

European Commission proposal for a Cyber Resilience Act

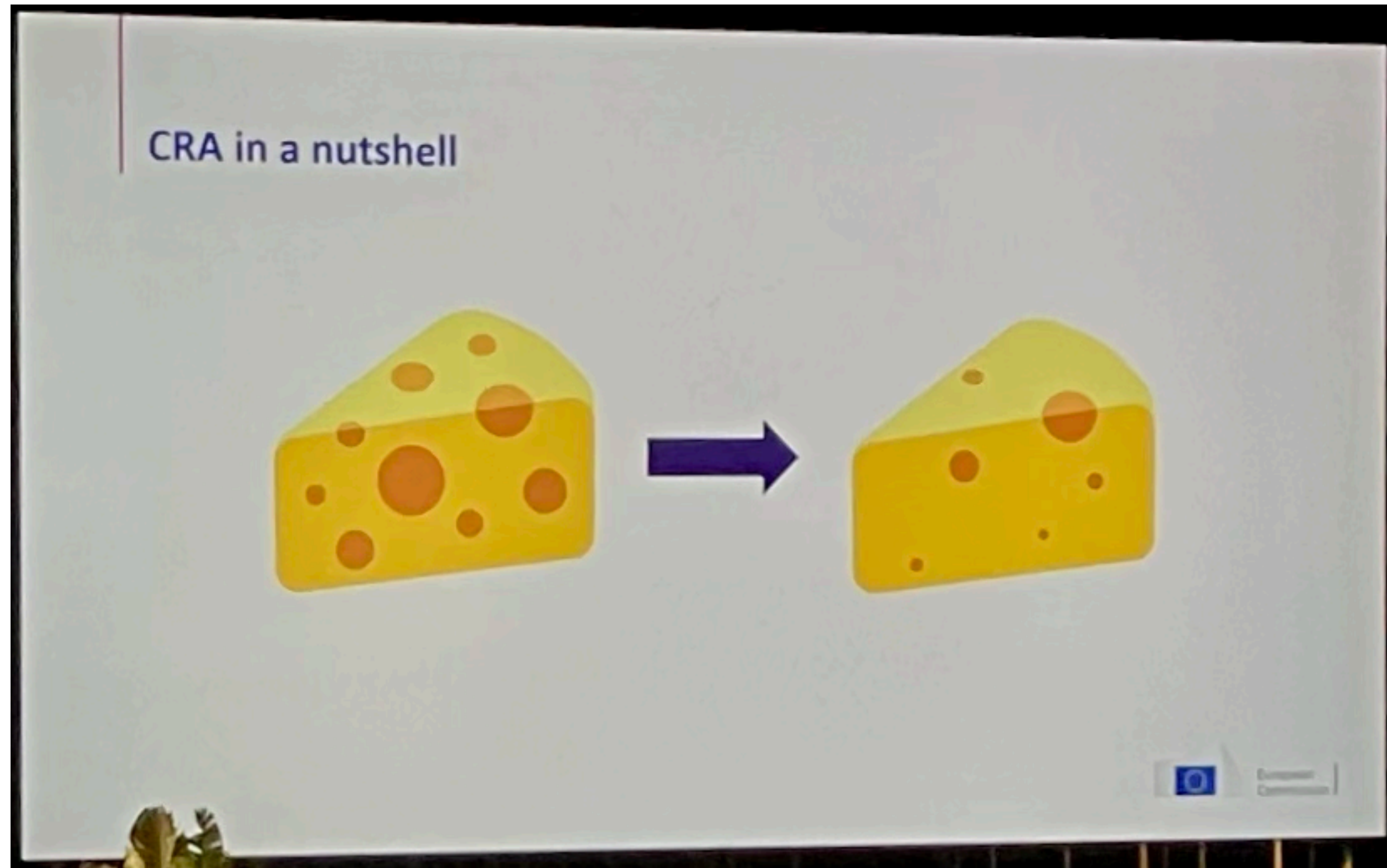
Effects on open source for internet infrastructure?

proposal text: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>



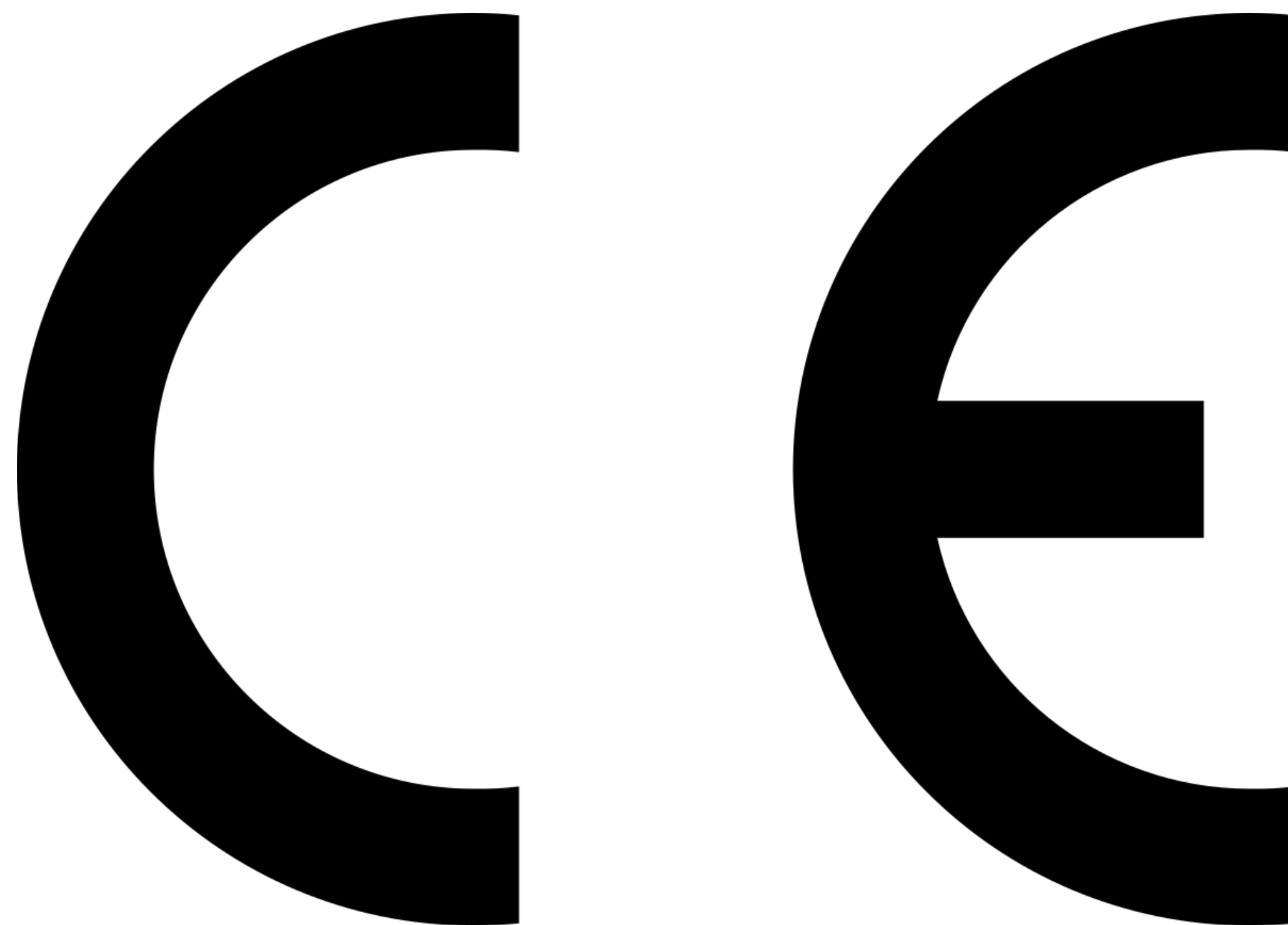
After regulating digital *services* under NIS2, EC sees two major problems for *products*

1. a low level of cybersecurity
2. an insufficient understanding and access to information by users



European Commission intends to regulate
products with digital elements
(\approx all hardware & software)

Image source: keynote by Christiane Kirketerp de Viron, EC's DG CONNECT at One Conference, the Hague



A few example critical products (Annex III)

- Operating systems
- Routers, switches
- Remote access software
- Network (configuration) management systems/tools
- Network traffic monitoring systems
- PKI/cert issuers

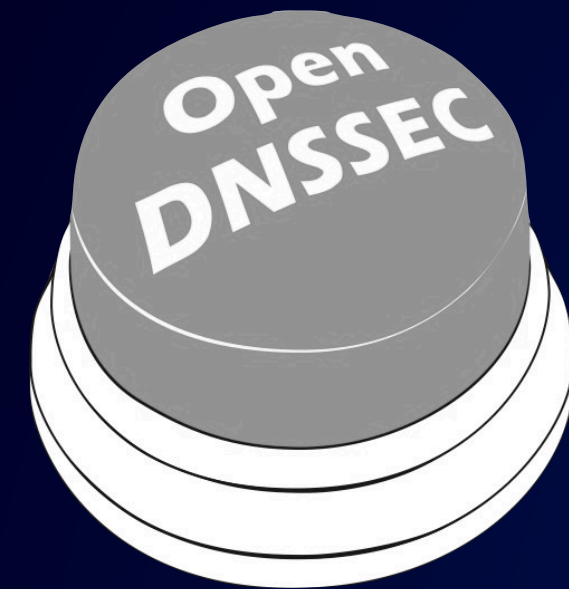
Product certification

Product security & vulnerability handling
(Annex I)

Information and instructions to the user
(Annex II)

Risk assessment & technical docs
(article 10.2, Annex V)

Conformity assessment:
1st / 3rd party (criticality)
(Annex IV, article 24)



Flexible key management
& zone signer

super-fast
authoritative
DNS name server



NSD



unbound

multi-purpose
DNS resolver

RPKI validator
("Relying Party Software")

The logo for ROUTINATOR, featuring the word "ROUTINATOR" in white with a blue rocket ship icon replacing the 'O'.



Krill

all singing and dancing
delegated RPKI

OSS out of scope?

"In order not to hamper innovation or research,
free and open-source software
developed or supplied
outside the course of a commercial activity
should not be covered by this Regulation. [..]"


- recital 10

"Commercial activity"?

"[...] **a commercial activity might be characterized** not only

1. by charging a price for a product, but also
2. by charging a price for technical support services,
3. by providing a software platform through which the manufacturer monetises other services, or
4. by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. "

- recital 10



A distinction between open source development with no income, some income and full income?

Legal uncertainty about the boundaries of the term *commercial activity*

Compliance costs for individuals & orgs now focussed on improving the quality of software.

Will this discourage volunteers from earning their living and work on OSS full-time?

Will developers avoid open source software made in the EU to avoid the CRA's effects?



What are the downsides to treating all open source software out of scope?

Alternatively, should “commercial activities” by *for-profit* and *not-for-profit* be distinguished?

At this point, we have more concerns and questions than answers and solutions.

Track this legislation if you care about the CRA’s impact on OSS for internet infrastructure

Aside: the “commercial activities” phrasing is also in the new defective product liability proposal

Please talk to us when you
have similar concerns,
want to team up or
can help us to provide technical
expertise in the right places.

Thanks

maarten@nlnetlabs.nl
@nlnetlabs



Further reading: [The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem](https://isoc.org/en/2022/05/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/) at isoc.org