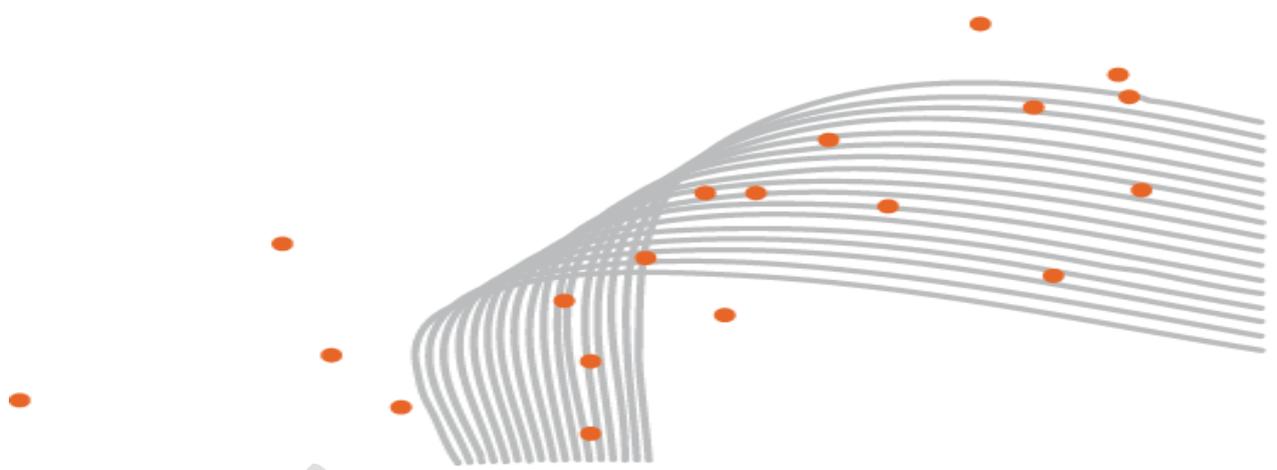




DINNOCAP

**Action Plan: Transnational Industry Dialogue and
policy support**



Contributors:

Torben Aaberg, Knud Erik Skouby, Anders Henten, Reza Tadayoni, Morten Falch, Henning Olesen and Idongesit Williams

Disclaimer: This report is delivered by the DINNOCAP project, an EU Interreg BSR financed project. The information presented in this study does not represent the views of either the EU commission or EU Interreg BSR. The contents of the report are extracted and analyzed from output reports produced in the DINNOCAP project.

Table of contents

Introduction	4
Proposed List of actions	6
Theme 1: Financial support for SME digitalisation	6
Challenges	6
Project activity	7
Observations	7
Ideas/proposals	8
Theme 2: Cyber Security and SMEs	8
Challenges	8
Project activities	9
Observations	10
Ideas/proposed actions	10
Survey: Cyber security threats and measures	10
Scope/content	10
Observations	11
Ideas/proposed actions	11
Theme 3: 5G technologies and SMEs	11
Challenges	11
Project activities	12
Observations	12
Ideas/proposed actions:	12
Theme 4: Artificial Intelligence (AI) and SMEs	13
Challenges	13

Project activities	13
Observations	14
Ideas/proposed actions	15
Proposed Policy Actions	16
Proposed policies for Funding SME digitalisation	16
Proposed policies for SMEs and cyber security	16
Proposed policies for SMEs and 5G	16
Proposed policies for SMs and Artificial Intelligence	16

Introduction

One of the objectives of the DINNOCAP project is to propose policy recommendations pertaining to challenges pertaining to access to finance, access to workforce, access to knowledge, infrastructure challenges and awareness raising. These policy proposals are concretized as lists of concrete actions necessary to solve the aforementioned challenges.

These aforementioned challenges were identified in the DIGINNO project (www.diginnoobsr.eu), of which DINNOCAP is an extension. These challenges were documented in the Business Needs Analysis and the SME Digital awareness toolkit produced in DIGINNO. In the DIGINNO policy white paper, which was the final output of the project, policy proposals for solving some of these challenges were outlined.

The policy proposals proposed in the DIGINNO white paper were generic policy proposals for which policymakers in each EU member state could derive action points necessary to promote SME digitisation for their SMEs. In DINNOCAP, the project partnership went one step further to propose concrete action points for policy makers. The action points are produced in partnership with SMEs and industry associations within and outside the partnership.

These were thematic webinars organised by Aalborg University on access to finance, cybersecurity, 5G, Artificial Intelligence (AI). A separate webinar on access to Knowledge and workforce was planned but cancelled due to practical circumstances. It was substituted by a workshop for dissemination to/knowledge exchange with European Digital Innovation Hubs (EDIH's) regarding digital assessment methods organised by Research Institute of Sweden (RISE). The participants in the webinars on access to finance, cybersecurity, 5G, and artificial intelligence were SMEs and industry associations in the BSR. The webinars on infrastructure were those on cybersecurity, 5G and AI.

In addition to the seminar on Cybersecurity, a survey was conducted to identify the cybersecurity challenges encountered by SMEs. The full report is available on the DINNOCAP website¹. This report also produced action points that supplement those gathered from SMEs and industry associations in the cybersecurity seminar.

The action points and proposed policy actions for these action points produced from the webinars and survey are presented in this report. This report is of value to policy makers involved in either facilitating and/or supporting SME digitization in their respective member states.

Proposed List of actions

To provide clarity on each list of actions, the problems (challenges), how DINNOCAP dealt with the problem (project activity), the observations from stakeholders (observations) are outlined. This provides context to the list of actions as well as provides the reader with insight into the minds of the stakeholders. The list of actions are presented based on the thematic seminars that produced them.

Theme 1: Financial support for SME digitalisation

Challenges

In general, financing digital transformation is seen as an issue for SMEs in all BSR countries

SME digital transformation is mainly financed by bank loans; bank loans can be quite heavy and the loans do not necessarily support costs associated with change, e.g. change of IT systems

All BSR countries have financial instruments for SME digitalisation. But public support is mostly based on annual budgets. That means the availability of grants can be unforeseeable which complicates long term planning for SMEs

¹ https://www.dinnocapbsr.eu/_files/ugd/8cf6e6_eda0c48874ce43bc942cc6f09fe5c87d.pdf

Lack of venture capital (VC) is an issue in the BSR, in particular the Eastern BSR. Also it is not likely that this situation will change in the short term as VC loans are mainly associated with hardware industries which are not common in the BSR countries. Therefore special attention must be given to existing financing instruments like bank loans and public sector grants.

There does not seem to be much coordination of funding opportunities across the countries. Legislative and transnational policies are not coherent, which impedes on the ability of SMEs to operate across borders.

Project activity

One thematic seminar has been organised as an online event with the title: *“Financial support for industry digitalisation: Challenges, plans and expectations”*. The aim was to give an idea of the situation in different partner countries and discuss commonalities in the BSR regarding access to funding ICT uptake in SMEs.

The seminar included:

- A focus on the new EU funds for recovering the economy (RRF) to give an idea about the national ambitions and intentions regarding funding SME digitalisation. Examples from Finland, Latvia and Lithuania were presented to exemplify how different countries are planning to utilise RRF funds regarding digital transformation of SMEs. Also a preliminary overview of trends in all national plans submitted to the EU by the time of the event had been circulated by organisers before the seminar.
- Sharing of information on what are the supportive actions and funding possibilities in the countries for digitalization in the post-crisis period.
- Discussion of the general outlook in the countries regarding challenges and opportunities for financing and investing in industry digitalisation

Observations

The landscape is rather diversified with rather huge variations between the countries regarding prioritised sectors and themes.

According to RRF rules min 20 pct of planned expenditures must be related to “digital transition”. However, the digitising industry is not necessarily in focus and SMEs even less.

Direct investments in SME digitalisation is generally not an intention. The planned digital transition investments will generally be based on development and implementation of broad digital strategies or road

maps. A broad spectrum of digitisation initiatives will be supported, e.g. digital innovation hubs, digital security, digital infrastructure, new technologies, innovation vouchers.

The funding will often be based on seed money with up to 50 pct co-financing demand where the aim is to catalyse existing funds and multiply the impact.

In one country all RFF funds are foreseen to be spent in public sector digitalisation, including open data, infrastructure development and digital public administration. A more efficient public sector – as well as public investments/procurement - can indirectly benefit SME digitalisation and improve framework conditions. Nevertheless, easy and non-bureaucratic access to funding of the first steps into digitalisation is often crucial for SMEs opportunities.

It varies from country to country how much industry representatives have been involved in the development of the national plan. Transnationally coordinated reactions from industry associations in the different countries could have been useful for drawing attention towards the needs of SMEs.

By Nov 2021 the European Commission (EC) has assessed the majority of the national RFF plans. Assessment-rating "A" has been given to all assessed plans regarding the criteria "Digital transition", A meaning "criterion met to a large extent". It seems that support to digital transformation of SMEs has not been explicitly assessed as 'support to small and medium-sized enterprises' is not sector-specific².

Ideas/proposals

- Funding schemes coordinated across borders should be given higher priority. Legislative and transnational policies should be more coherent. For example macro-regional, inter-ministerial coordination of national initiatives and instruments for financing ICT uptake in SMEs, including bilateral and multilateral funding that can make SMEs in the BSR more competitive.
- Open national and regional support structures and activities for SMEs operating in other countries and regions, provided that they collaborate with local companies.

² <https://www.bruegel.org/publications/datasets/european-union-countries-recovery-and-resilience-plans/>

Theme 2: Cyber Security and SMEs

Challenges

One of the main challenges in digitization of SMEs is how to deal with cyber security (CS) issues. Larger companies have specialised resources to deal with CS. They also know how to comply with regulation and laws on how to handle end users'/customers' data in a proper manner. Most SMEs, however, do not have such resources and in most cases lack the competency to deal with the issues.

There are many stories of intruders that have hacked company systems and data with severe consequences for the businesses, e.g. financial costs in case of ransomwares, waste of time in cases of Denial of Service (DOS) attacks and loss of company data when Brute-force attacks. In many cases, due to security issues and suboptimal processes in the companies, customer data is dealt with wrongly, resulting in compromised data protection and privacy regulations. This may have severe implications for the digitization process in SMEs and can be seen as a barrier for ICT uptake.

Project activities

One thematic seminar, *"Cyber Security and SME's in a Transnational Context"* has been organized as an online event, in collaboration with the project "COM-3" co-funded by Interreg EU North Sea programme, <https://northsearegion.eu/com-3/>. The aim was to provide project partners and other industry associations with knowledge and inspiration for how to raise awareness and encourage SMEs to take up Cyber Security (CS) technologies.

The seminar included:

- Exploration of how knowledge derived from user-oriented research can be used by SMEs to adopt new technologies in the area.
- Exploration of aspects of challenges in and solutions to cyber security in SMEs.
- Exchange of best practices, knowledge and inspiration for how to raise awareness and encourage SMEs to take up cyber security technologies.

Discussion points were:

- Why worry about cyber security? What happens if you don't?

- How can SMEs utilise knowledge in CS technologies?
- Have adequate solutions been developed that can inspire neighbouring countries?
- How to make cyber security a competitive advantage?
- How to raise awareness and promote solutions among SMEs?
- Any transnational solutions/actions to develop and take further?

Observations

- CS is an issue for SMEs, not only big companies are attacked.
- Many micro-companies are not aware that they need CS.
- It is important for SMEs to know the risk, to have competent staff to handle it and shape the organisation needed to handle risks.
- Access to knowledge is crucial. Expertise as well as general knowledge/awareness among employees.

Ideas/proposed actions

- Exchange (at the practical level) of information and best practice, e.g. on what kind of awareness raising activities are useful, which technical tools are efficient, what kind of data is needed.
- Illustrative cases are useful and important, also from neighbouring countries.
- A clearly explained policy for CS will strengthen competitive advantages for SMEs taking up the issue.
- Increase public investment in CS initiatives directed towards SMEs.
- Encourage cross-border collaboration with a focus on tracking down cyber criminals targeting SMEs.
- Further develop knowledge sharing initiatives aimed at creating awareness and solutions on cyber crime to SMEs.
- Harmonise national SME policies with joint indicators to monitor the state of readiness of SMEs to meet cyber attacks.

Survey: Cyber security threats and measures

Scope/content

A survey was conducted by Aalborg University (a DINNOCAP partner) to explore and characterise the challenges and problems for SMEs in relation to cyber security. 25 SMEs from Russia (Kaliningrad), Estonia, Latvia, Poland and Lithuania participated in the survey. Feedback from these SMEs were analysed and

compared with similar data from a similar survey conducted by the Danish Business Authority and Eurostat. The observations and list of actions derived from the analysis of the survey is presented in this section.

Observations

With the increased take-up of ICT-based solutions in industry activities generally, discussions on cyber security have developed. It seems obvious that with more ICT-based activity, cyber security must become a bigger concern. Within the project this was reflected in an online seminar on 16 Sept. 2021 on 'Cyber security and SMEs in a transnational context'. Inspired by the seminar, a project report on cyber security challenges in the BSR was developed based on EU reports, Danish national material and a survey on the cyber security situation in partner countries. The report recommends a number of actions to be taken to meet the challenges.

Ideas/proposed actions

- Create awareness raising programmes targeting SMEs and based mainly on illustrative examples on problems and solutions. The programmes should be:
 - o integrated into the activities of EDIHs
 - o promoted by sector regulators such as business registers, and
 - o promoted by industry associations Developments of training programmes resulting in a pool of experts able to assist SMEs in the region
- Develop certified, 'automated' procedures that SMEs can implement for typical/ common activities.
- Provide financial incentives to develop cyber security infrastructure in SMEs – e.g., via EU projects
- Incorporate the NIST Cybersecurity Framework into the e-delivery standards developed as building blocks by CEF (Connecting Europe Facility) such as eID, EBSI, CEF. When SMEs adopt these building blocks, they can automatically consider and also implement the cyber security framework as well.
- Industry associations should adopt tools that enable SMEs to measure and upgrade their cybersecurity readiness.
- Industry associations should guide SMEs to understand how to take advantage of the cybersecurity financing and technical possibilities developed by ENISA.

Theme 3: 5G technologies and SMEs

Challenges

5G is changing the communications landscape and will have a transformative effect on the companies' work processes and development of products and services in the future.

The equipment and telecom industry provide different showcases and solutions for larger companies on how 5G will enable digitalization of the companies and enable more efficient processes. Larger companies often have access to in-house competencies to utilise the potentials of 5G technologies on their own. It is, however, less clear how SMEs can get advantages of 5G in their internal work processes and development of products and services.

Project activities

One thematic seminar has been organised as an online event, under the title: *"The value of 5G technologies for SMEs"*.

The aims were to

- Explore and exchange knowledge and best practice
- Give examples of why and how SMEs can use 5G in their business
- Inspire how to raise awareness and encourage SMEs to prepare for upcoming 5G technologies

The seminar included these discussion points:

- How can 5G technologies become an enabler for SME digitalisation?
- What are the inspiring use cases and success stories?
- Are there any transnational learnings to take forward in the Baltic Sea Region?

Observations

- There is a huge unexplored business potential for SMEs in 5G.
- There is a need to build 5G-based ecosystems where SMEs can enter new value chains.
- SMEs do not necessarily understand what added value they can get and what role they can play in the ecosystems.
- Some big companies run their own 5G networks, using their own technologies. But it is not always clear how SMEs can get access to this knowledge and technologies.

Ideas/proposed actions:

- New 5G-based ecosystems should be built and existing 5G-based ecosystems should be open for SMEs to enter new value chains.
- It would help SMEs to enter the ecosystems if they understand and accept what role they can play; they should be encouraged and guided by demonstration and dialogue.
- Therefore, telling the good stories (use cases) is important. But they must be accompanied by advice and guidance on how to apply to the specific situation of the individual SME; this is where the industry associations can play an active role as guides and intermediaries.
- Cross-border test beds, e.g. covering several BSR countries, could be a way to share and provide knowledge in this area directed towards SMEs.
- Some of the DIH's (Digital Innovation Hubs) have taken up 5G in their support to SMEs; the upcoming European platforms (E-DIH's) could take it further and connect existing test beds, starting with exchange of experience.
- The Latvian "5G Techritory" initiative could be a model for BSR that brings together key players, aiming at developing "a robust and aligned 5G ecosystem in Europe and beyond".

Theme 4: Artificial Intelligence (AI) and SMEs

Challenges

- With the application of Machine Learning and new AI tools, AI will in the coming years be an increasingly important technology area to implement in various business activities. The rudimentary statistics that already exist in the field of AI use in industries clearly show that SMEs are lagging behind.
- The transformation challenges caused by implementation and adoption of AI to existing forms of organisation and management practice has, to a large extent, been left untouched by research, by consulting firms, and by policy initiatives.
- Especially processes related to management of professional knowledge workers using AI solutions and the drawbacks in the capacity of both management and employees in SMEs to properly understand the potentials and limitations of AI need to be addressed both in research, in consulting and in policy initiatives and regulations.
- Adding the perspective of different industries and firm size with a focus on SMEs only makes it clear that more practical knowledge to guide the AI transition process is needed.

Project activities

One thematic seminar has been organised as an online event, under the title: 'Artificial Intelligence in SMEs'.

The aims were to.

- Explore existing knowledge and practice.
- Give examples of why and how SMEs can use AI.
- Inspire how to raise awareness and encourage SMEs to prepare for upcoming AI technologies.

Observations

Applications by industries

- The utilisation of artificial intelligence is most widely used in information and communication industries followed by business services and manufacturing; the use is smallest in building and construction.
- Information and communication industries are using AI, among other things, for marketing, business process management, management, IT security and HR.
- The industrial sector makes the most use of AI software and systems for production processes, while trade and transport make use of artificial intelligence for logistics.
- For those companies that work with artificial intelligence, automation of workflows using, for example, software robots for process automation, is the most frequently used AI-solution.
- Next, the most used AI tools are machine learning for data analysis and AI that can analyse text.
- Autonomous robots are most widespread in the manufacturing industry, while all other AI technologies are most widespread in the information and communication sector.
- Software-based AI is most often used to support management for example in the form of business intelligence, business forecasts and risk assessment.
- The second most common application is related to IT security, for instance approval of users by face recognition or prevention of cyber-attacks.
- Virtual assistants, automated scheduling, or translation is the third most widely used application.

AI and new competences

- Companies in many lines of business are already and will continue to invest in AI which will require redesign of workflows, jobs, and work organisation to take full advantage of the potentially increased agility and to free up resources for other more value-creating tasks.
- Thus, AI demands new competency requirements for both employees and managers.
- A recent Danish analysis, using big data from online job postings for AI positions in DK, indicates an increasing demand for a new type of labor: knowledge mediators and integrators.
- Thus, not only an increased demand for advanced STEM competency, but also context-dependent knowledge of customers behaviour, public regulations, and management decision-making processes.

Ideas/proposed actions

- Although some forms of AI are already relatively widespread – especially in larger companies – there is still a need for awareness raising from industry organisations and from public authorities with respect to the economic and growth potentials when implementing AI solutions in production, administration, decision-making and marketing.
- This applies especially for SMEs, as many SMEs will not in their daily work have the surplus time and energy to examine the potentials in AI.
- There are immediate gains to be reaped in making production, transportation and administration more efficient, however, there are also important advantages to be established in the decision-making and marketing activities when data on customers are being processed using AI tools.
- The gains with respect to customer contact and improved information on customers does not only relate to increasing sales but also to improved innovation processes; innovations are often sparked by the customer encounter, and AI can help systematise the potentially innovative ideas which come from customer encounters. Most digital customer interfaces used currently are ‘stupid’ and the information derived from such interfaces are difficult to use for any innovation purposes.
- Research on AI has hitherto concentrated on the technical development of AI systems and lately also on the ethical issues related to the algorithms and data used in AI. Such research trends are clearly important and should be enhanced. However, research on the organisational aspects and on the needed competence profiles of employees and management should be upgraded.
- The need for knowledge and initiatives regarding organisational implications and competence profiles should be reflected in public research programs as well as activities by industry organisations.

- The need for new competence profiles should also be reflected in educational programs. A recent Danish survey has documented the need not only for traditional STEM profiles of educations and the resulting candidates but also for competences regarding knowledge integration and mediation requiring integration of STEM and SSH competences.
- Companies need to be aware of the many ethical issues that the algorithms and data raise; campaigns to increase this awareness are needed, including privacy concerns, but should be balanced not to scare companies away from making use of AI solutions that are ethically and politically acceptable.

Proposed Policy Actions

In order to implement the lists of action, national policy makers responsible for digitalisation (government agencies) should convert the action points into national and where necessary cross-border policies. Cross-border policies could be forged either bilaterally or multilaterally between member states. The thought pattern should be on:

1. *How can policy support these lists of action?*
2. *Identifying the new policy initiatives in the pipeline that can address the issues (challenges) raised?*
3. *Identifying opportunities for developing a structured dialogue with industry partners to identify SME needs in e.g. awareness raising? etc. for further list of actions and policy measures.*

In the project, the following policy proposals were extracted from the list of actions proposed by SMEs and Industry associations in the project.

Proposed policies for Funding SME digitalisation

- Funding schemes should be coordinated across borders. Legislative and transnational policies should be more coherent. For example macro-regional, inter-ministerial coordination of national initiatives and instruments for financing ICT uptake in SMEs, including bilateral and multilateral funding that can make SMEs in the BSR more competitive
- Open national and regional support structures and activities for SMEs operating in other countries and regions, provided that they collaborate with local companies.

Proposed policies for SMEs and cyber security

- A clearly explained policy for cyber security will be a competitive advantage.
- Public investment into cyber security initiatives by SMEs.
- Cross-border collaboration tracking down cyber criminals targeting SMEs
- Knowledge sharing initiatives aimed at creating awareness and solutions on cyber crime to SMEs.
- Harmonisation of national SME policies with joint indicators to monitor the state of readiness of SMEs to meet cyber attacks.

Proposed policies for SMEs and 5G

- Telling the good stories (use cases) is part of it but must be accompanied by advice on how to apply to the situation of the individual SME; this is where the industry associations can play a role
- Cross-border test beds, e.g. covering several BSR countries, could be a way to share and provide competences
- Some of the DIH's (Digital Innovation Hubs) have taken up 5G in their support to SMEs; the upcoming European platforms (E-DIH's) could take it further and connect existing test beds, starting with exchange of experience
- The Latvian "5G Techritory" could be a model for BSR that brings together key players, aiming at developing "a robust and aligned 5G ecosystem in Europe and beyond"

Proposed policies for SMEs and Artificial Intelligence

- awareness raising from industry organisations and from public authorities with respect to the economic and growth potentials when implementing AI solutions in production, administration, decision-making and marketing
- The need for knowledge and initiatives regarding organisational implications and competence profiles should be reflected in public research programs as well as activities by industry organisations
- The need for new competence profiles should also be reflected in educational programs

