Sound check script

Please read out loud

Hello, my name is - - - and I will be speaking during the session today.

I am testing my audio to confirm that the technical service providers can hear me clearly.

ICANN 86 POLICY FORUM

ccNSO Community Sessions

Resilience Session (1 of 2)

9 June 2026

ICANN | ccNSO

SPEAK SLOWLY AND CLEARLY.

USE A HEADSET FOR BETTER AUDIO AND INTERPRETATION.

RAISE YOUR HAND IN ZOOM TO JOIN THE QUEUE.

ON SITE? PLEASE MUTE YOUR ZOOM AUDIO.

REMOTE? PLEASE TURN ON YOUR CAMERA WHEN SPEAKING.

NON-ENGLISH SPEAKER? LET US KNOW FOR INTERPRETATION.

Have a headset ready!

Participants could present, ask questions, or contribute in languages other than English.

Resilience Session (1 of 2)

Regulatory Trends on DNS resilience affecting ccTLDs

Tuesday, 9 June 2026 | 14:45-16:00 local

Session Chair: Annaliese Williams, .au (IGLC Chair)

- Dan York, ISOC
- Elena Plexida, ICANN org
- Dimitris Zacharias, ICANN org
- Maarten Aertsen, NLnetLabs

ICANN | ccNSO

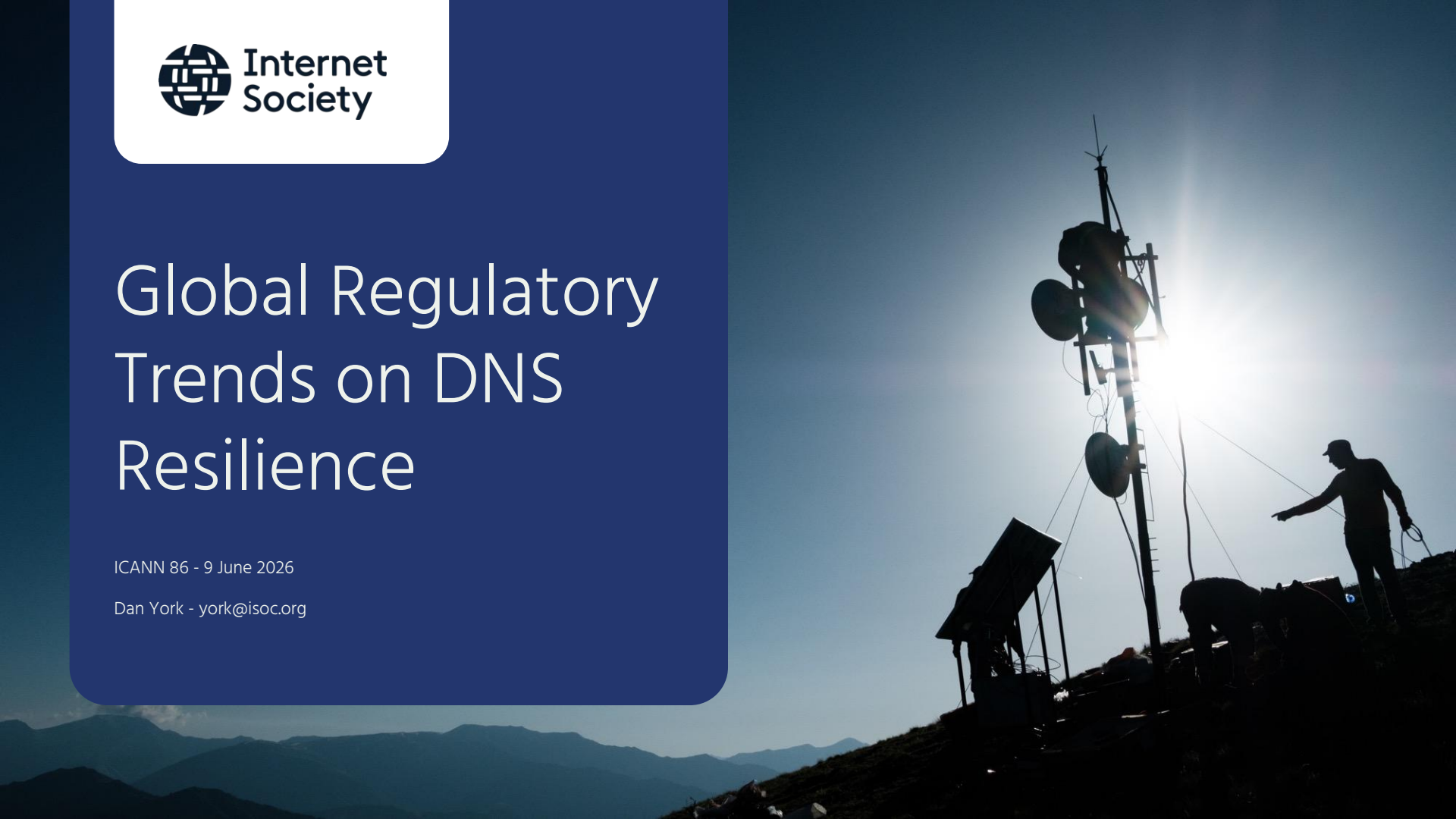
https://www.icann.org/en/ccnso/resources/governance/statements-of-interest

Internet Society

Global Regulatory Trends on DNS Resilience

ICANN 86 - 9 June 2026

Dan York - york@isoc.org



Why This Conversation Matters now

- DNS was once treated as background plumbing; regulators now consider it critical infrastructure
- Foundation for digital economy and services
- Increasing government attention and oversight
- What was a European conversation two years ago is now a global one

Technical coordination → Regulatory oversight

Global Regulation

EU

- NIS2 Directive (EU 2022/2555)
- Digital Operational Resilience Act (DORA) (EU 2022/2554)
- Critical Entities Resilience (CER) Directive (EU 2022/2557)
- Cyber Resilience Act (CRA) (EU 2024/2847)

UK

- Cyber Security and Resilience Bill 2024-26

US

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
- CISA Protective DNS / CPG 2.0

China

- Cybersecurity Law (Revised 2026)

India

- CERT-In Directions (2022)

Australia

- Cybersecurity Act 2025
- Security of Critical Infrastructure (SOCI) Act

Singapore

- Cybersecurity Act 2024

Saudi Arabia

- Essential Cybersecurity Controls (ECC)

Zambia

- Cyber Security Act 2025

Why the Acceleration?

- Increasing cyber threats targeting infrastructure
- Growing dependence on digital services
- National security and economic stability concerns
- Digital security now a political issue – governments taking stronger role

Converging Global Trends

1

Operational Resilience

2

Incident Reporting & Accountability

3

Data Governance & Autonomy

4

Mandatory Minimum Security Baselines

5

Supply Chain

Trend 1 – Operational Resilience

Resilience Becomes Mandatory

- Risk management requirements
- Business continuity expectations

Examples:

- NIS2 Directive (EU)
- Singapore Cybersecurity Act

Trend 2: Incident Reporting

Incidents ⟶ Regulatory Events

- Rapid reporting requirements (often ≤24h), often to a government agency
- Mandatory disclosure obligations
- Increased executive accountability and liability (including fines)

Examples:

- NIS2 Directive
- US CIRCIA
- India CERT-In Directions

Trend 3: Data Governance & Autonomy Pressure

- WHOIS / registration data constraints
- Cross-border data restrictions
- Law enforcement access requirements
- Aggressive takedown mandates

Examples:

- GDPR (EU)
- China Cybersecurity & Data Laws
- Discussions of “foreign control” and a “kill switch”

Trend 4: Minimum Security Baselines

From Risk-Based → Prescriptive Controls

- Defined minimum security requirements
- Secure-by-design expectations
- Lifecycle vulnerability management

Also:

- “Voluntary” frameworks becoming mandatory
- AICPA SOC 1/2, ISO 27001, NIST baselines, certification schemes

Trend 5 – Supply Chain

Regulators focus on supply chain as a new attack surface

- You are responsible for security of your vendors, not just your own systems
- For ccTLDs: your open source DNS software vendor, anycast provider, registrar accreditation program – all could be in scope

Examples:

- Cyber Resilience Act (EU)
- US CIRCIA guidance
- NIST SBOM (Software Bill of Materials)

Implications for ccTLDs

- Increasing classification as critical infrastructure
- Tension: global DNS vs national regulation – multiple reporting and disclosure requirements
- Compliance requirements may require significant resources
- Expanding supply chain obligations

- Opportunity to influence policy development
    - Given that ccTLDs are critical infrastructure, opportunity to engage
    - Potential to work regionally (APTLD, AFTLD, LACTLD, CENTR) on compliance approaches

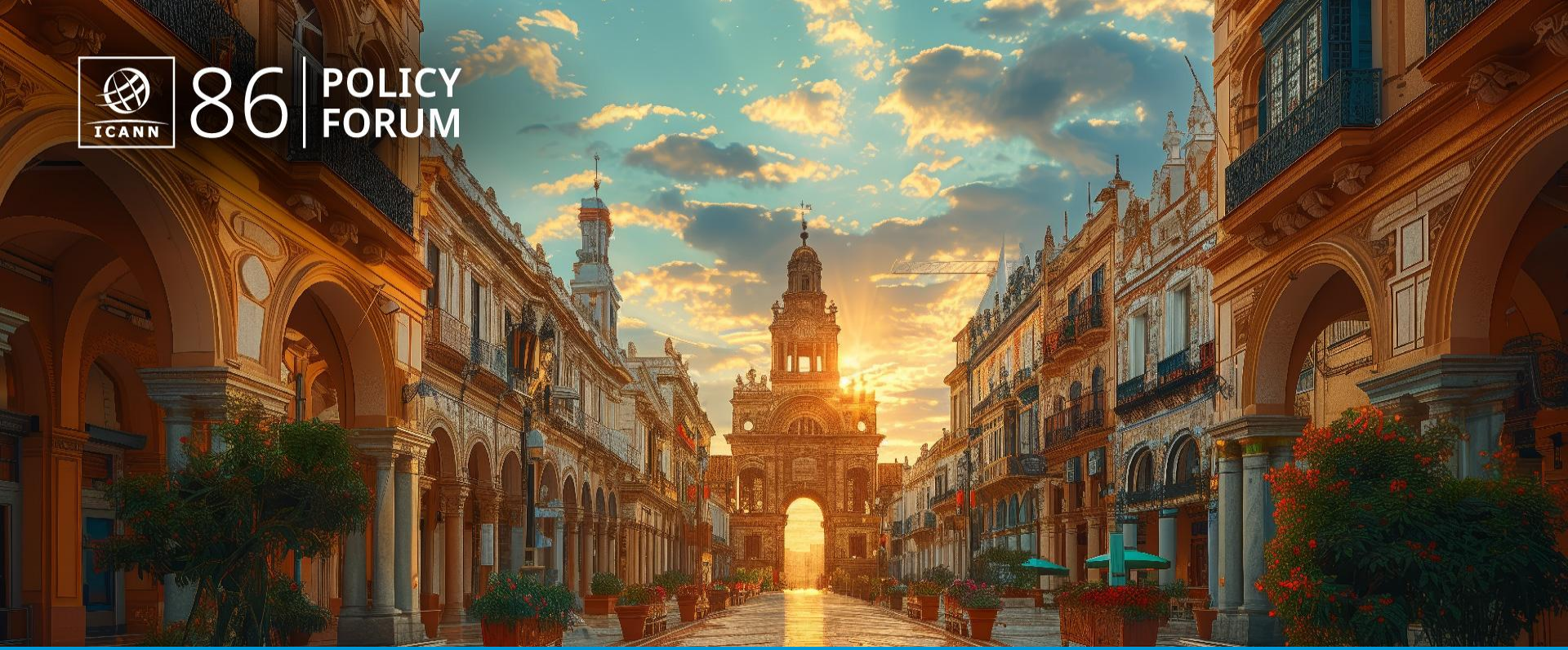
Questions:

- Do your government's cybersecurity regulators know you exist? (and do they know what a ccTLD is?)
- Is your ccTLD in scope of one of these regulations – and do you know what that means operationally?

Thank you.

Dan York
york@isoc.org

internetsociety.org
@internetsociety



ccNSO Session

Regulatory Trends on DNS Resilience Affecting ccTLDs

EU Regulatory Initiatives

NIS2 Directive, Targeted Amendments to NIS2, CSA2, CRA.

NIS2 Directive | Introduction

Classification of Sectors and Entities

Essential and **Important** Entities

Size Cap Rule

Sectors of **High Criticality** and **Other Critical Sectors**

Differentiated **Enforcement** Approach

Cybersecurity Risk Management Measures

Technical, **operational** and **organisational** measures to manage the risks posed to the security of network and information systems

Article 21 and Annex to Implementing Regulation

Incident Reporting Requirements

Early warning **(24hrs)**

Incident notification **(72hrs)**

Final report **(1 month)**

Implementing Regulation **specifying significant incidents**

NIS2 Directive | Implementing Act

Significant Incident

The Implementing Regulation specifies what constitutes a **significant incident** with regards to DNS service providers and other digital infrastructure providers

Cybersecurity Risk Management Measures

The Annex specifies the **technical** and **methodological requirements** of the cybersecurity risk-management measures.

NIS2 Directive | Targeted Amendments

EU's New **Cybersecurity Package**:
Targeted Amendments to the NIS2 Directive

***Objective**: increase legal clarity by simplifying jurisdictional rules, streamlining the collection of data on ransomware attacks and facilitating the supervision of cross-border entities.*

Proposed changes:

Amendment to Scope | Size-cap Rule and introduction of Small Mid Caps

Certificate on **Cyber Posture**

Maximum harmonization for the implementation of cybersecurity risk management measures (Implementing Regulation | Art 21, NIS2)

Ransomware-specific reporting requirements

Registry of essential and important entities to coordinate **cross-border supervision**

Cybersecurity Act 2.0 | Introduction

EU's New **Cybersecurity Package**:
Cybersecurity Act 2

***Objective**:enhance the security of the EU's ICT supply chains, and that products reaching EU citizens are cyber-secure by design*

- Address **supply-chain** risks, especially those linked to third-country influence
- Improve the effectiveness and uptake of **certification schemes**
- Reduce fragmentation across Member States
- Strengthen EU strategic autonomy in critical technologies
- Support businesses through clearer and more streamlined compliance mechanisms

Cybersecurity Act 2.0 | Pillars

Security of ICT Supply Chain

Designation of of **High-Risk** Third Countries

Mitigation measures in the ICT Supply Chain

Identification of **High Risk Suppliers**

Restrictions on certain high-risk ICT suppliers in sectors covered by NIS2

European Cybersecurity Certification Framework

Extended **Scope** and Cybersecurity posture

Timeline clarification and streamlined governance

Low - Substantial - High **Assurance Leves**

Supply chain integration

Mandate of ENISA

Enhanced situational awareness and coordination role

Vulnerability management and incident reporting

ECCF lead and Cybersecurity Skills Academy

Cybersecurity Package | Impact on ccTLDs

Critical Infrastructure

ccTLDs are designated as **essential entities** in sectors of high criticality - compliance with cyber and reporting obligations.

The Annex of the NIS2 Directive serves as the **foundation** on which other sectoral/cyber legislation is built.

Potential de facto inclusion of ccTLDs and the wider DNS space in future initiatives ushering in obligations.

Key ICT Assets

DNS is identified as a component of the **core networks functions** of both mobile and fixed electronic communications networks.

The EU's trusted ICT supply chain framework will address **non-technical risks related to high-risk suppliers** and dependencies in sectors of high criticality.

Potential **binding mitigation measures** triggering downstream consequences.

Cyber Resilience Act | Introduction

The CRA introduces mandatory cybersecurity standards for all **hardware** and **software** products **with digital elements**

Requirements:

- **Security by design**: products with digital elements are delivered with secure default configurations
- **Vulnerability & Patch Management**: handle security flaws and provide timely security updates
- **Transparency**: documentation and reporting obligations regarding vulnerabilities and cyber incidents
- **CE Marking**: compliant products will bear a CE mark to attest cyber secure hardware and software
- Compliance to be demonstrated before products on the EU market.

Cyber Resilience Act | Obligations

Secure Product Development

Cybersecurity Risk Assessments

Assess 3rd party risks and open source components

Minimize risk surfaces and unauthorized access

Integrate cybersecurity into development, testing and maintenance processes

Vulnerability Management & Operational Security

Vulnerability handling and disclosure procedure

Remediate vulnerabilities and provide security updates

Report actively exploited vulnerabilities

Maintain support throughout declared support period

Compliance and Transparency

Technical documentation

Conformity Assessments

Declarations of conformity and application of CE marking

Ensure importers, distributors and manufacturers fulfill responsibilities

Cyber Resilience Act | Impact on ccTLDs

Operating the Registry

Largely a **NIS2**/critical infrastructure issue - cybersecurity and reporting obligations

Registry developed or commercialized software products for 3rd parties could potentially fall within the scope of the CRA

CRA-compliant software and hardware

Supply Chain Security and Reporting Ecosystem

CRA obligations throughout the software and hardware supply chain.

Registries may need to assess whether products they depend on are CRA-compliant (particularly for security-critical systems)

Thank you!

Elena Plexida & Dimitris Zacharias | ICANN GE Team

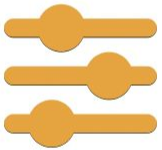
NLnet *Labs*

Through the eyes of an open source implementer of DNS software

the impact of recent EU regulatory developments
on the DNS and related services

Key Takeaways from SAC132

The DNS Runs on FOSS

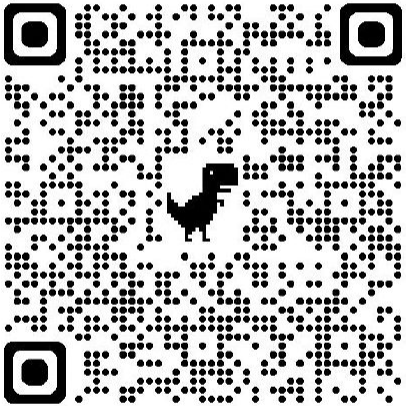


FOSS is Different

↳ *Policy Must Adapt*

We Can Get It Right

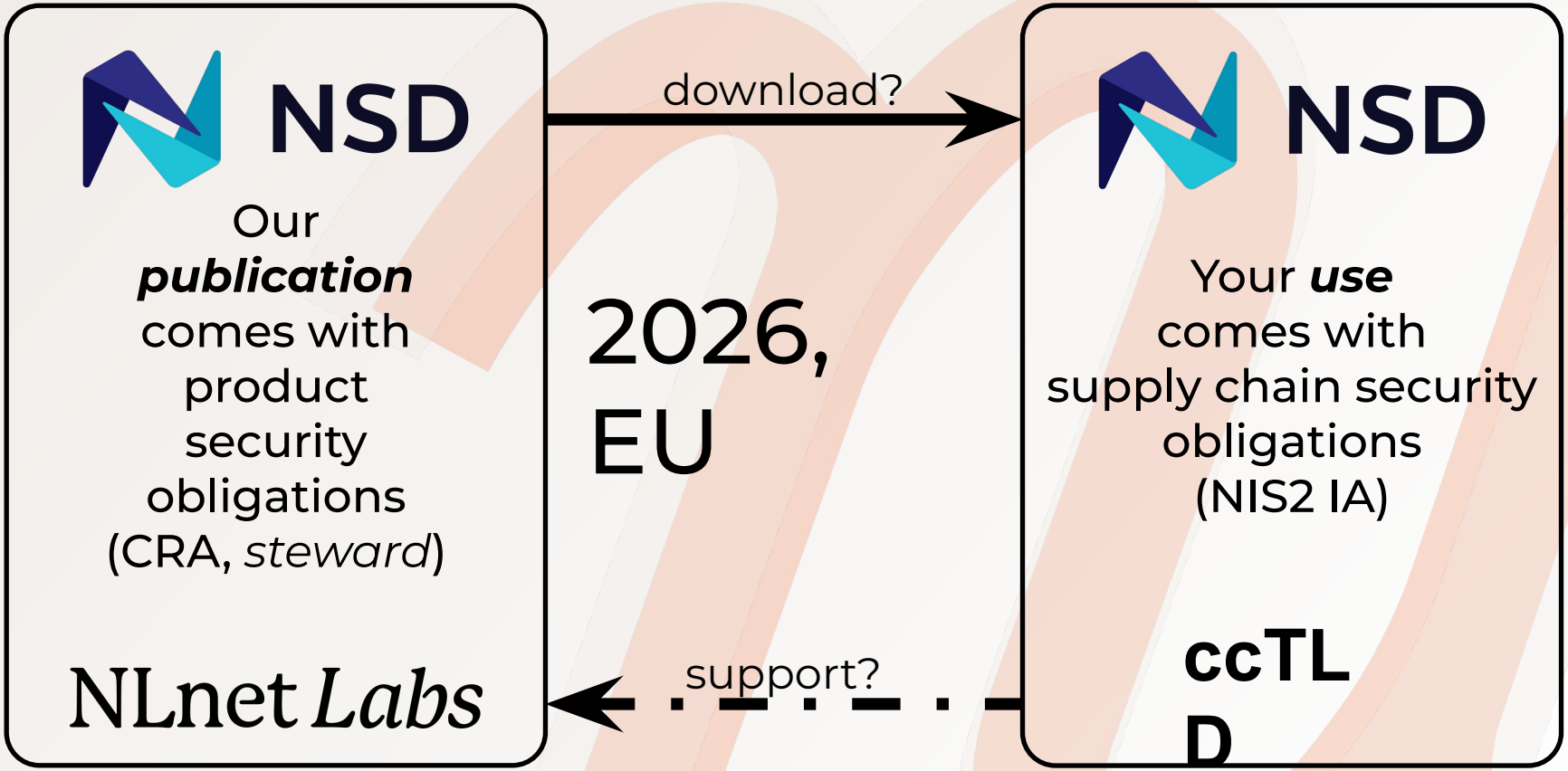
↳ *Good Examples Exist*



Your use of open source software is not an implementation detail.

Supply chain security for open source software is different.

That maintainer, is not your supplier.


NSD
Our
publication
comes with
product
security
obligations
(CRA, *steward*)
NLnet *Labs*
download?
2026,
EU
support?
NSD
Your ***use***
comes with
supply chain security
obligations
(NIS2 IA)
ccTL
D

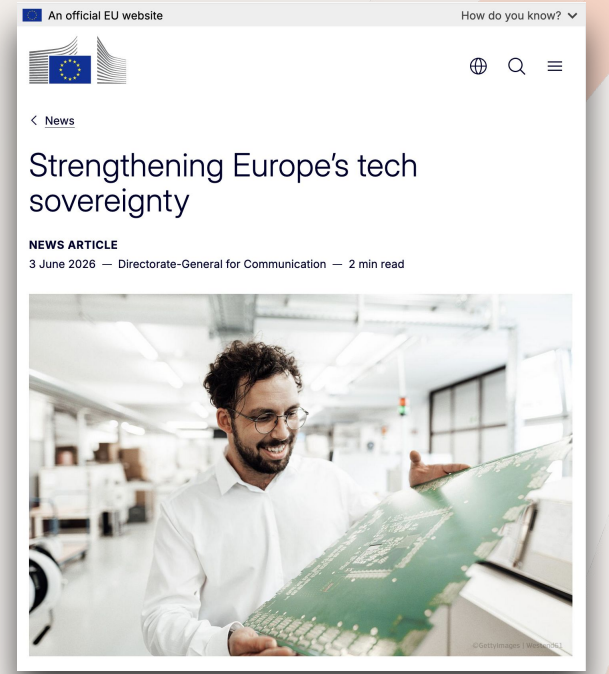
EU policy on FOSS is shifting, in ways that will affect us

"[..] communities and projects that openly develop, maintain and distribute [FOSS] may not be considered direct suppliers or service providers

- where no contractual relationship exists between the relevant entity and the open source project [..], or
- where the contractual relationship is with an open source software steward [..]."

NLnet *Labs*

EU policy on FOSS is shifting, in ways that will affect us?



Any questions? Please type them here.

No questions from the audience!

Incoming questions will show up here so that you can answer them one by one.

menti.com

2754 3202

Waiting for participants

Thank you!