Cybersecurity Research as an Instrument for Value Creation.

Challenges and opportunities for the Norwegian industry

Vasileios Gkioulos, PhD

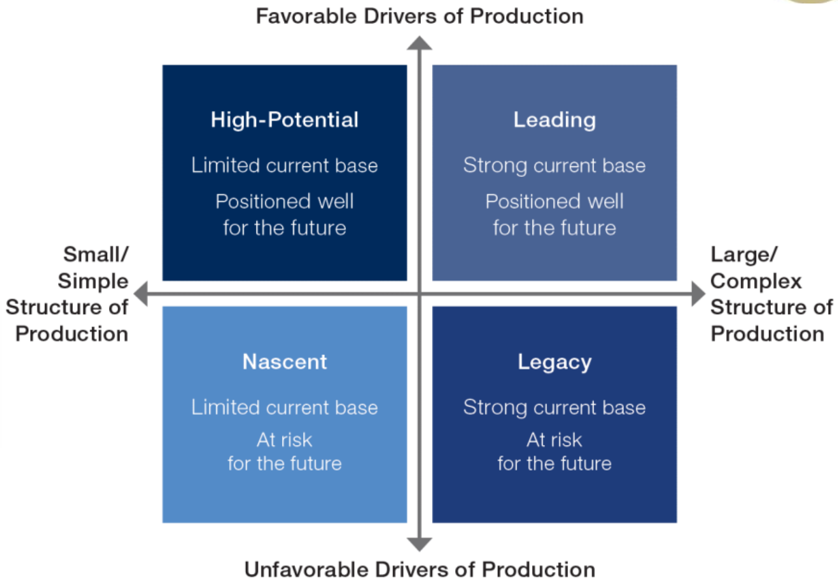
NTNU Associate Professor in secure systems engineering

DNV Senior cybersecurity consultant in OT security management

Norway at the Macro-level

Norway at the Macro-level

- **Readiness for the Future of Production Report 2018**
- Analyses how well positioned 100 countries are today to shape and benefit from the changing nature of production in the future.



Favorable Drivers of Production

High-Potential
Limited current base
Positioned well for the future

Leading
Strong current base
Positioned well for the future

Small/ Simple Structure of Production

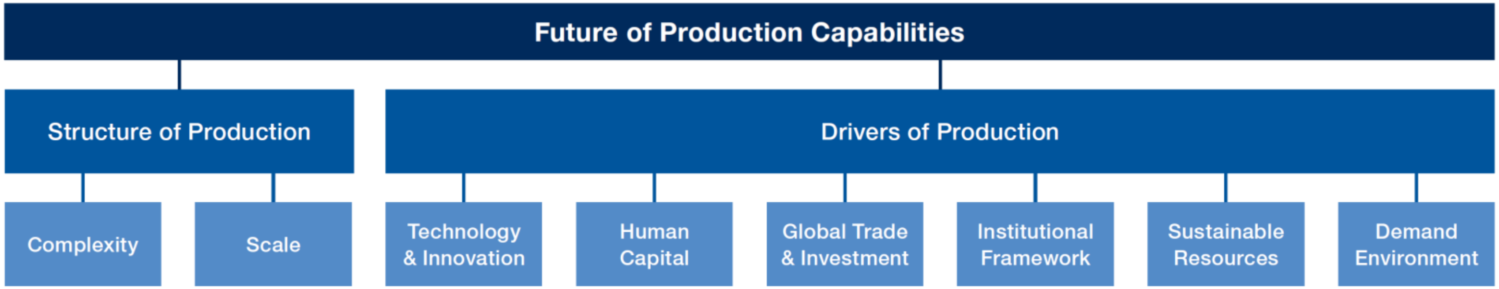
Large/ Complex Structure of Production

Nascent
Limited current base
At risk for the future

Legacy
Strong current base
At risk for the future

Unfavorable Drivers of Production

WORLD ECONOMIC FORUM

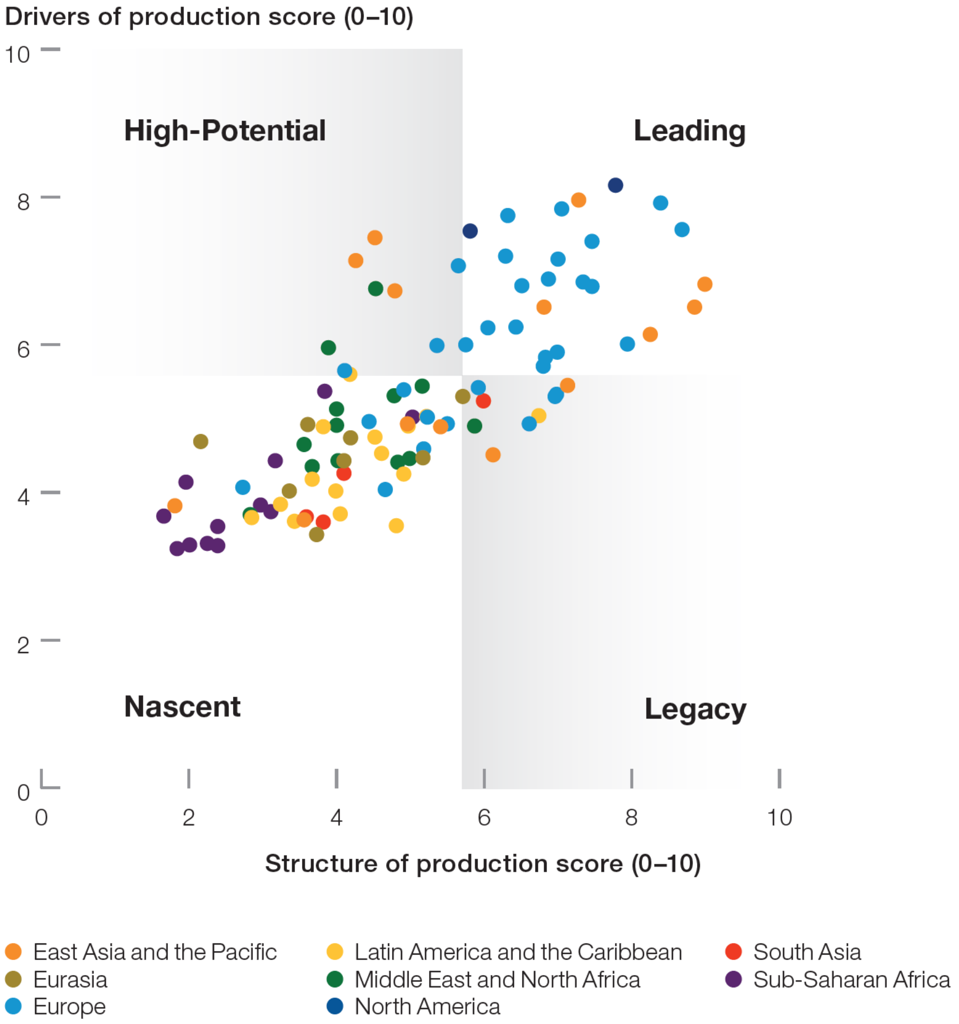


Future of Production Capabilities

Structure of Production
- Complexity
- Scale

Drivers of Production
- Technology & Innovation
- Human Capital
- Global Trade & Investment
- Institutional Framework
- Sustainable Resources
- Demand Environment

Norway at the Macro-level



Note: Average performance of the top 75 countries is at the intersection of the four quadrants.

Norway at the Macro-level

Readiness Overall Assessment

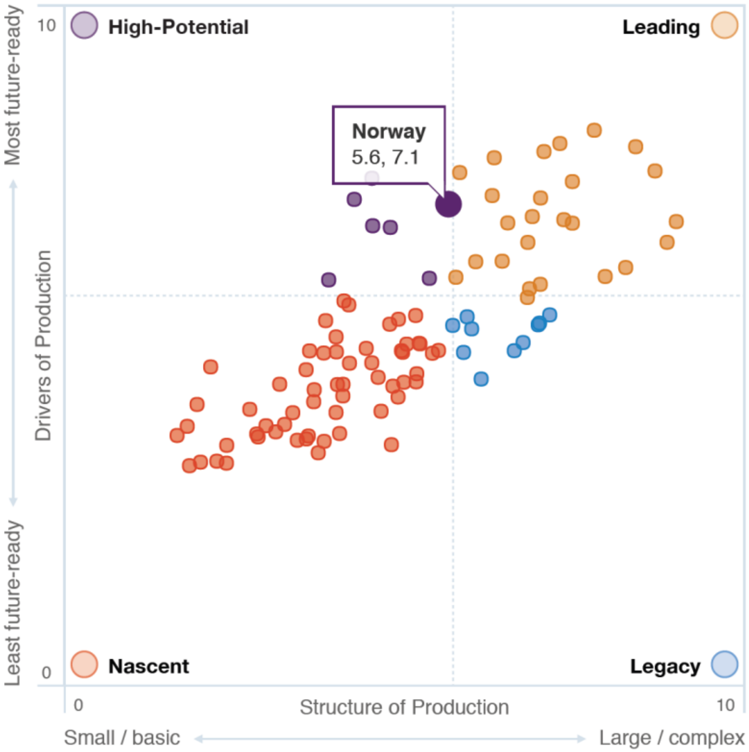
Drivers of Production 7.1

Driver	Weighting	Rank	Score /10
Technology & Innovation	20%	13th	6.9
Human Capital	20%	5th	7.8
Global Trade & Investment	20%	38th	5.7
Institutional Framework	20%	7th	8.7
Sustainable Resources	5%	1st	8.8
Demand Environment	15%	32nd	5.5

Structure of Production 5.6

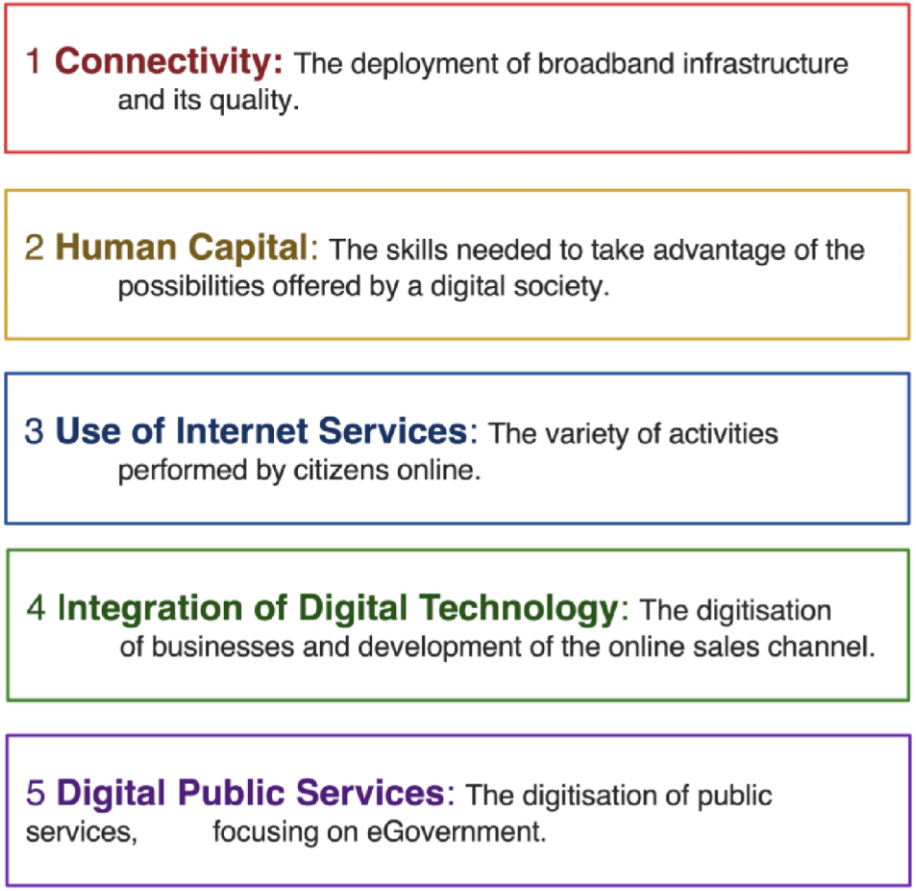
Structure	Weighting	Rank	Score /10
Complexity	60%	26th	7.1
Scale	40%	67th	3.5

Archetype



Norway at the Macro-level

- **The International Digital Economy and Society Index (I-DESI)**



1 **Connectivity:** The deployment of broadband infrastructure and its quality.

2 **Human Capital**: The skills needed to take advantage of the possibilities offered by a digital society.

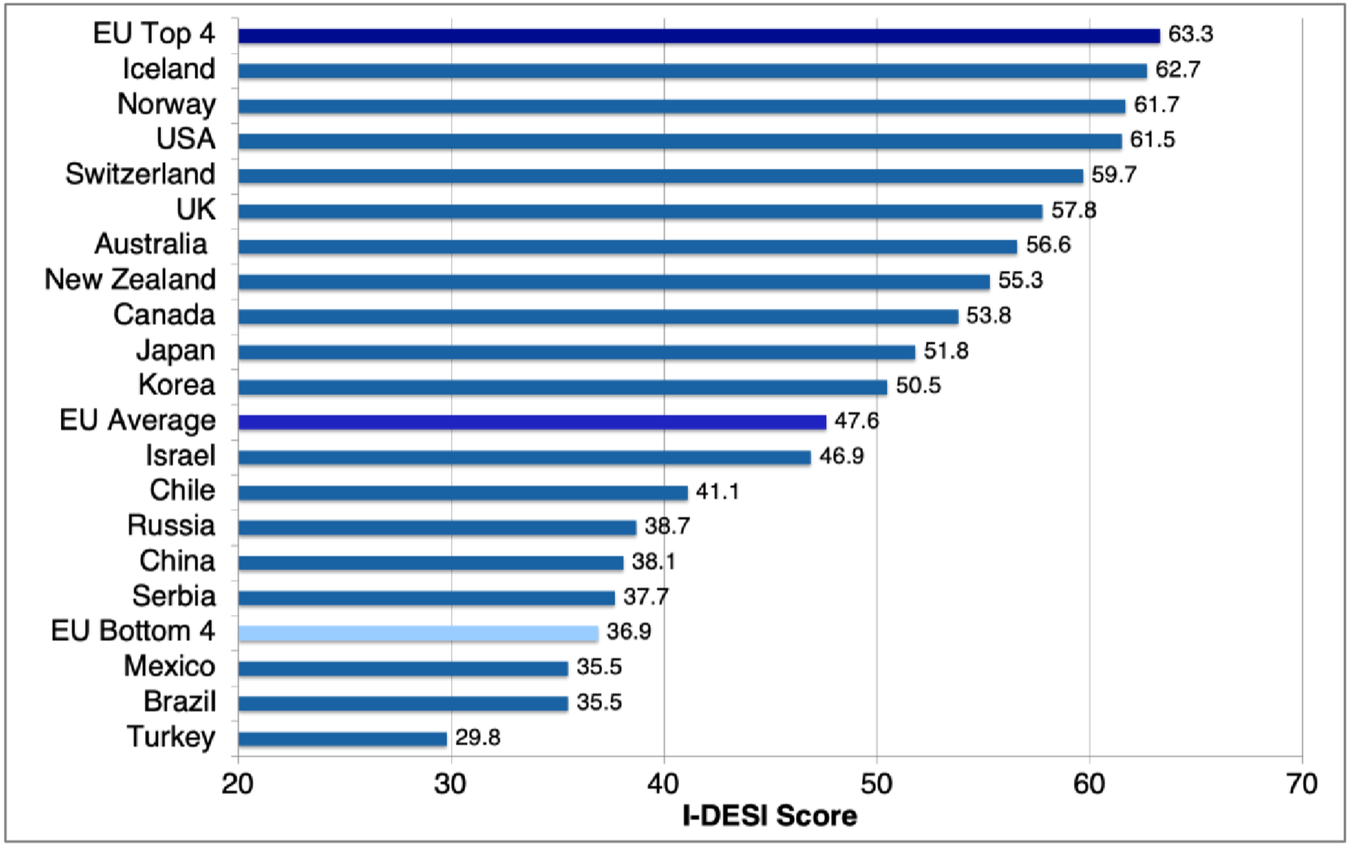
3 **Use of Internet Services**: The variety of activities performed by citizens online.

4 **Integration of Digital Technology**: The digitisation of businesses and development of the online sales channel.

5 **Digital Public Services**: The digitisation of public services, focusing on eGovernment.

Norway at the Macro-level

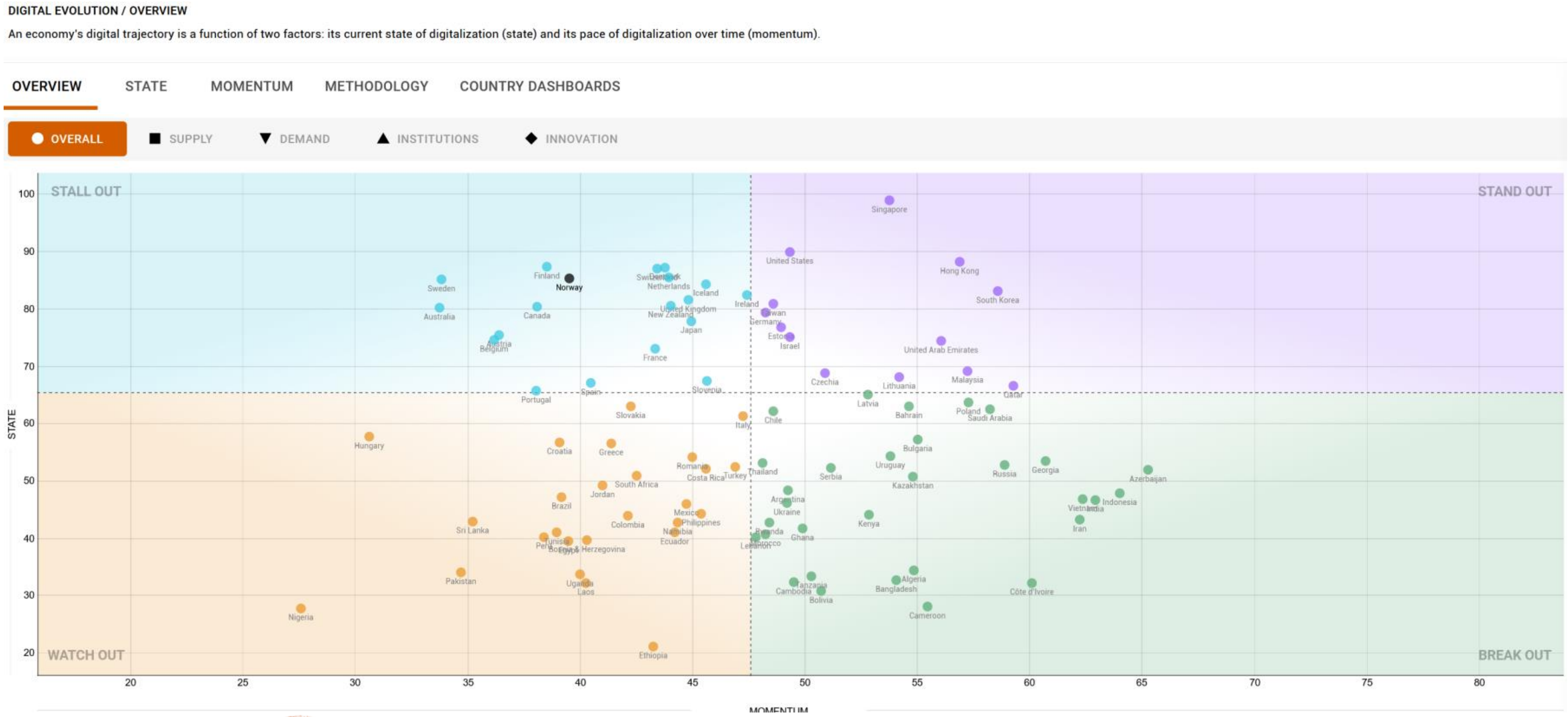
- **The International Digital Economy and Society Index (I-DESI)**



Non-EU countries normalised performance scores for I-DESI

Norway at the Macro-level

- Digital Intelligence Index (DII)
- Combines 160 indicators into four key drivers.



DIGITAL EVOLUTION / OVERVIEW

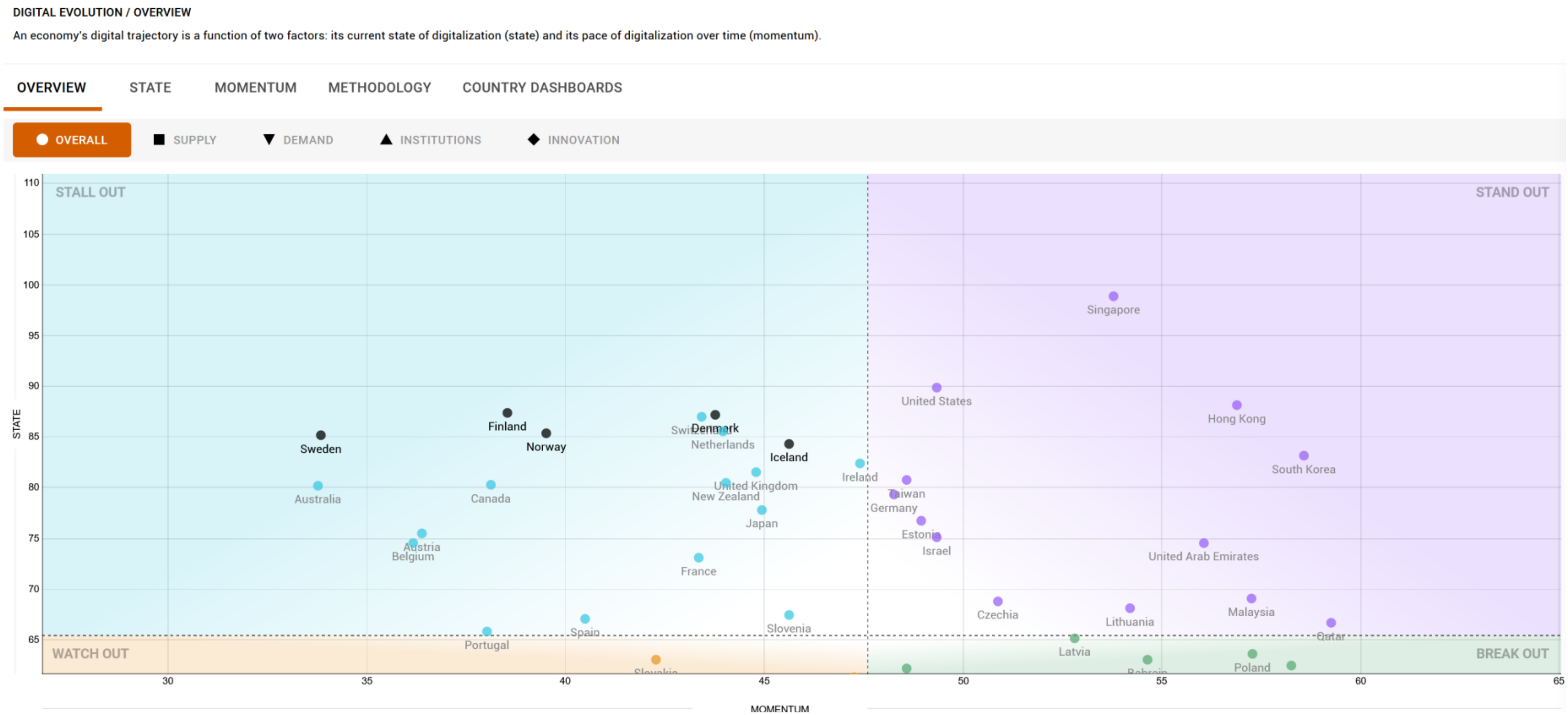
An economy's digital trajectory is a function of two factors: its current state of digitalization (state) and its pace of digitalization over time (momentum).

Digital Planet
Where Digital Innovation Meets the World

THE FLETCHER SCHOOL
TUFTS UNIVERSITY

Norway at the Macro-level

- Digital Intelligence Index (DII)



DIGITAL EVOLUTION / OVERVIEW

An economy's digital trajectory is a function of two factors: its current state of digitalization (state) and its pace of digitalization over time (momentum).

Digital Planet
Where Digital Innovation Meets the World

The Fletcher School
Tufts University

Global strategies

Europe's Digital Compass

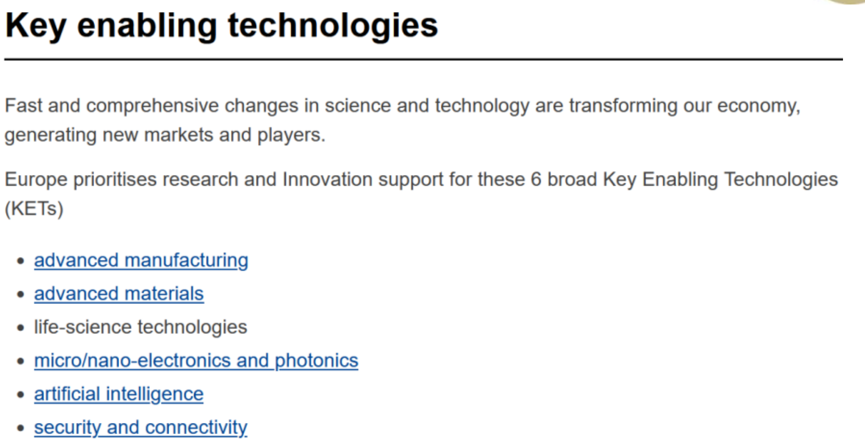
The Commission proposes a **Digital Compass** to translate the EU's digital ambitions for 2030 into concrete terms. They evolve around four cardinal points:

1) **Digitally skilled citizens and highly skilled digital professionals**; By 2030, at least 80% of all adults should have basic digital skills, and there should be 20 million employed ICT specialists in the EU – while more women should take up such jobs;

2) **Secure, performant and sustainable digital infrastructures**; By 2030, all EU households should have gigabit connectivity and all populated areas should be covered by 5G; the production of cutting-edge and sustainable semiconductors in Europe should be 20% of world production; 10,000 climate neutral highly secure edge nodes should be deployed in the EU; and Europe should have its first quantum computer;

3) **Digital transformation of businesses**; By 2030, three out of four companies should use cloud computing services, big data and Artificial Intelligence; more than 90% SMEs should reach at least basic level of digital intensity; and the number of EU unicorns should double;

4) **Digitalisation of public services**; By 2030, all key public services should be available online; all citizens will have access to their e-medical records; and 80% citizens should use an eID solution.



Key enabling technologies

Fast and comprehensive changes in science and technology are transforming our economy, generating new markets and players.

Europe prioritises research and Innovation support for these 6 broad Key Enabling Technologies (KETs)

- advanced manufacturing
- advanced materials
- life-science technologies
- micro/nano-electronics and photonics
- artificial intelligence
- security and connectivity

Advanced Technologies for Industry (ATI)

1. Advanced Manufacturing Technology
2. Advanced Materials
3. Artificial Intelligence
4. Augmented and Virtual Reality
5. Big Data
6. Blockchain
7. Cloud Computing
8. Connectivity
9. Industrial Biotechnology
10. Internet of Things
11. Micro- and Nanoelectronics
12. Mobility
13. Nanotechnology
14. Photonics
15. Robotics
16. Security

European Commission

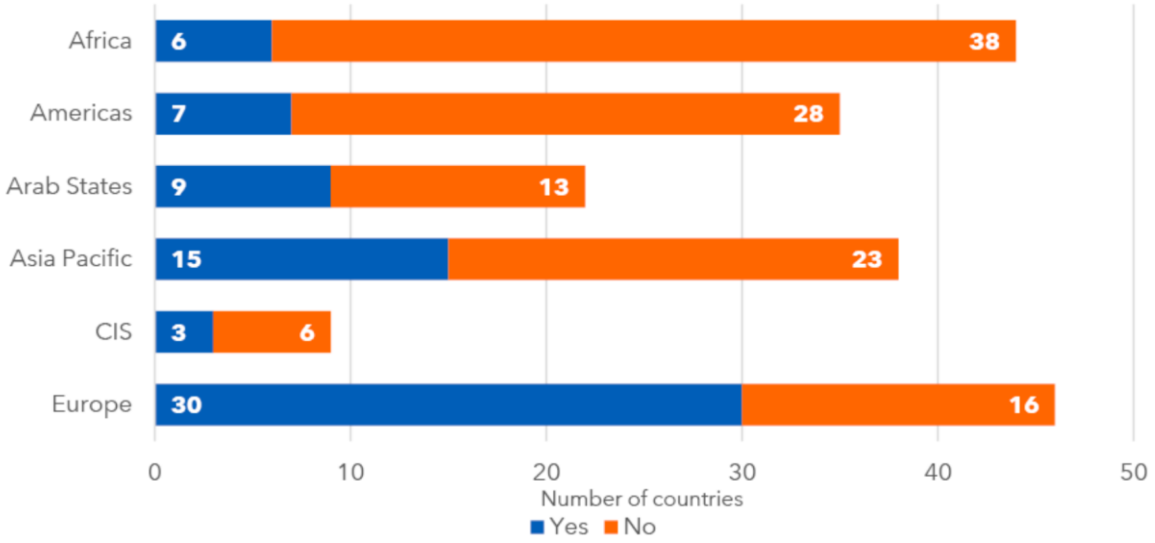
Global strategies

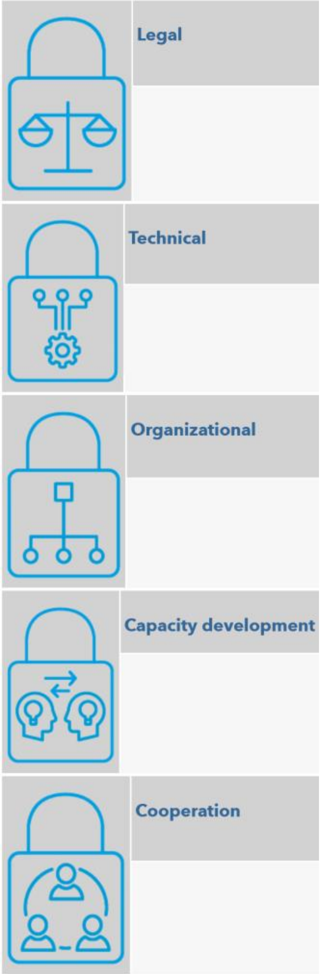
Government incentives for cybersecurity development lags behind

Countries can promote cybersecurity adoption in the private sector through incentive mechanisms, such as tax incentives based on cybersecurity parameters, tax holidays, or including cybersecurity standards as part contracts. These will encourage private sector actors to prioritize cybersecurity within operational structures and processes, in turn improving a country's cybersecurity posture in the short-, medium-, and long-term.

However, this edition of the GCI shows that 124 countries did not provide any cybersecurity incentives, reflecting the need for Member States to adopt such incentives to fast track cybersecurity measures.

Figure 21: Number of countries with a cybersecurity capacity development incentive mechanism





Legal

Technical

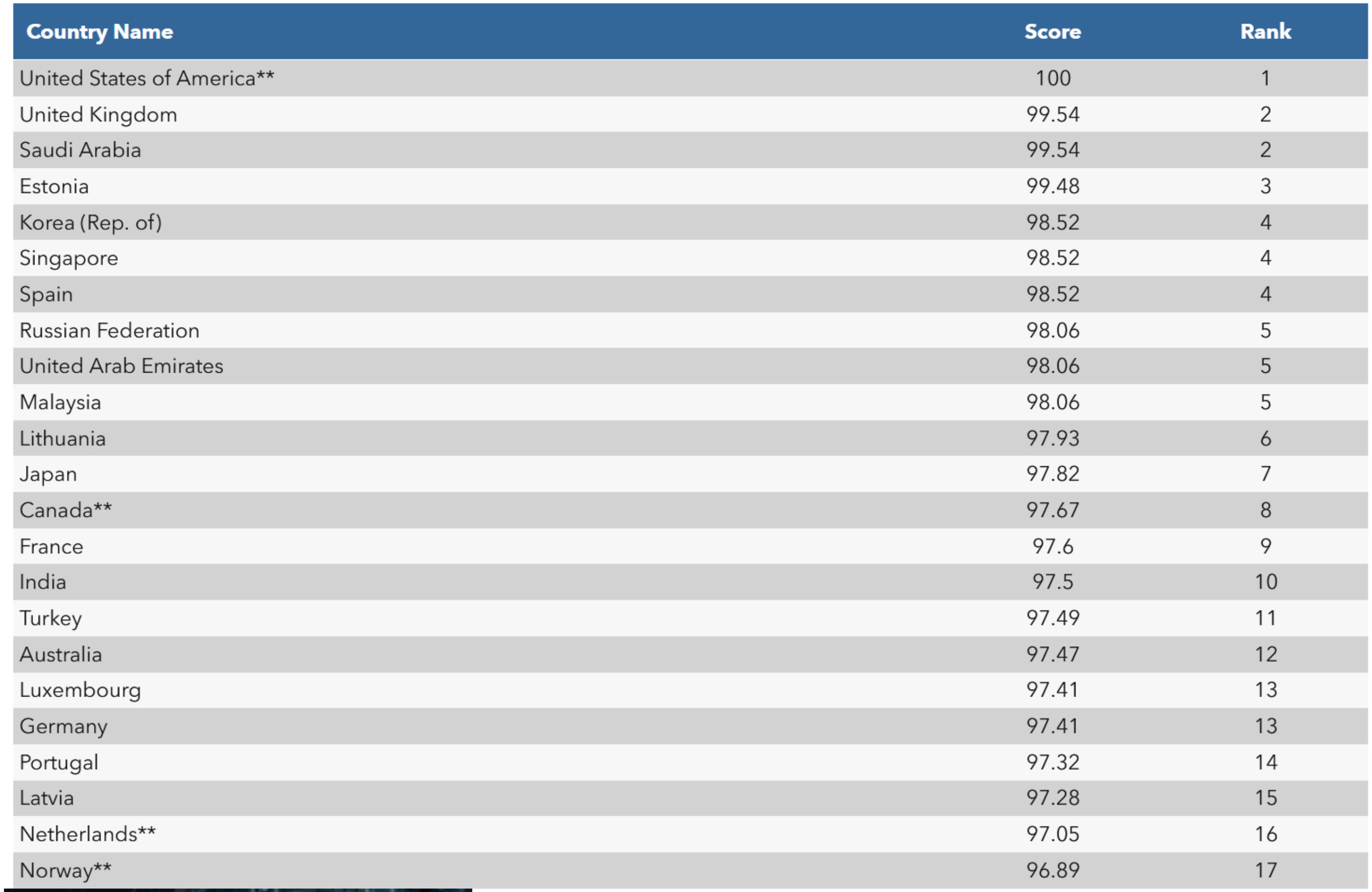
Organizational

Capacity development

Cooperation

Global strategies

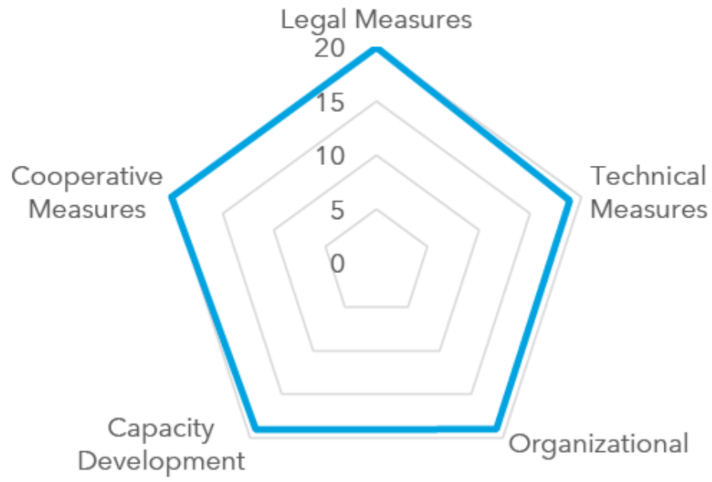
Table 3: GCI results: Global score and rank



Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15
Netherlands**	97.05	16
Norway**	96.89	17

Norway at the Macro-level

Norway**



Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures, Cooperative Measures

Area(s) of Potential Growth
Capacity Development, Technical, Legal Measures

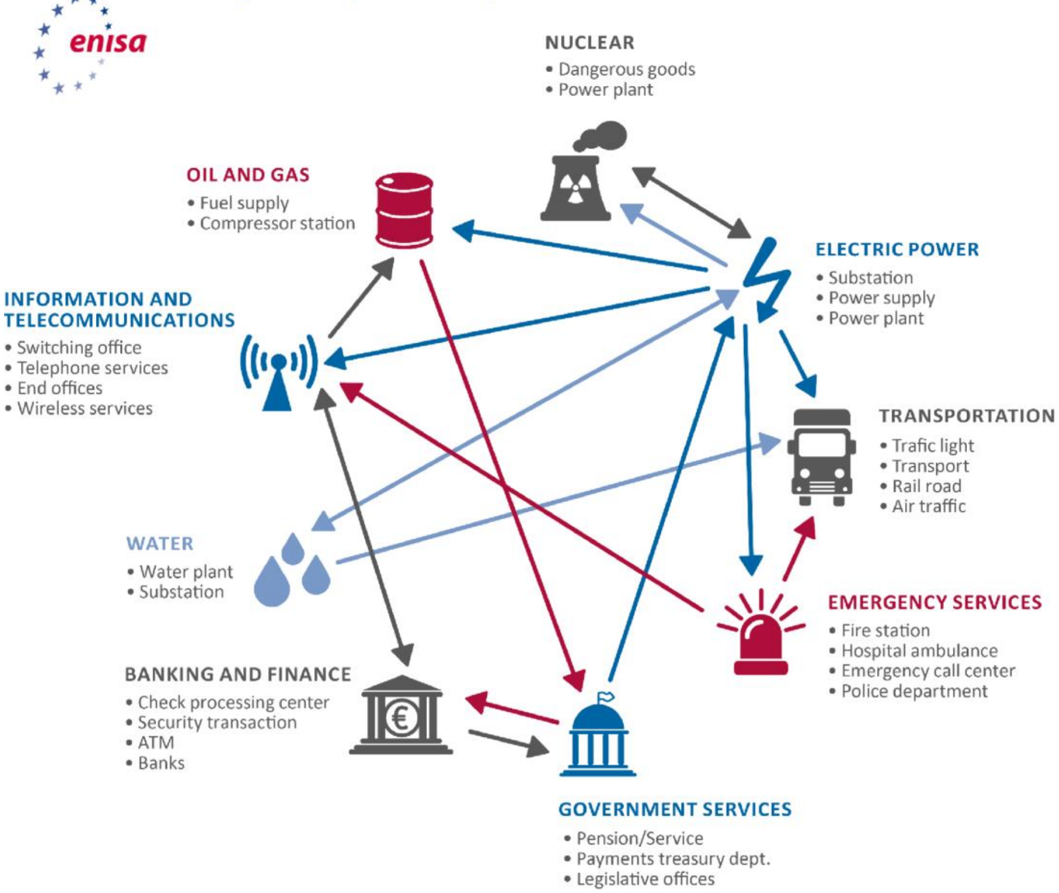
Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.89	20.00	18.86	18.98	19.04	20.00

Source: ITU Global Cybersecurity Index v4, 2021

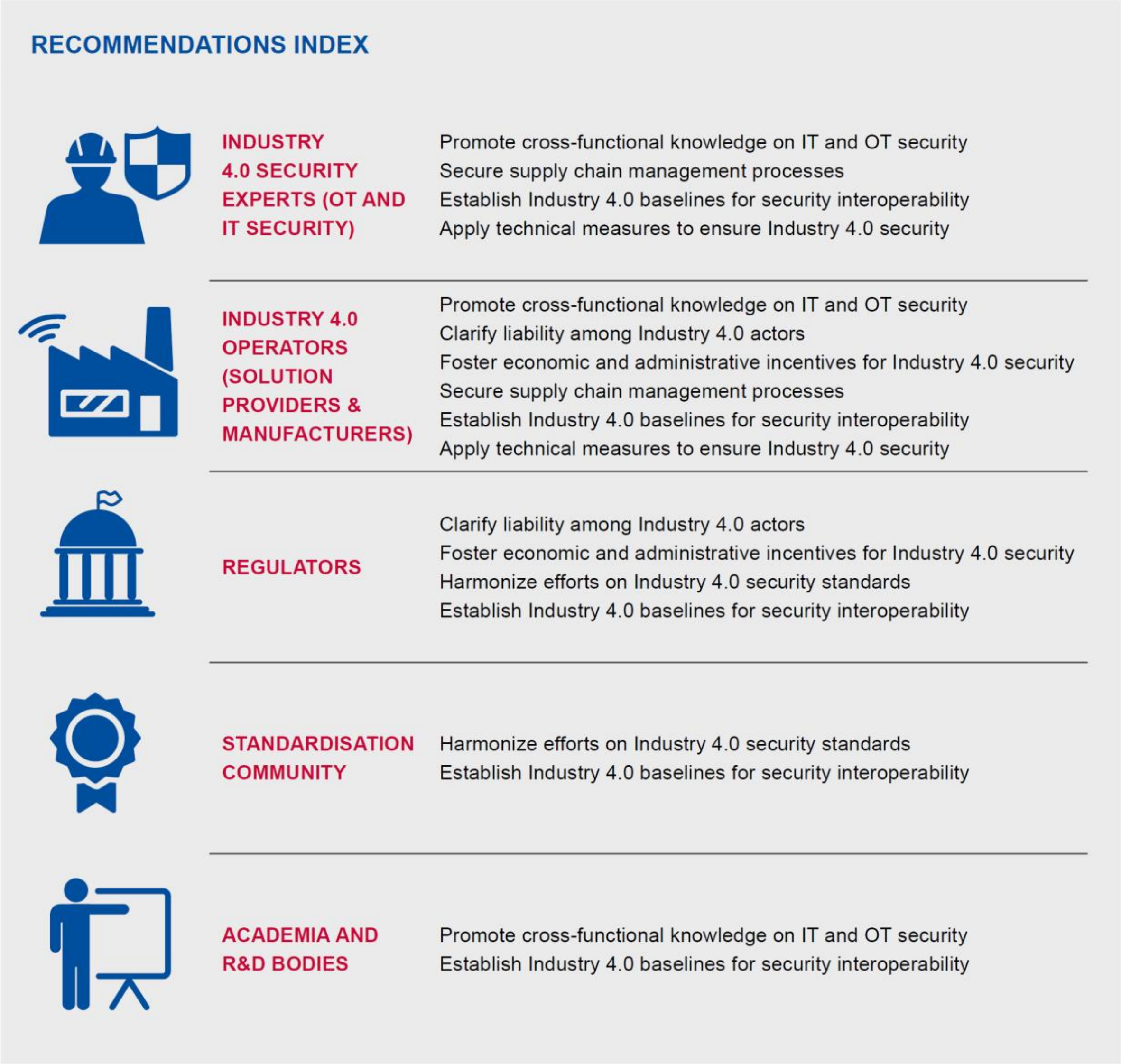
Why? At the Micro-level

- Regulatory and compliance requirements
- Impact of security incidents

Figure 5: Concept of the interdependencies of each Critical Infrastructure.



What?



RECOMMENDATIONS INDEX

INDUSTRY 4.0 SECURITY EXPERTS (OT AND IT SECURITY)	Promote cross-functional knowledge on IT and OT security Secure supply chain management processes Establish Industry 4.0 baselines for security interoperability Apply technical measures to ensure Industry 4.0 security
INDUSTRY 4.0 OPERATORS (SOLUTION PROVIDERS & MANUFACTURERS)	Promote cross-functional knowledge on IT and OT security Clarify liability among Industry 4.0 actors Foster economic and administrative incentives for Industry 4.0 security Secure supply chain management processes Establish Industry 4.0 baselines for security interoperability Apply technical measures to ensure Industry 4.0 security
REGULATORS	Clarify liability among Industry 4.0 actors Foster economic and administrative incentives for Industry 4.0 security Harmonize efforts on Industry 4.0 security standards Establish Industry 4.0 baselines for security interoperability
STANDARDISATION COMMUNITY	Harmonize efforts on Industry 4.0 security standards Establish Industry 4.0 baselines for security interoperability
ACADEMIA AND R&D BODIES	Promote cross-functional knowledge on IT and OT security Establish Industry 4.0 baselines for security interoperability

NORCICS

SFI Norwegian Centre for
Cybersecurity in Critical
Sectors

SFI NORCICS: Addressing cybersecurity challenges when integrating IT and OT

Professor Sokratis Katsikas (sokratis.katsikas@ntnu.no)

https://www.ntnu.edu/norcics

NTNU | Norwegian University of
Science and Technology

The SFI scheme - NFR

- The Centers for Research-based Innovation are to develop expertise in fields of importance for **innovation** and **value creation**.
- Through **long-term research** conducted in close collaboration between **research-performing companies** and **prominent research groups**, the SFI centers are to enhance **technology transfer, internationalization** and **researcher training**.
- The scientific merit of the research must be of **high international caliber**.

NORCICS - Facts

- The only NFR-funded center on cybersecurity
- Started: 01.10.2020
- Funding for 5(+3) years
- Total budget: 215,643,000 NOK
- Funding: 96,000,000 NOK NFR (44.5%)
- Coordinator (NTNU) + 18 partners (4 research, 14 user)
- Sectors represented: Energy, Manufacturing, Oil & Gas, Security, Healthcare, Police, Process industry, Defense

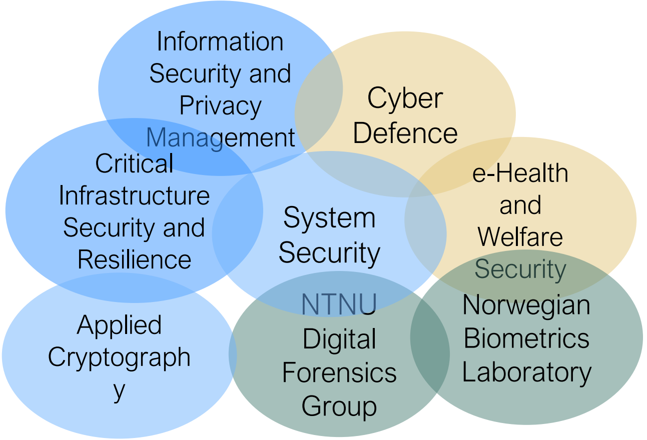
NORCICS – Vision

- Norway is among the world's most digitized societies.
- **NORCICS's vision** is to contribute to making Norway the most securely digitalized country in the world, by improving the cyber security and resilience of its critical sectors, through supporting research-based innovation.

Objectives

- **Create new knowledge** to improve our understanding of the dynamics and interdependencies among Critical Sectors; and of cyberattacks against CPS.
- **Develop, test, validate, and demonstrate** novel, advanced and innovative **methods** for preventing **cyberattacks against industrial control systems** in Critical Sectors.
- **Develop** novel methods and tools for **cyber security training and awareness improvement.**
- **Transfer the knowledge** created within NORCICS among its user partners and other Norwegian businesses and stakeholders.

Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS


Information Security and Privacy Management

Cyber Defence

Critical Infrastructure Security and Resilience

System Security

e-Health and Welfare Security

Applied Cryptograph y

NTNU Digital Forensics Group

Norwegian Biometrics Laboratory

Michigan Tech

UF IoT

UNIVERSITY of GUELPH

POLYTECHNIQUE MONTRÉAL UNIVERSITÉ D'INGÉNIERIE

TUHH Technische Universität Hamburg

Technical University of Munich TUM

TELECOM SudParis

IP PARIS

ma

SINGAPORE UNI TECHNOLOGY A

جامعة نيويورك أبوظبي NYU ABU DHABI

UNIVERSITÄT PASSAU

DTU Technical University of Denmark

SIEMENS

HELGELAND KRAFT

YARA

Lyse

POLITIET OSLO POLITIDISTRIKT

NTNU

equinor

Elvia

mnemonic Securing your business.

NorSIS Norsk senter for informasjonssikring

UiA Universitetet i Agder

Hydro

Sykehuset Innlandet HF

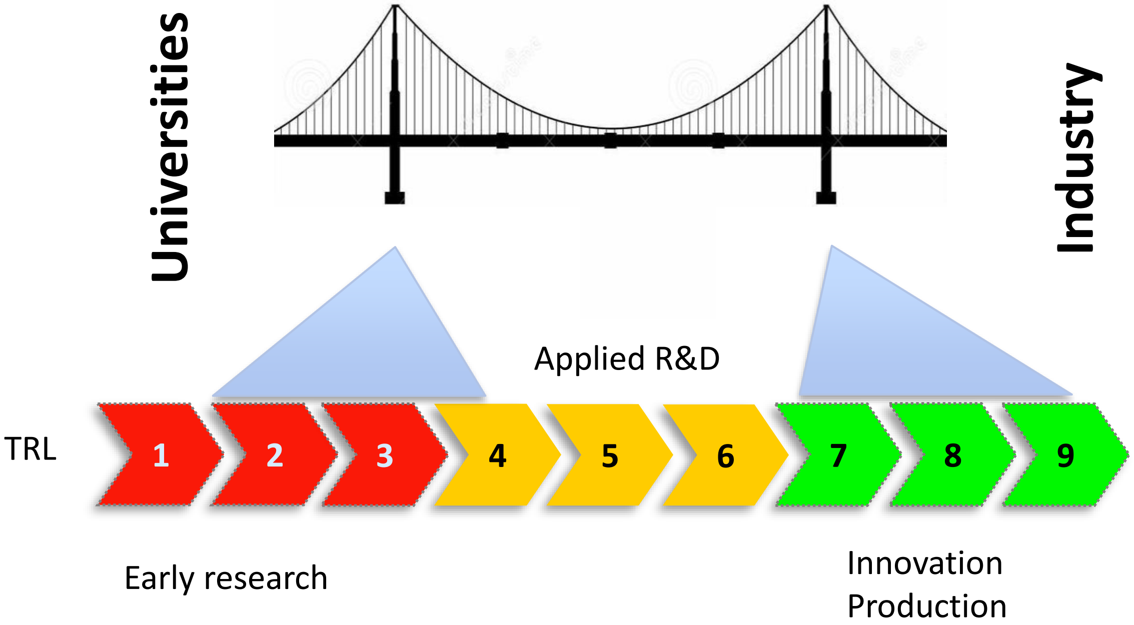
SINTEF

NR Norsk Regnesentral NORWEGIAN COMPUTING CENTER

KONGSBERG

NC-SPECTRUM

How to bridge the Valley of death?



Universities

Industry

Applied R&D

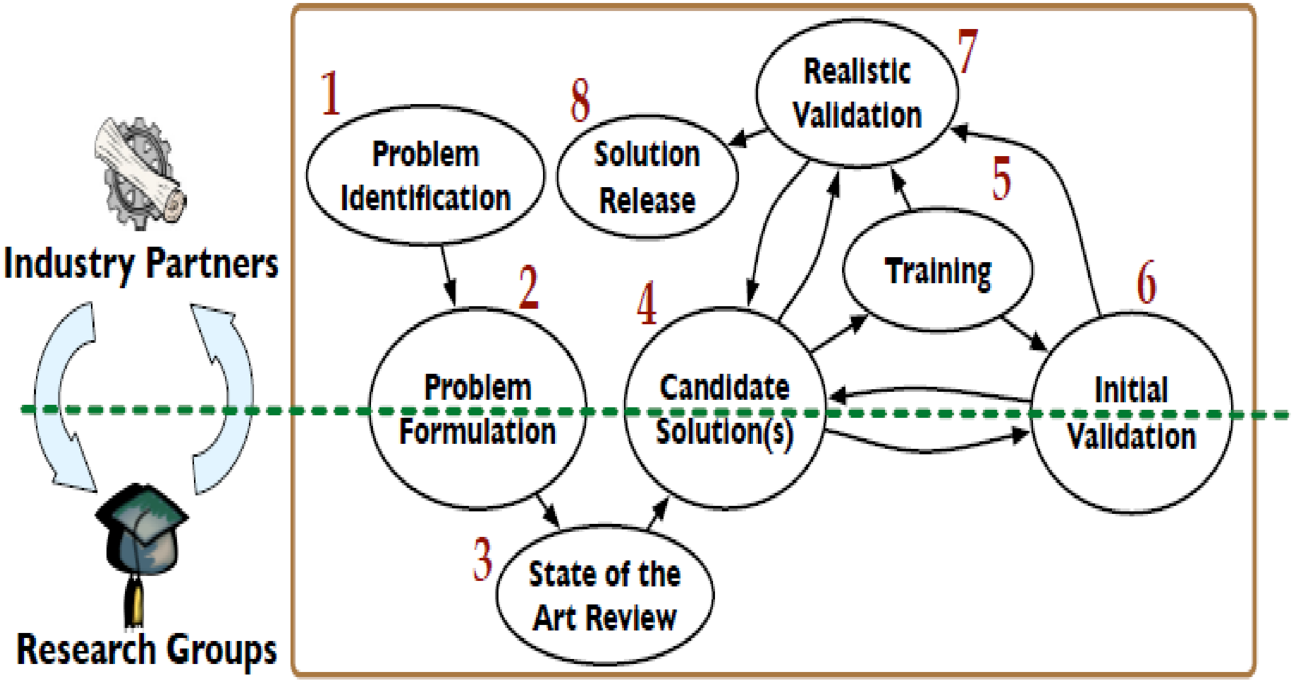
TRL

1 2 3 4 5 6 7 8 9

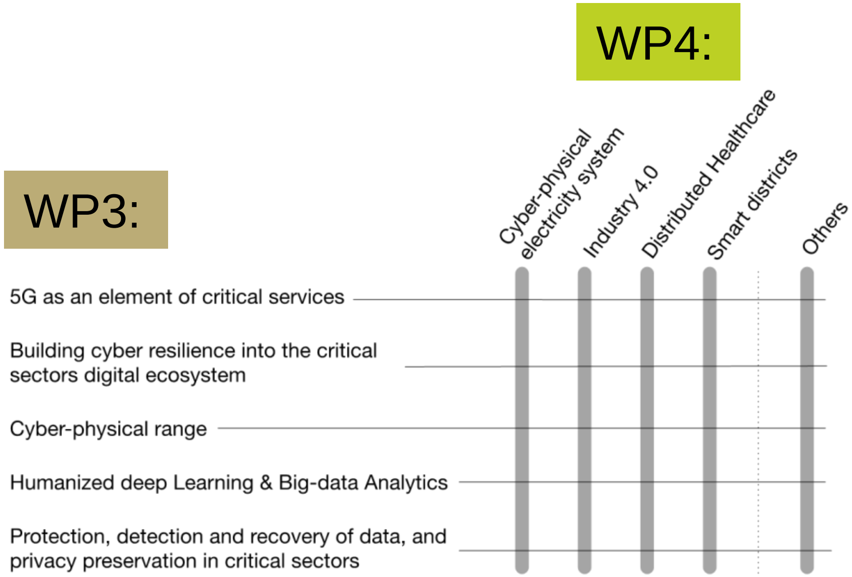
Early research

Innovation
Production

Research-based innovation process



Tasks addressing critical sectors



WP4:

Cyber-physical electricity system

Industry 4.0

Distributed Healthcare

Smart districts

Others

WP3:

5G as an element of critical services

Building cyber resilience into the critical sectors digital ecosystem

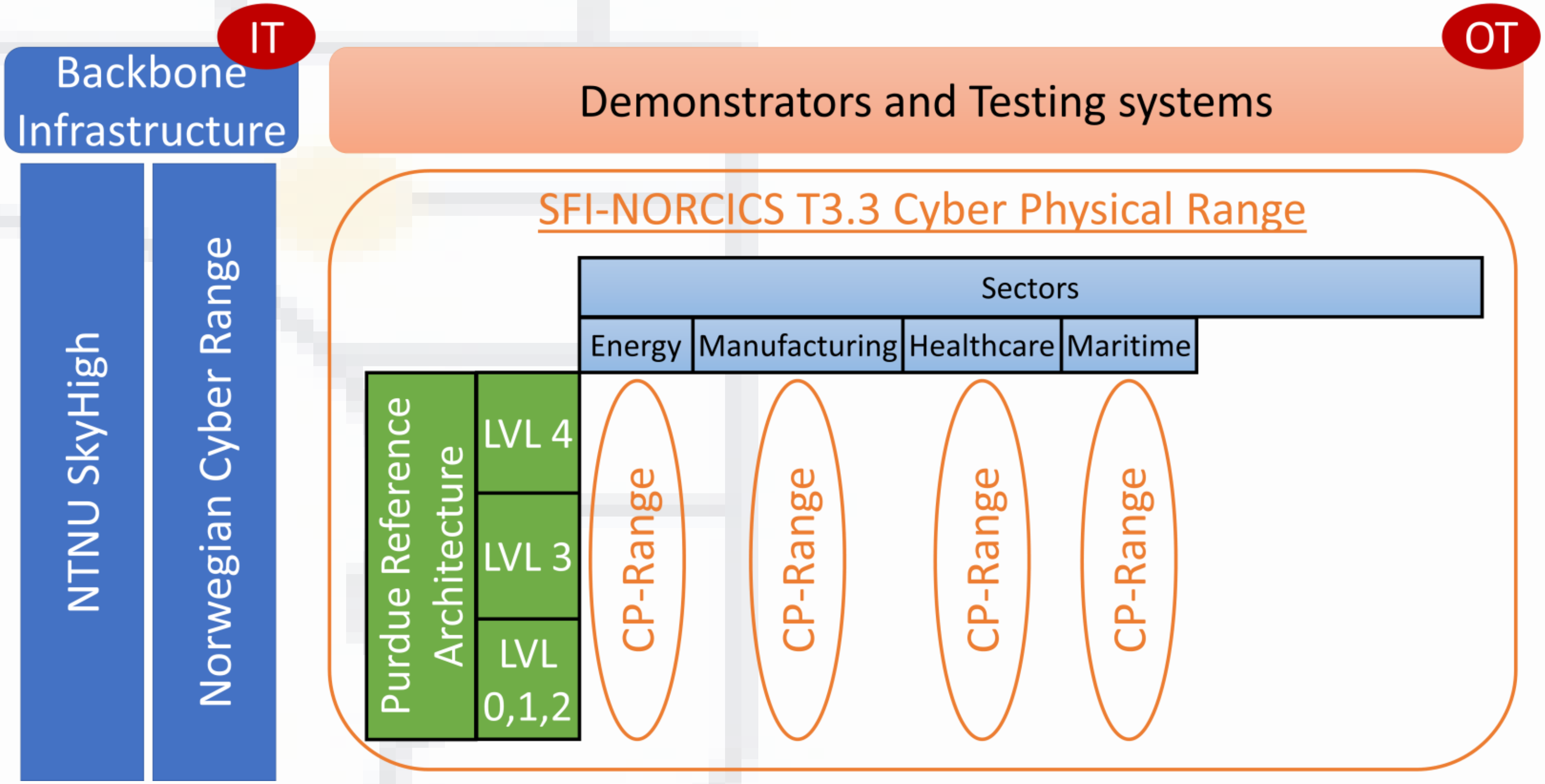
Cyber-physical range

Humanized deep Learning & Big-data Analytics

Protection, detection and recovery of data, and privacy preservation in critical sectors

- T4.1: Secure cyber-physical electricity system
- T4.2: Secure Industry 4.0
- T4.3: Secure Distributed Healthcare
- T4.4: Secure smart districts

NORCICS Cyber Physical range



“Collaboration = innovation”

https://www.ntnu.edu/norcics

NTNU | Norwegian University of Science and Technology