Why Cybersecurity Assurance and why now?

Speaker: Arnaud Taddei
ITU-T SG17 Vice Chairman
Global Security Strategist – Symantec by Broadcom

Intentions

Give a context to cybersecurity assurance practices …

… and the conditions are not good!

- Neither from the attacking side
- Nor from the defending side

But standardization could help a little bit

And hopefully it will help all stakeholders to make wise decisions

And offer a better foundation to cybersecurity assurance

A deteriorating landscape in a widening paradox

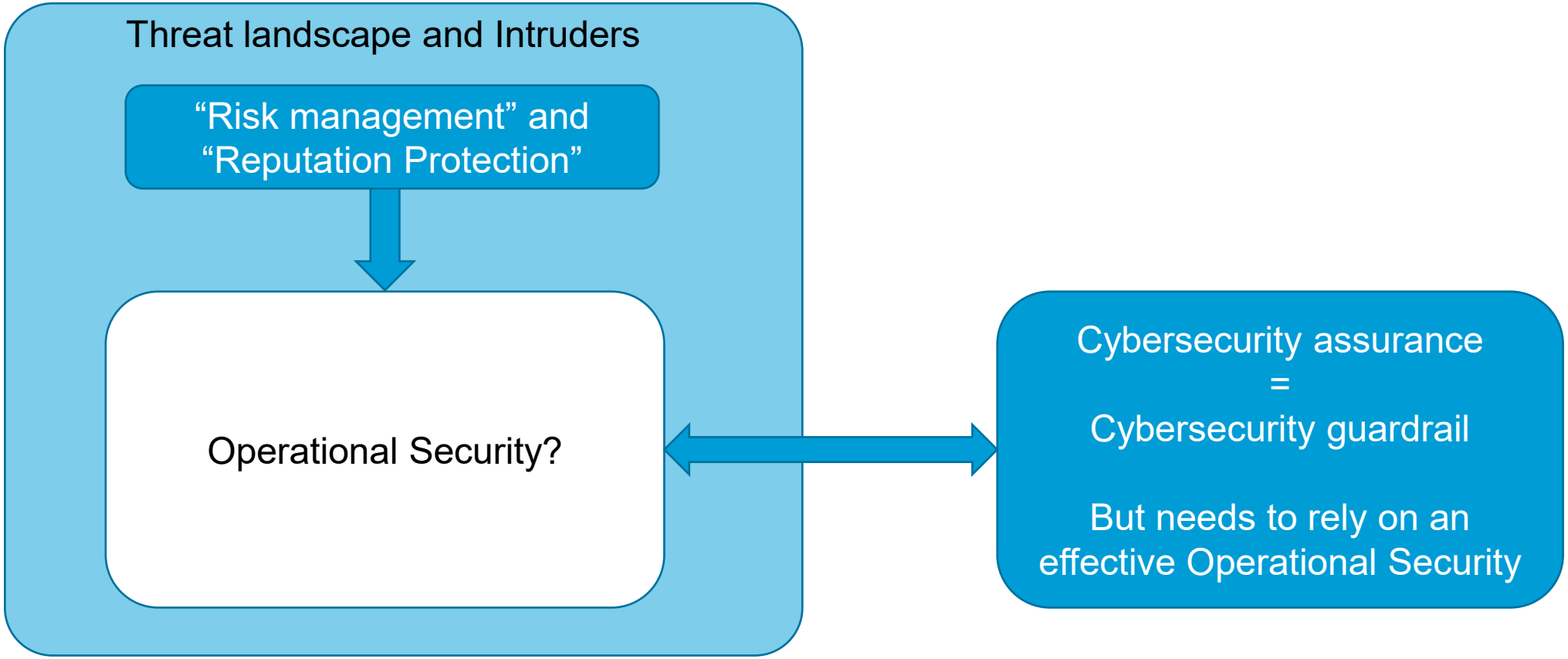
Cyber criminal business at $6T (source French Gendarmerie Colonel)	1/3rd of EU GDP!
Ransomware #1 priority	But accounts for very small $$ in above!
Email still #1 attack vector	Phishing is not a technical attack, it is a brain attack! (think ChatGPT!)
Zero Trust is the answer for everything	But some organizations are disinvesting from it! (and operational teams think it is 'marketing')
SASE/SSE/MESH moves towards a new 'product'	But no formal international consensus on Security Architecture since X.800 (1991)!

Zoom on the threat landscape – Ransomware #1

Cyber insurance?
Cyber assurance?

- Despite a decrease, Ransomware is number #1 priority by LARGE
- Many statistics that are difficult to reconcile with $30B or more damage in 2023
    - Why is it so small vs $6T of cybercriminal business because the real money comes from data exploitation and trade!
- A vast range of variations, victims, on all segments and regions
- Examples of ransomware attacks on large multinational (€34B on 85 countries) showed
    - They could have lost entirely one of their subsidiary, an MNO, a 30 years business of €1.3B
    - The attack succeeded on all layers BUT on one backup link!
    - Massive insight lessons learnt and some conclusions:
        - Preparedness including simulations and team training and coherency
        - Crisis management and Risk management including a Cyber insurance financial view
        - The lack of an integrated Cyber Defence Center (CDC)
        - Do anticipate that IT WILL SUCCEED – How to reconstruct (Backups and online Backups)

A high-level view of why we need Cybersecurity assurance



So what's the problem with Operational Security?

Recognize we are missing a common foundation

Last international consensus?

First Firewalls (Perimeter Defense) 1994

Let's remove the Firewall (BeyondCorp) 2007

Shift from ZT'school' to SBOM 'school'

COVID

1990 | 2000 | 2010 | 2020

ITU X.800 1991

Jericho Forum 2003

BeyondCorp (Google) 2007

ZT (Forrester) 2010

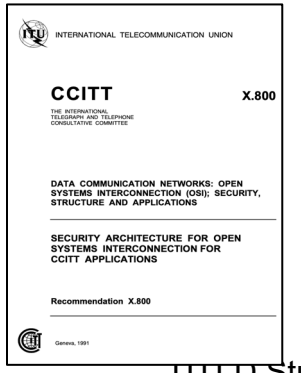
Defense in Depth (NIST) 2012

NIST / UK NCSC / … ZT Architectures

SASE (Gartner) 2019

SSE (Gartner) 2022

MESH (Gartner) 2022


INTERNATIONAL TELECOMMUNICATION UNION

CCITT X.800

THE INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE

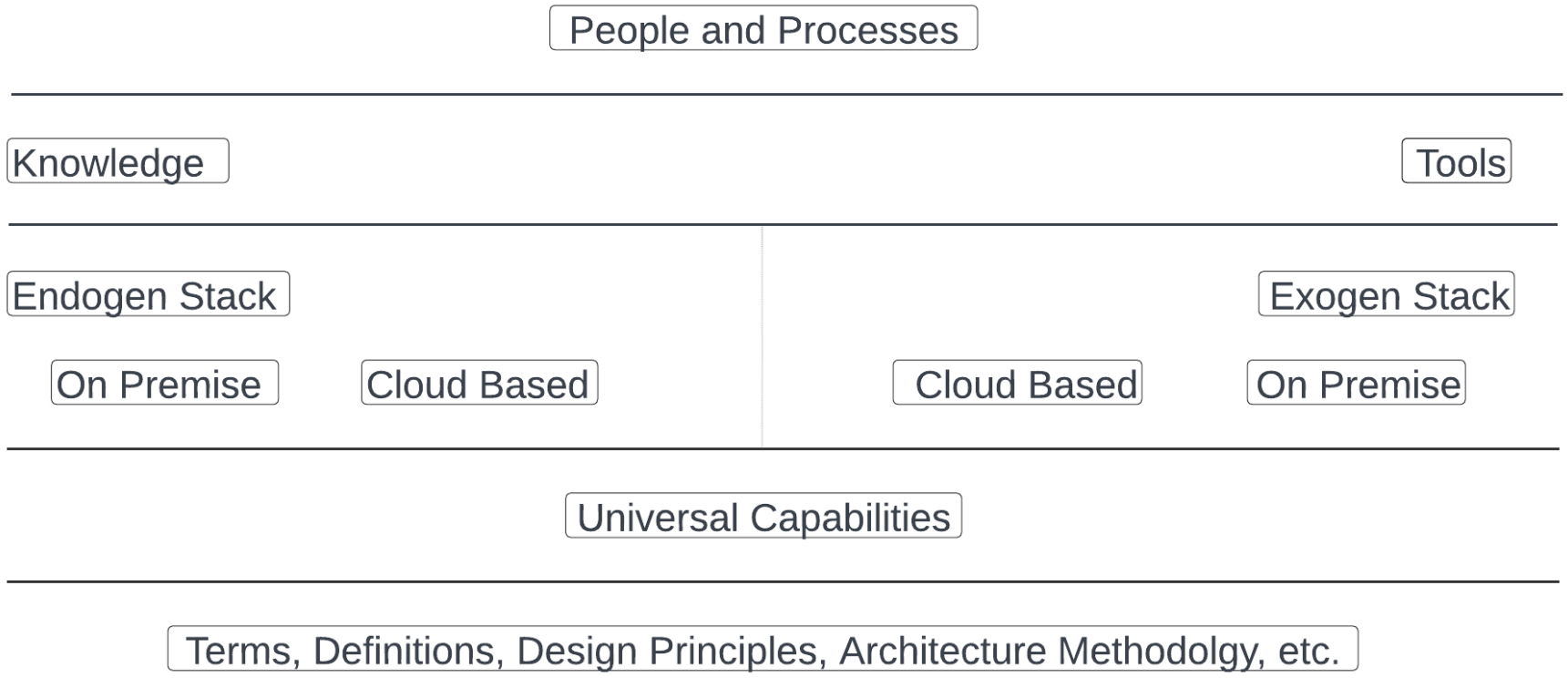
DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Recommendation X.800

Geneva, 1991

Acknowledge the need for an ”OSI model for security”

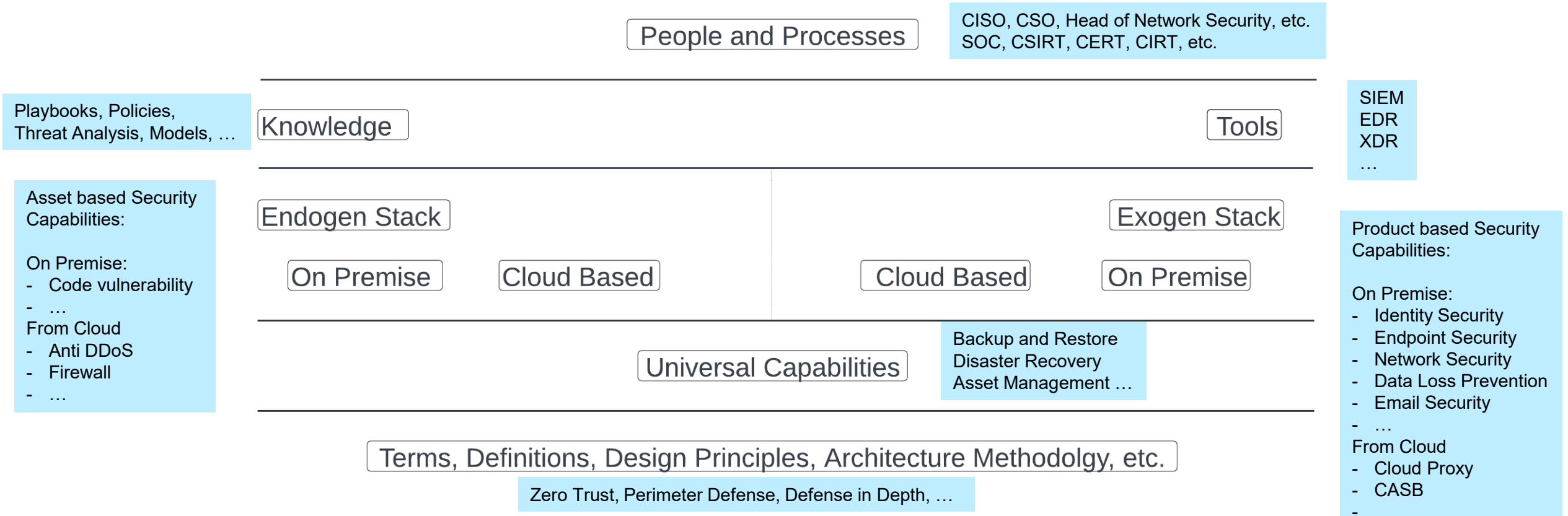


Under study at ITU-T SG17

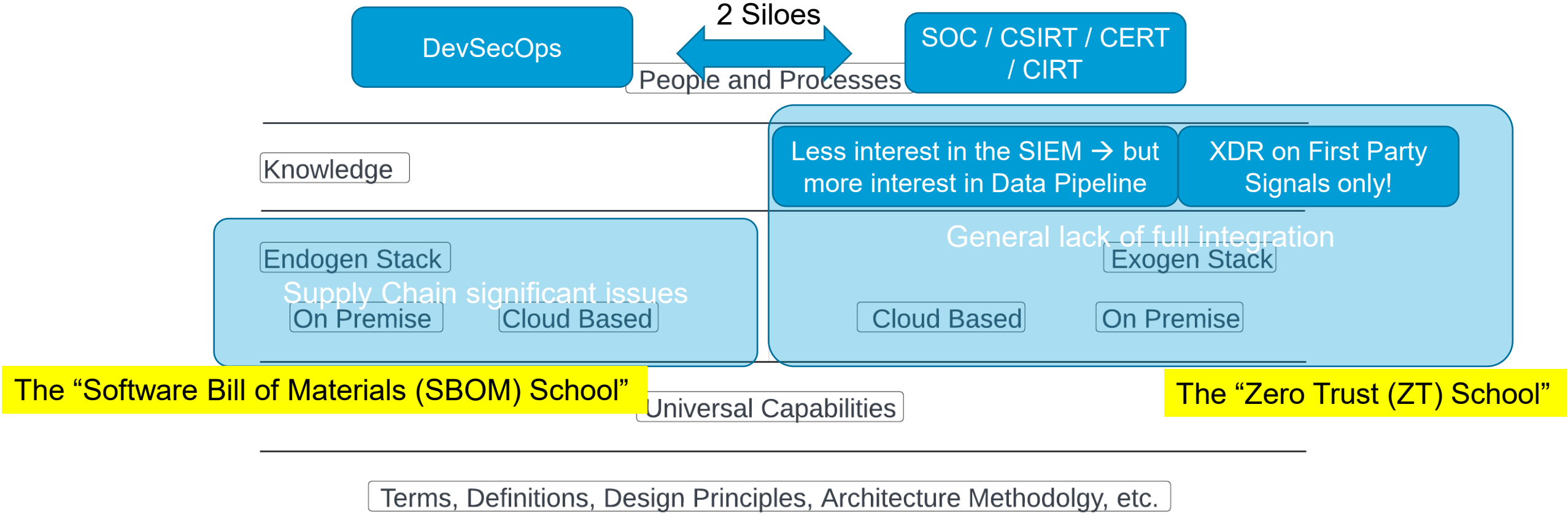
Narrative: “if all the job is to reduce risk and protect reputation then what are the key constituencies for a reasonable operational security:

- People and process …
- … who extract their knowledge …
- … to instruct a product stack …
- … to protect assets”

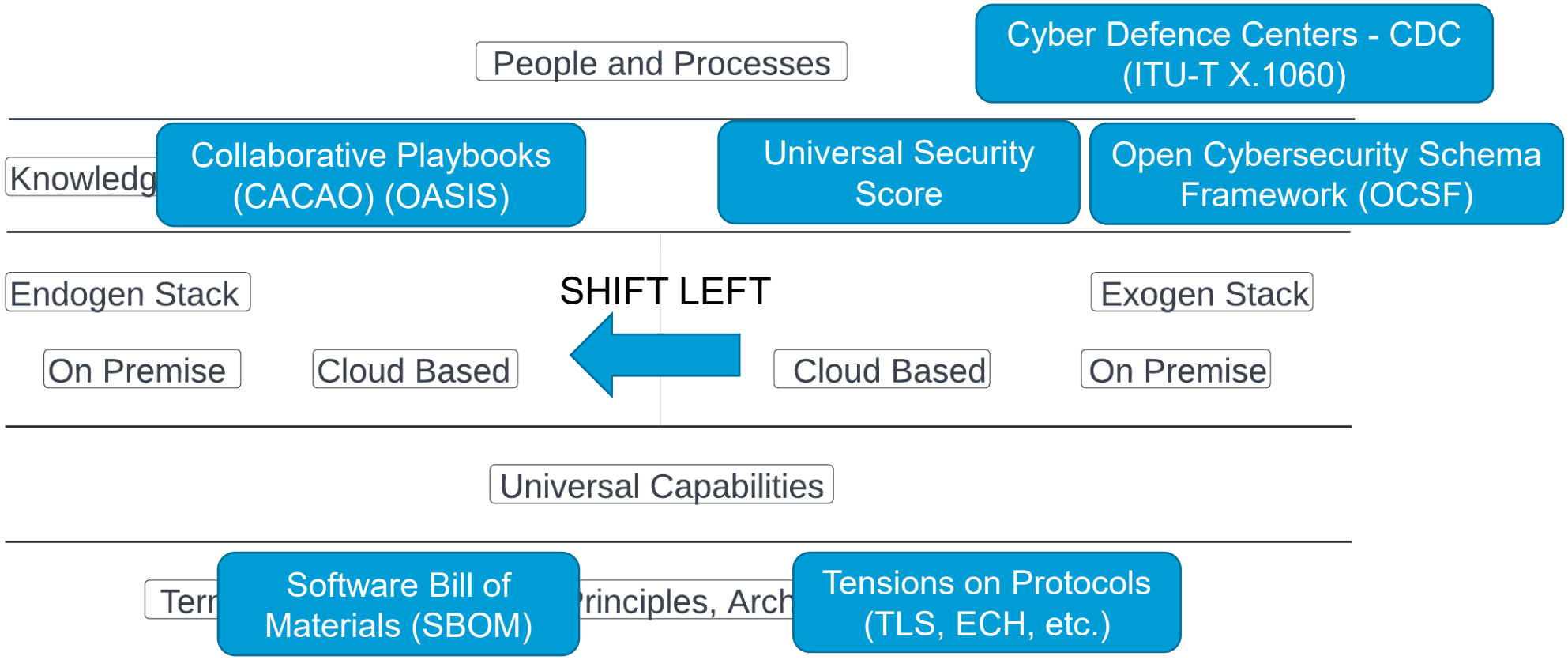
Acknowledge the need for an ”OSI model for security”



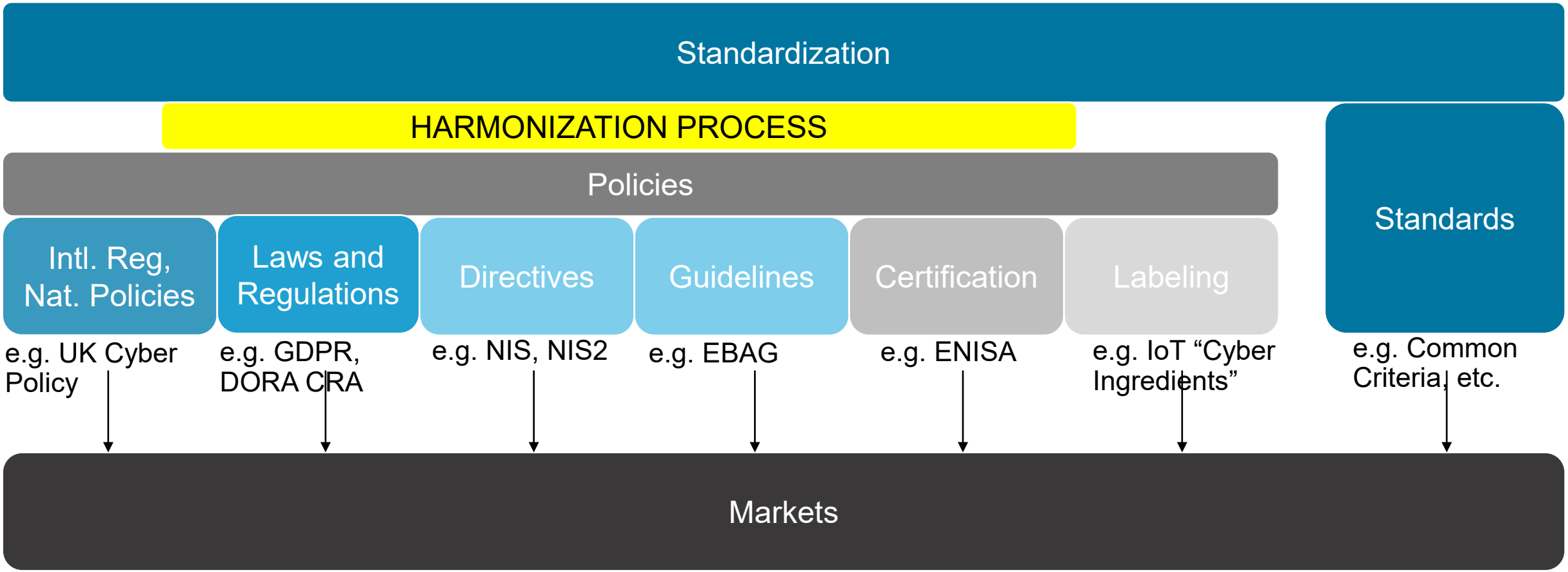
Industry Gaps (Examples)



Standardization Limited Progress (Examples but still many gaps)



Why Standardization is important?



Regulatory example: is the future EU Cyber Resilience Act (CRA) a way to help Cybersecurity Assurance?

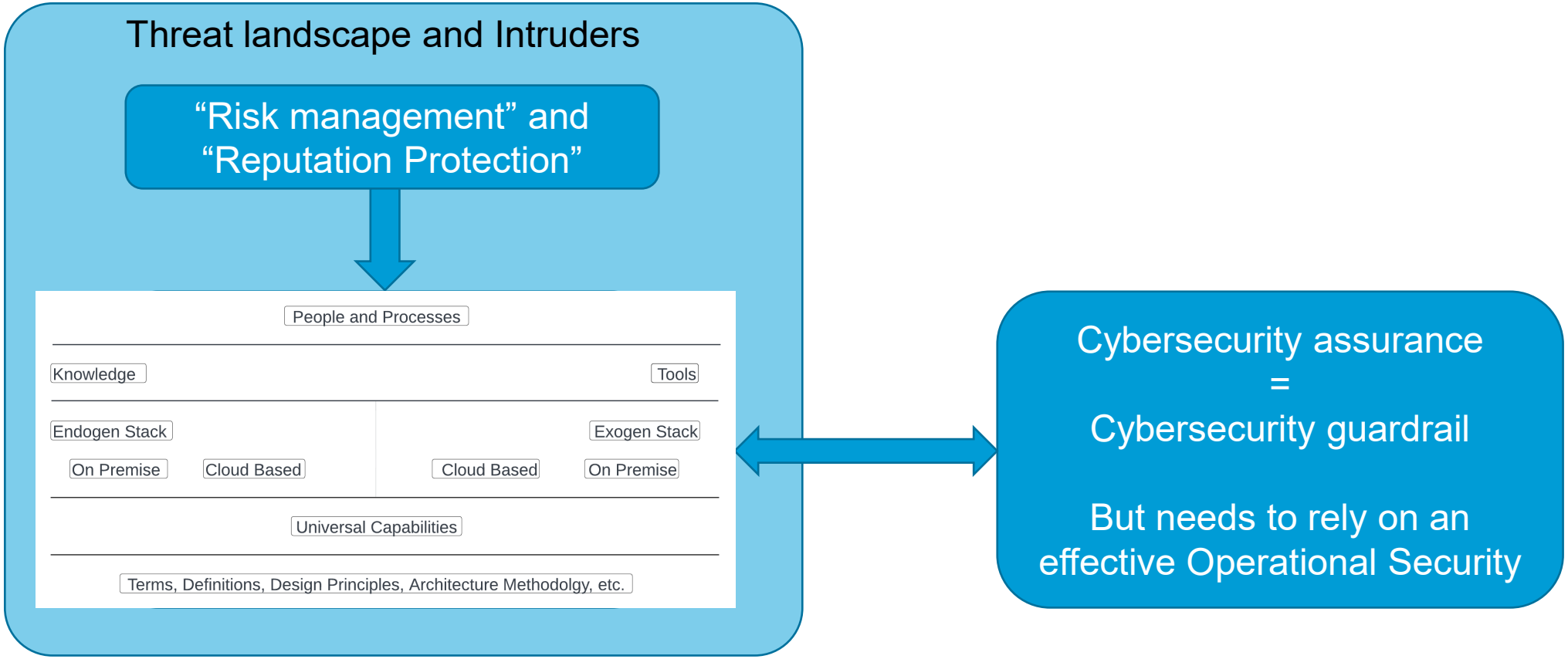
- If yes, then at which cost and at which tradeoffs?
- 30'10" https://www.youtube.com/watch?v=CvcpMfEzkww
- CRA Weakest point being the lack of language on International aspect
- CRA will need a lot of standards …
  - SBOM Annex 1 page 2 (1)
  - Article 19!!!
  - The word standards appears 38 times
    - (w/o annex)!
- ... And we see that are missing a lot of standards
- and MANY other things like something called: MANPOWER

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

Maybe some light in the tunnel



Conclusions

Cybersecurity Assurance is needed to guardrail Cybersecurity itself

Given the current threat landscape AND the paradoxical state of Operational Security it is urgent now

Yet, Cybersecurity Assurance and Operational Security are intricately linked to each other

Operational Security be in a better state would give a better foundation to Cybersecurity Assurance