

DIGITALEUROPE's recommendations for a more ambitious EU Cyber Defence Policy

**CCMI hearing 28 Feb. 2023
EESC**

DIGITALEUROPE 



We represent over 45,000 businesses across Europe

The voice of digitally transforming industries

1010
1010

- platform services
- data analytics
- software & hardware
- cybersecurity
- telecoms
- semiconductors
- cloud technology



- Healthcare
- Manufacturing
- Finance
- Buildings
- Mobility

DIGITALEUROPE



41

NATIONAL ASSOCIATIONS

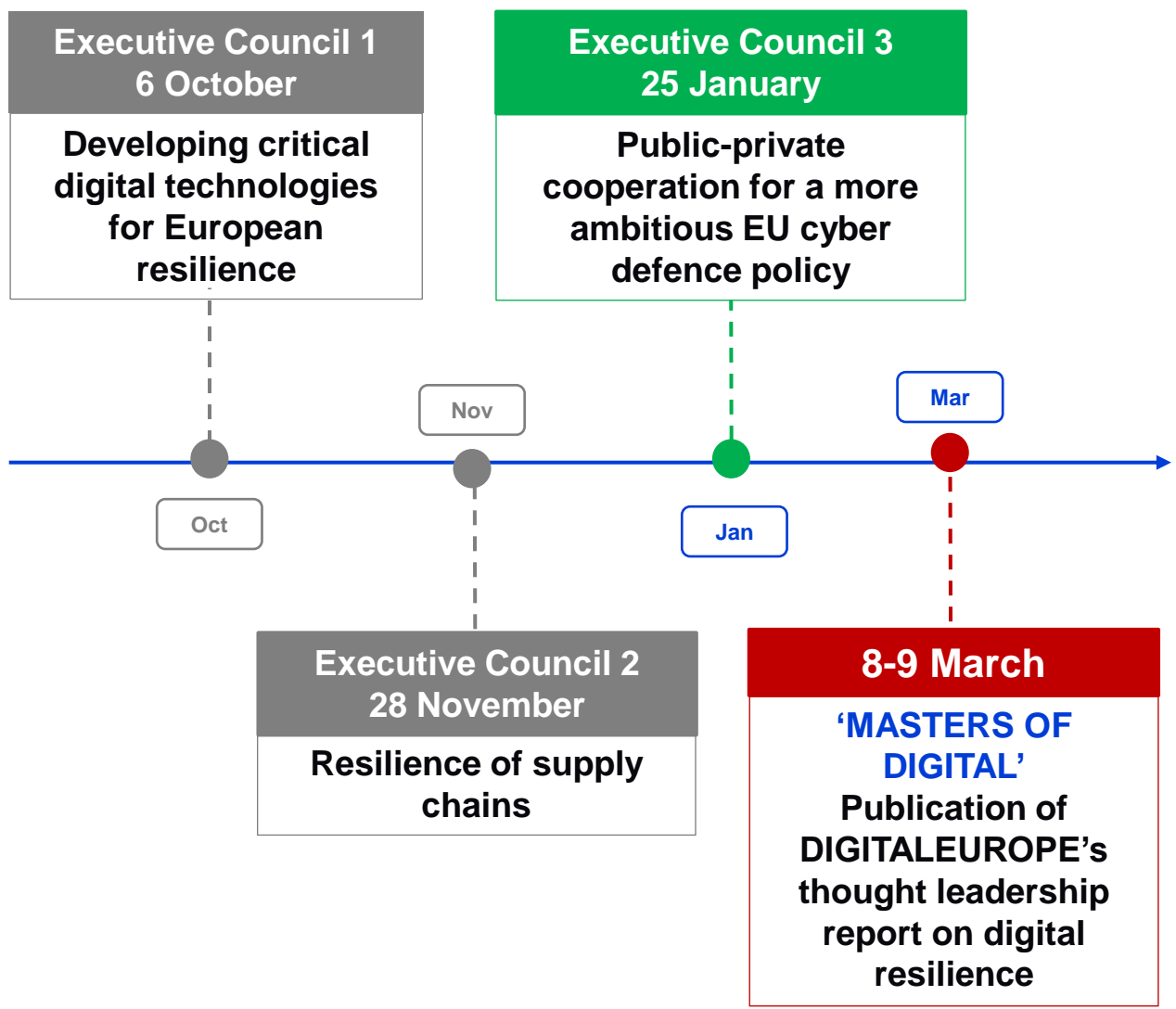
100

COMPANIES

Digital Resilience Executive Council

A forum for high-level public sector coordination with our member CEOs

| | | |
|--|--|---|
|  <p>Margaritis Schinas Vice-President European Commission</p> |  <p>Bozhidar Bozhanov Minister of e- Governance Bulgaria</p> |  <p>Janusz Cieszyński Secretary of State for Cybersecurity Poland</p> |
|  <p>Lillia Malon Commissioner for Telecommunications Ukraine</p> |  <p>David van Weel Assistant Secretary- General for EDTs NATO</p> |  <p>Ludwig Decamps General Manager NCIA</p> |
|  <p>Kim Jørgensen Director Danish Defence Denmark</p> |  <p>Jiří Šedivý Chief Executive EDA</p> |  <p>Juhan Lepassar Executive Director ENISA</p> |
|  <p>Rachel Ellehuus DEFAD U.S. Mission to NATO</p> |  <p>Joanneke Balfoort Director for Security and Defence EEAS</p> |  <p>Nathaniel C. Fick U.S. Ambassador for Cyberspace and Digital Policy</p> |



20%

**increase in
cyberattacks** on global
critical infrastructure in
2022

25%

**increase of mortality
rates** after a
ransomware attack.

19

days delay for patients
to receive some form of
care after cyberattacks

4

Months of disrupted
medical care after a
cyberattack



Technology

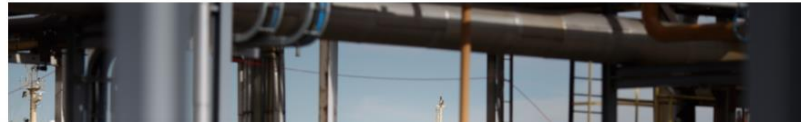
1 minute read · November 3, 2022 11:01 PM GMT+1 · Last Updated 2 months ago

Danish train standstill on Saturday caused by cyber attack

Reuters

European oil port terminals hit by cyberattack

Updated / Thursday, 3 Feb 2022 11:18



Guardian hit by serious IT incident believed to be ransomware attack

Incident has hit parts of media company's technology
infrastructure, with staff told to work from home

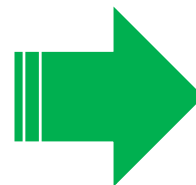


Technology

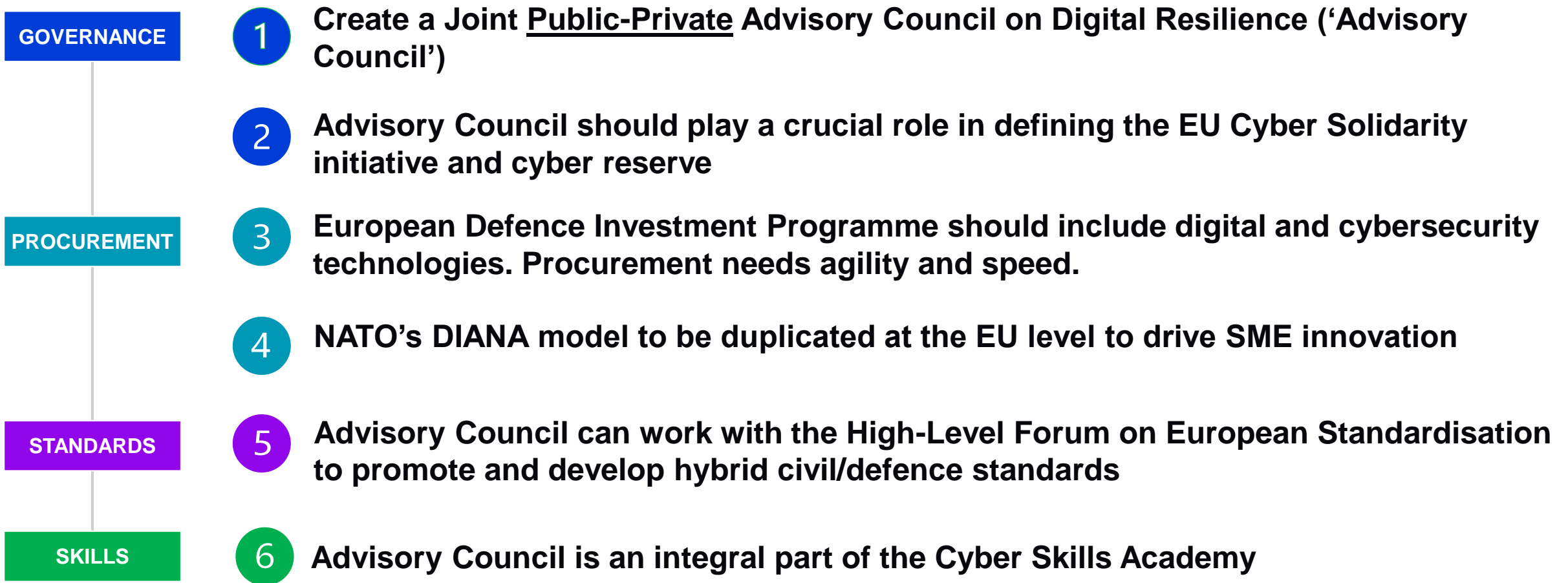
1 minute read · January 10, 2023 11:55 PM GMT+1 · Last Updated 18 hours ago

Hackers hit websites of Danish central bank, other banks

Reuters



**The role of Digital in building EU Cyber
Defence resilience is part of the solution.**



OUR RECOMMENDATIONS

- Governance
- Procurement
- Standards
- Skills

1. Governance

1 Create a Joint Public-Private Advisory Council on Cyber Resilience ('the Advisory Council').

- It supports and facilitates strategic cooperation and preparedness for a high level of security of network and information systems in the EU. The Advisory Council could be set up by the European Defence Agency. We need to streamline the number of organisations and clarify roles and responsibilities when implementing the EU Cyber Defence Policy.

EXAMPLES OF INFORMATION-SHARING MODELS

- ISACs – European Union
- Critical emergency response group – United States
- Katakri - Finland

2 The Advisory Council plays a crucial role in defining the EU Cyber Solidarity initiative and cyber reserve.

- It suggests criteria for cybersecurity certification schemes for trusted private providers and develops them.
- It supports the framework to set up the EU-level cyber reserve.

2. Procurement

3

European Defence Investment Programme (EDIP) to include relevant provisions for the joint procurement of digital and cybersecurity technologies.

- Upcoming regulation prioritises digital and cybersecurity as core components of our efforts to increase the security of EU citizens. It should be a pan-European while earmarking dedicated funds for SMEs.

4

NATO's DIANA model to be duplicated at the EU level to drive SME innovation.

- A similar bureaucratically agile and streamlined model replicated at the EU level could spur more SME innovation.

3. Standards

5 Advisory Council can work with the High-Level Forum on European Standardisation to promote and develop hybrid civil/defence standards.

- It can contribute industry expertise to establish a strong common ground in standardisation (e.g., on Common-and-control, Emergency Management, Cyber Threat Intelligence, data & information risk levels).

EXAMPLES OF CERTIFICATIONS

- The Cyber Trust mark – Singapore

4. Skills

6

The Advisory Council is an integral part of the initiative on a Cyber Skills Academy.

- The Advisory Council can contribute to outlining the framework for the Cyber Skills Academy. For example, DIGITALEUROPE is already coordinating similar programmes such as Women4IT.
- We encourage both the EU and NATO to pool resources, investments, and capabilities in developing this initiative.

EXAMPLES OF PROGRAMMES

- NATO's Locked Shields exercise
- EU Network of Cybersecurity campuses

The digital front line - 15 actions to boost Europe's Digital Resilience

Four pillars

1. **A strong and inclusive cybersecurity and cyber governance:** The ability to react swiftly and in a unified way to cyber threats.
2. **A solid and reliable critical infrastructure:** The ability to create and utilise critical platforms and tools needed to detect and handle hybrid threats.
3. **Resilient supply chains:** The ability to access the components and materials needed for a digital society to function.
4. **Fast-track procurement for critical emerging & disruptive technologies (EDTs):** The ability for Europe and its allies to encourage innovation and stay one step ahead of its adversaries.



Masters of Digital 2023

08 - 09 March 2023

Publication of DIGITALEUROPE's thought leadership report on digital resilience

FOCUS GOING FORWARD

€500
mil.

Joint procurement initiative (short-term):

- Addresses the most urgent defence capability gaps.
- Incentivises Member States to procure defence products jointly.

OUR CALL: include critical digital technologies.

Cross-
border
SOCs

Security Operation Centres (SOCs):

- The Commission is looking into setting up cross-border SOC.
- Some of the clusters on SOC are BENELUX; the Nordics; Italy/France/Romania; Greece/Bulgaria/Cyprus.

OUR CALL: include the private sector in the SOCS.

Cyber
campu
ses

Network of cybersecurity skills campuses across Member States to facilitate and support local training initiatives.

OUR CALL: use SOC + cyber reserve to promote relevant skilling programmes at national and multi-national level



DIGITALEUROPE 

Masters of Digital 2023

8-9 MARCH 2023 | BRUSSELS & ONLINE...

A resilient digital Europe in times of crisis

accenture

SIEMENS


Johnson & Johnson

 Microsoft

NOKIA



Teknikföretagen

 TechSverige



Věra Jourová
Vice President for
Values and Transparency



Margaritis Schinas
Vice President
for Promoting our European
Way of Life



Mariya Gabriel
European Commissioner for
Innovation, Research, Culture,
Education and Youth



Florian Tursky
State Secretary for
Digitilisation &
Telecommunications, Austria



Alexandra van Huffelen
Minister for Digitalisation,
Netherlands



Valeriya Ionan
Deputy Minister, Ministry of
Digital Transformation
of Ukraine

Thank you for your attention!


Don't forget to post about the event using
#ResilientDigitalEurope

DIGITALEUROPE 

Find us

 @DIGITALEUROPE

 DIGITALEUROPE

 @DigitalEuropevideo

