidly deploy common environments that SME-s need to customize based on their or their customer needs.

Target group: industry and start-ups

Activities to be funded in the project

- First initial operating environment will be created, this includes hardware, software and security equipment to operate the OCR capability, as well as civil works to install and set up the OCR for the next activities;
- Secondly project specific support elements will be developed, this includes specifications for API-s, security and data protection requirements, documentation guidelines, KPIs, OCR collaboration tools, define common scenario language, how hybrid solutions can be added (e.g. 5G, IoT, ICS systems) etc:
- Third activity will be research, development and implementation of the OCR environment, including management system, digital library, simulations, monitoring, scoring and evaluation, feedback module, social aspect module and potential federation with other similar capabilities. This activity includes also security testing of the environment.
- The last activity will provide actual content within the OCR environment for the customers to use and reuse, this includes sample software, virtual machines, attack simulations, scenarios, test environments and other artifacts. Also a testing facility will be created to test, experiment and validate new solutions. Some custom malicious content will be created that can be used in OCR environment.

Expected outcomes and effect on the target group:

- **Expanded capabilities for education and training**, by moving from static class courses to dynamic training and exercises that can simulate the enterprise network. Training capability will be supported by partners for OCR.
- **Innovation**, by allowing industry and academia to share newly created software and tools through Solution Library for fast delivery and testing in OCR community and participants.
- **Better security**, by allowing students and trusted third party pen-testers and red teams to evaluate the solutions used in an enterprise network on a safe environment.
- **Cost effectiveness**, by providing tools and solutions that are not part of traditional enterprise network, like Internet simulation, user simulation, virtual equipment etc and would be otherwise expensive to use.
- **Faster delivery**, by providing pre-packaged, pre-configured and easy-to-deploy tools and software that can be installed in simulated enterprise network.
- **Intensified cooperation**, by binding similar minded users to OCR community that share common goals for better and secure solutions both from developer and user side.

For the first three years the predictions to involve SME-s are moderate (as indicated 15), as the initial operating capability will be achieved in 2020 and first SME-s can be engaged in 2021, but they are able to use just a subset of planned services/capabilities until the full operating capability has been achieved. When more capabilities come online also more SME-s can be engaged to meet their requirements. After the full operating capability has been achieved it is foreseen that up to 10 SME-s could operate simultaneously.

In early 2019 Estonian MoD supported a cybersecurity accelerator CyberNorth[2] that was a joint project between Estonian Defence Industry Association and Estonian private investors to support new start-ups in cybersecurity. Out of this programme 8 start-ups emerged (with their financial body established in Estonia) that would have benefitted from OCR capabilities while developing their products and services.

However, it is noteworthy that not all of these ventures succeed and it is estimated that there is about 50% success rate for start-up companies to survive the first year and find enough customers or investors to keep their business running.

There are no changes planned in the legislation to execute the OCR project, Estonian government has necessary support measures to successfully execute the project, these include ability to agree on cooperation and governance models for OCR, operate an existing support system for emerging companies (Start-Up Estonia), ability to issue special start-up visas for emerging companies etc.

Key performance indicators:

No	Core Indicator Name	Additional description	Indicator (by 2022)
1.	Number of SMEs supported	Number of SMEs supported to test new products/services/processes in the Open Cyber Range	30
2.	Number of new products/technologies developed	New products developed and introduced to the OCR: • cybersecurity training and exercise services (that include developing threat actors, scenarios, indicators, vulnerabilities, custom malware etc. that can be sold separately as a product); • cybersecurity products (that include components of innovative technologies in fields like Industry 4.0, ICS, IoT, 5G, AI and other emerging technology topics) etc. Baselines for these services and products come from different security standards and frameworks, e.g.:	10

[2] https://startupwiseguys.com/cybernorth/

		NICE Cybersecurity Workforce Framework (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework) MITRE ATT&CK Framework (https://attack.mitre.org/wiki/Main_Page) MITRE STIX 2.0 (https://oasis-open.github.io/cti-documentation/stix/intro)	
3.	Number of professional staff trained	Staff that has participated on the cybersecurity trainings and exercises that have been developed in the OCR format.	100

For the OCR project there is no single beneficiary, previous experience has shown that a Cyber Range is a capability that can fully utilized only by very large entities (for example US military), for smaller nations, universities and private sector it is feasible to share a common capability for cost effectiveness and knowledge transfer. Thus a common project promoter is needed who will be responsible for engaging partners, leading the project and promoting the capability. A vast amount of knowledge, procedures and also technology can be transferred from the Estonian Cyber Range for the benefit of the OCR project.

Estonia has operated the Cyber Range since 2012 and altogether about 10M€ has been invested to existing capability, however this capability is now and in the future for government-to-government activities while OCR will be open for wider audience. On the existing Cyber Range world's largest multinational cybersecurity exercises take place – Locked Shields and Cyber Coalition providing training capabilities for more than thousand trainees simultaneously.

The current funding of the Estonian Cyber Range covers the governmental requirements for training and experimentation, however making the capability available for industry and academia requires a dedicated environment with modified toolset to meet their requirements.

The main funding gaps lie in:

1. Creating an underlying physical and logical environment based on the COTS technology that will provide environment for the OCR to operate;
2. Developing both technical and procedural OCR specific concepts, methods, rules of engagements and tools to support resolving the challenges mentioned in the beginning of the document;
3. Researching and developing OCR specific tools e.g. automation of the deployment, providing situational awareness, simulation of user activity and Internet, sanitation and integrity of the environment etc.;
4. Creating sample scenarios, trainings, exercises, test and experimentation environments to support participants introducing their ideas, concepts and products to the OCR and to provide overview of the OCR capabilities;
5. Integration and/or federation with other Cyber Range, Cyber Lab and/or relevant capabilities (non-enterprise environments such as ICS, IoT, medical equipment, legacy systems etc.) from OCR will benefit.

Cooperation between Estonia and Norway

Estonian MoD will be responsible for the execution of the project, while some of the responsibilities of project management will be shared with organizations governed by the MoD, these include Foundation CR14[3] and Estonian Defence Investments Agency[4].

Bilateral dimension is executed in the development of the OCR project while Estonian and Norwegian counterparts conduct common R&D to develop OCR components, develop common tools, promote the capability in both countries etc. NTNU has also involved local municipality to the project to find common interest.

Within the OCR project NTNU will provide the knowledge and experience from operating their academic Cyber Range, also NTNU has specific strengths in cybersecurity disciplines that are not covered on Estonian side, more specifically social aspects, feedback loop and evaluation.

Estonian MoD, TalTech and NTNU had preliminary meetings in May 2018 to define project scope and there are 18 Work Packages defined to be executed in the next three years. In almost all of these Work Packages all participants are included while the lead of the Work Packages will be shared based on the best knowledge of the topic between participants. The content of Work Packages and exact responsibilities shall be reviewed once the project is agreed, overall it is foreseen that the partner costs are divided 50:50 during the project execution.

Estonian MoD and NTNU have signed a Memorandum of Understanding (MoU) in May 2018 regarding co-operation on cyber defence exercises, training, development and research activities and OCR project will be formalized as one of the co-operation activity under this MoU. Dedicated contract (technical agreement) will be signed to define participant responsibilities, work shares, financial aspects etc.

Intellectual Property Rights model considered for this project foresees sharing the intellectual property as much as possible between project partners.

Link to national policies and strategies

Estonia has issued its third cybersecurity strategy[5] in early 2019, among other topics a commitment to develop the OCR platform is described in activity area 2.1 (Supporting and promoting cybersecurity R&D and research-based enterprise), allowing to offer solutions to sectoral (start-up) companies and universities for carrying out R&D activities, testing and products and training.

This is supported by other activities under the support for innovation generation and export potential, but also ensuring an environment conducive to the inception and development of start-ups and leveraging productive cooperation between private sector, state and academia. The OCR project checks out all three priority categories.

In Estonian MoD a cybersecurity policy has been introduced[6] in 2017 that includes Cyber Ranges (National, NATO, Open and Classified) as part of the core capability to support cybersecurity capability development, training and exercises, not just in the governance area of MoD, but nation-wide as this is the only governmental Cyber Range capability operated in Estonia. Also the

[3] Operator of the Cyber Range

[4] Responsible for public tenders in governance area of MoD

[5] https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

[6] In Estonian, currently under review, will be updated by the end of 2020

cybersecurity policy include cybersecurity knowledge transfer and export from MoD to rest of the nation, allies and partners.

MoD’s policy is also to promote Estonian defence industry that includes a cyber-cluster, companies included to this cluster are not defence companies per se, rather they are providing dual-use solutions that the Defence Forces have adopted (for example these include cybersecurity of autonomous vehicles). Same channels can be used to promote SME-s using OCR capabilities once their products and services are mature.

Measures and expected deliverables:

Measure 1 (30%): procure and set up the initial operational capability of the OCR environment based on the COTS products that forms the core of the OCR (computing, storage, networking etc.). This measure will deliver the baseline upon OCR specific research, tools etc. will be applied.

Measure 2 (10%): develop and implement OCR specific requirements such as specifications for APIs, minimal security requirements, requirements for federating technical capabilities, guidelines for documentation, KPIs etc.

Measure 3 (30%): research and develop automation tools for activity deployment, testing capability of the deployed activities, simulation services to support activities, situational awareness tools for different use cases, sanitation technology to clean the OCR between activities, integrity platform to detect unauthorized changes etc.

Measure 4 (10%): populate OCR library with sample software, virtual machines, attack simulations, scenarios, trainings, exercises, test environments and other artefacts, document the use of forenamed items. This is a prerequisite for SMEs to be able to utilize the OCR, an initial set of the library will be populated by the project participants, and however SMEs are encouraged to contribute to this library while using the OCR capability they are not included in the development period of the OCR.

Measure 5 (10%): develop connections and make available additional external capabilities that supplement OCR capabilities and support OCR activities, this is achieved through integration and/or federation of other capabilities, this might include public cloud services for additional computing power, specialized Cyber Ranges/Labs for specific task (ICS, IoT etc.)

Measure 6 (10%): project management costs to cover one full time project manager for the duration of the project and other project management related costs.

Operations and Maintenance:

The initial operations will be supported by the Estonian Ministry of Defence in co-operation with project partners. During the project period when the capability and its operations mature, an operations and maintenance model will be developed to support the capability after the project period, this will include manning, financial provisions etc.

Estonian Ministry of Defence is planning to support the OCR capability with manning throughout and beyond the project lifecycle through the Foundation CR14. To maintain the hardware and software a business model will be created to charge SMEs for the use of capability, this allows also to operate the capability for users that have a sustainable business model themselves. Alternatives include requesting financing from national budget and opening the concept for wider sponsoring model from larger enterprises.

Risk overview:

1. Operational requirements change throughout the implementation of the OCR that leads to difficulty to support requested requirements.
    a. Probability: Likely;
    b. Impact: Moderate;
    c. Response: Contracts with universities will be implemented in a way that allows changing the necessary requirements if needed.
2. Procurements for hardware and/or software fail or will be delayed that leads to difficulty to support requested activities.
    a. Probability: Unlikely;
    b. Impact: Major;
    c. Response: Existing solutions from current Cyber Range capability will be provided in a smaller scale until procurements have succeeded.
3. Universities are not able to deliver requested functionalities for OCR that leads to limited capability.
    a. Probability: Possible;
    b. Impact: Major;
    c. Response: Funding model will be changed to outsource the missing functionalities to industry. This can be achieved while universities find the partners to deliver the functionalities or project promoter will launch a public tender.
4. Lack of interest from industry that leads to underuse of the OCR capability.
    a. Probability: Possible;
    b. Impact: Moderate;
    c. Response: Engage additional entities (Start-up Estonia, start-up accelerators etc.) to promote the capability, promote capability in conferences, meetups, seminars etc. Provide additional operational support from governmental agencies (e.g. datasets that can be used only on OCR to solve specific problems).

Terms and acronyms

Abbreviation	Content
API	Application Programming Interface
Activity	Event conducted on the OCR, this includes trainings, exercises, testing, evaluation, validation and other similar activities.
Artefact	By-products produced during the development of software, trainings, exercises etc., e.g., use cases, class diagrams, and other Unified Modelling Language models, requirements and design documents
COTS	Commercial-Off-The-Shelf
ICS	Industrial Control System
ICT	Information and communications technology
IoT	Internet-of-Things
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
Library	An environment to store, document and make available items used in OCR

Abbreviation	Content
OCR	Open Cyber Range
SME	Small and medium-sized enterprises