

A decorative geometric pattern covers the left side of the slide. It features a repeating grid of hexagons in shades of orange, yellow, and blue, with some hexagons containing white diagonal lines.

# Building digital competences in national and regional clusters

FIIF event on "Digital Trust and Security"

14.2.2019

Jarno Salonen



# Agenda

**Background**

**Building competences in national clusters via FISC**

**Building competences in regional clusters via NECC**

**Building competences within the EU via ECSO**

**Other initiatives**

**Conclusion**



# Background

## “Europe faces a shortage of 350,000 IT security staff by 2022” (6.6.2017)

- *Benchmarking Workforce Capacity and Response to Cyber Risk*, released from the 2017 Global Information Security Workforce Study

## “Cryptominers have impacted 55% of organizations globally” (15.1.2018)

- *Check Point, 2018* (<https://blog.checkpoint.com/2018/01/15/decembers-wanted-malware-crypto-miners-affect-55-businesses-worldwide/>)

## “Cyber-defenders should be paying attention to new threats in 2019 such as: 1) Exploiting AI-generated fake video and audio, 2) Poisoning AI defenses, 3) Hacking smart contracts, 4) Breaking encryption using quantum computers, 5) Attacking from the computing cloud”

- *Five emerging cyber-threats to worry about in 2019, January 2019* (<https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/>)

## Current “high-level” competence market in Finland

- 15 000 graduates from higher education per annum
- 1 700 Doctoral graduates per annum

- *Onko huippuosajille Suomessa töitä? Ylen aamu-tv | TV | Areena, 13.2.2019* (<https://areena.yle.fi/1-50072755>)



## Background

ITU-T Global Cybersecurity Index ranks countries according to the following five pillars:

- 1. Legal**  
(legislation, regulation, **training**)
- 2. Technical**  
(CIRT's, standards and certification, online protection)
- 3. Organizational**  
(policy coordination and national strategies)
- 4. Capacity Building**  
(**R&D, education and training programmes + certification**)
- 5. Cooperation**  
(**partnerships, cooperative frameworks and information sharing**)

Country	Score	Global Rank
<i>Singapore</i>	<i>0,925</i>	<i>1</i>
<i>USA</i>	<i>0,919</i>	<i>2</i>
<i>Malaysia</i>	<i>0,893</i>	<i>3</i>
<i>Estonia</i>	<i>0,846</i>	<i>5</i>
<i>France</i>	<i>0,819</i>	<i>8</i>
<i>Norway</i>	<i>0,786</i>	<i>11</i>
<i>Finland</i>	<i>0,741</i>	<i>16</i>
<i>Sweden</i>	<i>0,733</i>	<i>17</i>
<i>Latvia</i>	<i>0,688</i>	<i>21</i>
<i>Denmark</i>	<i>0,617</i>	<i>34</i>
<i>Lithuania</i>	<i>0,504</i>	<i>56</i>
<i>Iceland</i>	<i>0,384</i>	<i>77</i>

Source: ITU-T GCI Report 2017



# Finnish Information Security Cluster (FISC)

Association established: 2012

Purpose of the association:

*To improve cybersecurity and support its member organizations' activities in the following areas:*

- *increase cross-border activities,*
- *promote public-private-partnerships,*
- *conduct market surveys,*
- *enable national depth and width of high-level education*
- *dialogue with national and international regulatory bodies*

Currently more than 80 member organisations



<https://www.fisc.fi/>



# North European Cybersecurity Cluster (NECC)

Association established: 2018

Purpose of the association:

*Promote issues in the field of information security and cybersecurity in the Nordic region.*

Since its establishment, NECC has received more interested partners from the original countries and Iceland. Since this is a cluster of clusters, the number of member organisations is difficult to determine





# European Cyber Security Organization (ECSO)

Association established: 2016

Purpose of the association:

*Support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity, and in particular to:*

- *Foster and protect from cyber threats the growth of the European Digital Single Market;*
- *Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position;*
- *Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.*

*ECSO has currently about 240 members*





## Other initiatives

- European Cybersecurity Industrial, Technology & Research Competence Centre & Network of National Coordination Centres along with a large, open and diverse Competence Community
- H2020 call SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap
  - Total of four projects (CONCORDIA, SPARTA, ECHO, CyberSec4Europe) lasting for four years with a budget of 16M€ each
- Digital Trust Business Finland programme (to be published during this spring)
- Cross-European collaboration started by Pole d'Excellence Cyber, Bretagne France





## Conclusion

### Everything seems to be ok...

- We have the necessary knowhow for building competences in Digital Trust and Security
- There are many national, regional and even European-wide initiatives to support competence-building

### ...so why aren't we proceeding with the development?

- Lack of resources to group companies together with universities and other research organisations
- Lack of coordination especially in the national level



A brighter future is created  
through science-based innovations.



[www.vttresearch.com](http://www.vttresearch.com)  
[#vttpeople / @VTTFinland](https://twitter.com/VTTFinland)

