Upcoming government regulation/certification of hardware, software and services

https://berthub.eu/qpss23.pdf

bert@hubertnet.nl / https://berthub.eu/

Goals

Lots of upcoming and mooted legislation. Goals of this presentation:

- Educational - forewarned is forearmed. Know what is coming
  - Also know how to use this regulation **to our advantage**
- Governments will not create good rules without our input:
  - What are governments thinking?
  - How can we provide technical input?
  - How can we shape the narrative?
- What WOULD be good regulation?
- **Together we can hopefully find ways to reason about this difficult subject**

I hope this session results in something I can blog up with concrete insights gained.

QUESTION: Anything else?

“FEC”:

KIESRAAD

Very sorta “FISA Court”

Toetsingscommissie Inzet Bevoegdheden

POWERDNS

Sorta CIA, MI5/MI6

IETF

TU Delft

FOX-IT
FOR A MORE SECURE SOCIETY

POWERDNS

POWERDNS

“Reverse Engineering the source code of the BioNTech/Pfizer SARS-CoV-2 Vaccine”

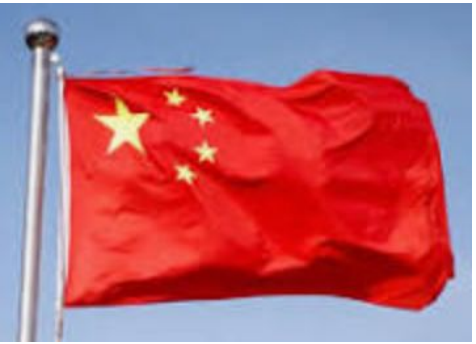
TU Delft

I do not speak on behalf of the Dutch (or any) government!

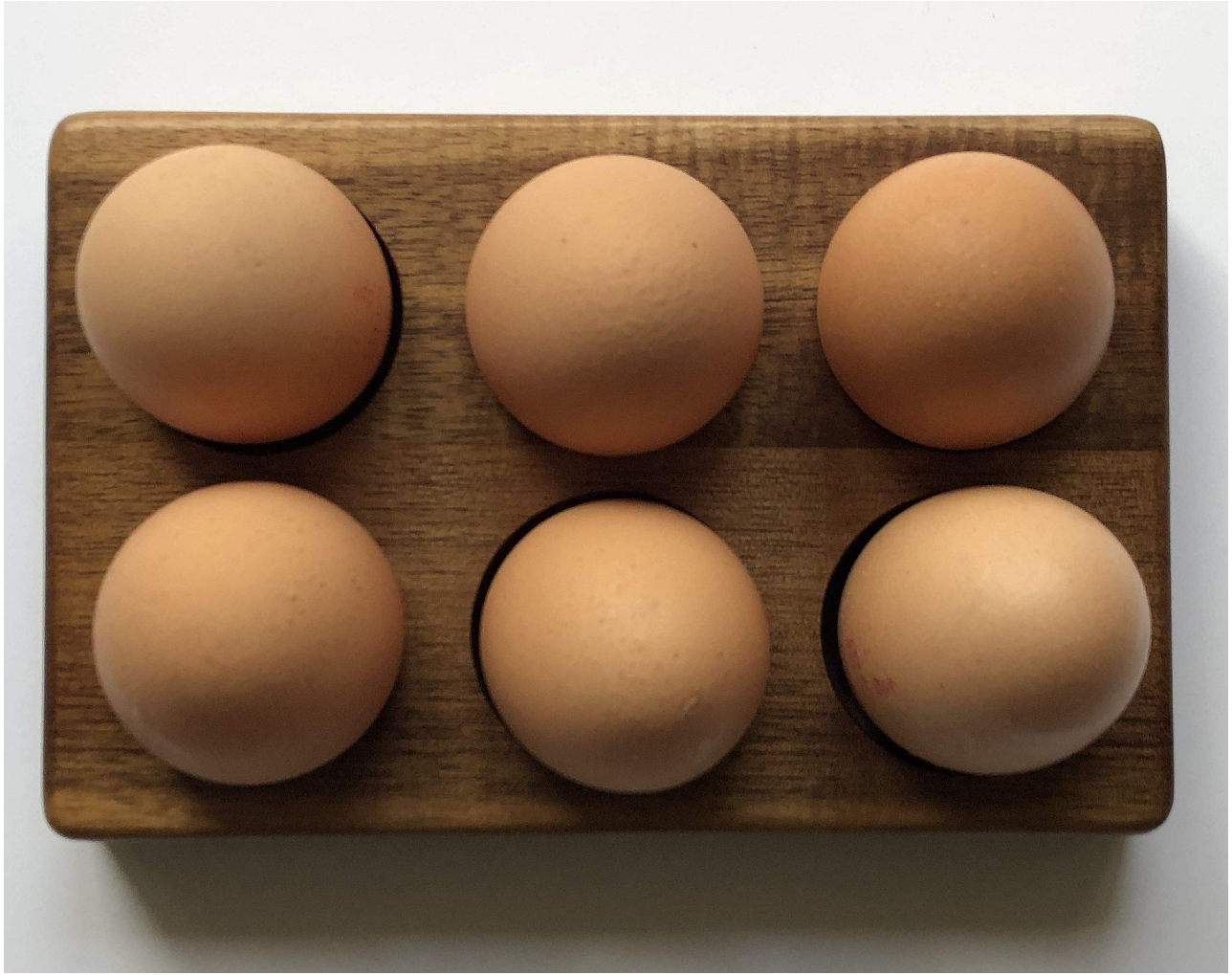

NLUUG
Open systemen
Open standaarden
NLUUG
NLUUG
Open systemen
Open standaarden

Governments are coming to help us make more secure stuff!

“The top 9 most terrifying words in the English Language are: I'm from the government, and I'm here to help” - a famous Californian




>_
1010
1001



Politician’s view: it is like there is a huge arson problem, houses keep burning down

Bring Me The News

Ransomware attack confirmed at Rochester Public Schools, FBI alerted

Yesterday

Star Tribune

Rochester schools confirm district suffered ransomware attack

2 days ago

The Washington Post

Analysis | Influential task force takes stock of progress against ransomware

2 days ago

GIZMODO

Avos Ransomware Gang Hijacks Bluefield's Emergency System

3 days ago

After Dallas Ransomware Attack, Restoration Could Take Time

2 days ago

WNCT

‘Ransomware cult’ claims to have hacked two local schools

9 hours ago

CBS SACRAMENTO

$1.1M paid to resolve ransomware attack on California county

Yesterday

Italian water supplier serving 500,000 people hit with ransomware ...

4 days ago

The New York Times

NEWS ANALYSIS

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

European oil facilities hit by cyber-attacks

By Joe Tidy
Cyber reporter

3 February

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

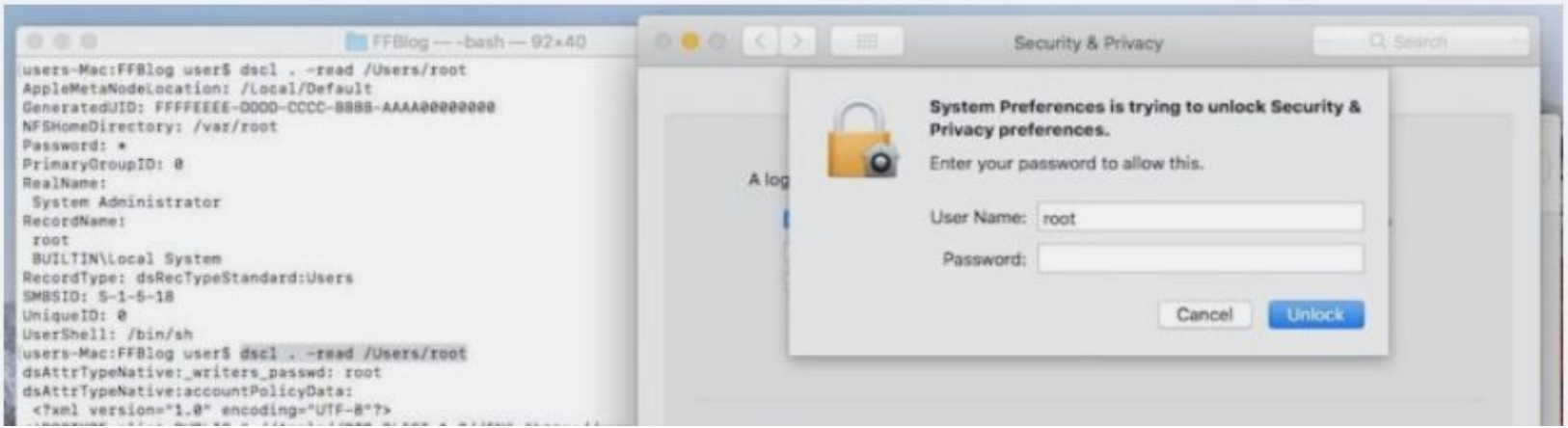
WE feel this has nothing to do with us. Yet policy people see the us declaring stuff like this every day:

MOTHER OF ALL BUGS —

macOS bug lets you log in as admin with no password required

Here's how to protect yourself until Apple patches bafflingly bad bug.

DAN GOODIN - 11/29/2017, 12:05 AM



Slashdot
@slashdot

Apple Patches Dozens of Security Flaws With iOS 15.5, Over 50 Fixes For macOS 12.4

apple.slashdot.org

Apple Patches Dozens of Security Flaws With iOS 15.5, Ov...

Apple has released iOS 15.5, macOS 12.4, and more today with updates like new features for Apple Cash, the Podcast...

12:00 AM · May 17, 2022 · slashdotbot

200 Retweets **20** Quote Tweets **1,447** Likes

CERT-EU

Security Advisory 2022-034

Multiple Critical Vulnerabilities in Microsoft Products

May 17, 2022 — v1.1

TLP:WHITE

History:

- *11/05/2022 — v1.0 – Initial publication*
- *17/05/2022 — v1.0 – Updated with information about issues with Domain Controllers*

Summary

On May 11th, Microsoft issued May 2022 Patch Tuesday including fixes for three zero-day vulnerabilities and 75 flaws. Among the zero-days, the vulnerability tracked as CVE-2022-

We can’t credibly claim things are going well. “Cyber” must become more secure.

“Everything is on fire and we admittedly ship highly flammable products”

Governments are coming for us.

© picture-alliance/dpa/T. Bozuglu

Thanks to BS EN 13772:2011, EN 1021:1994, EN 1021-1, EN 1021-2

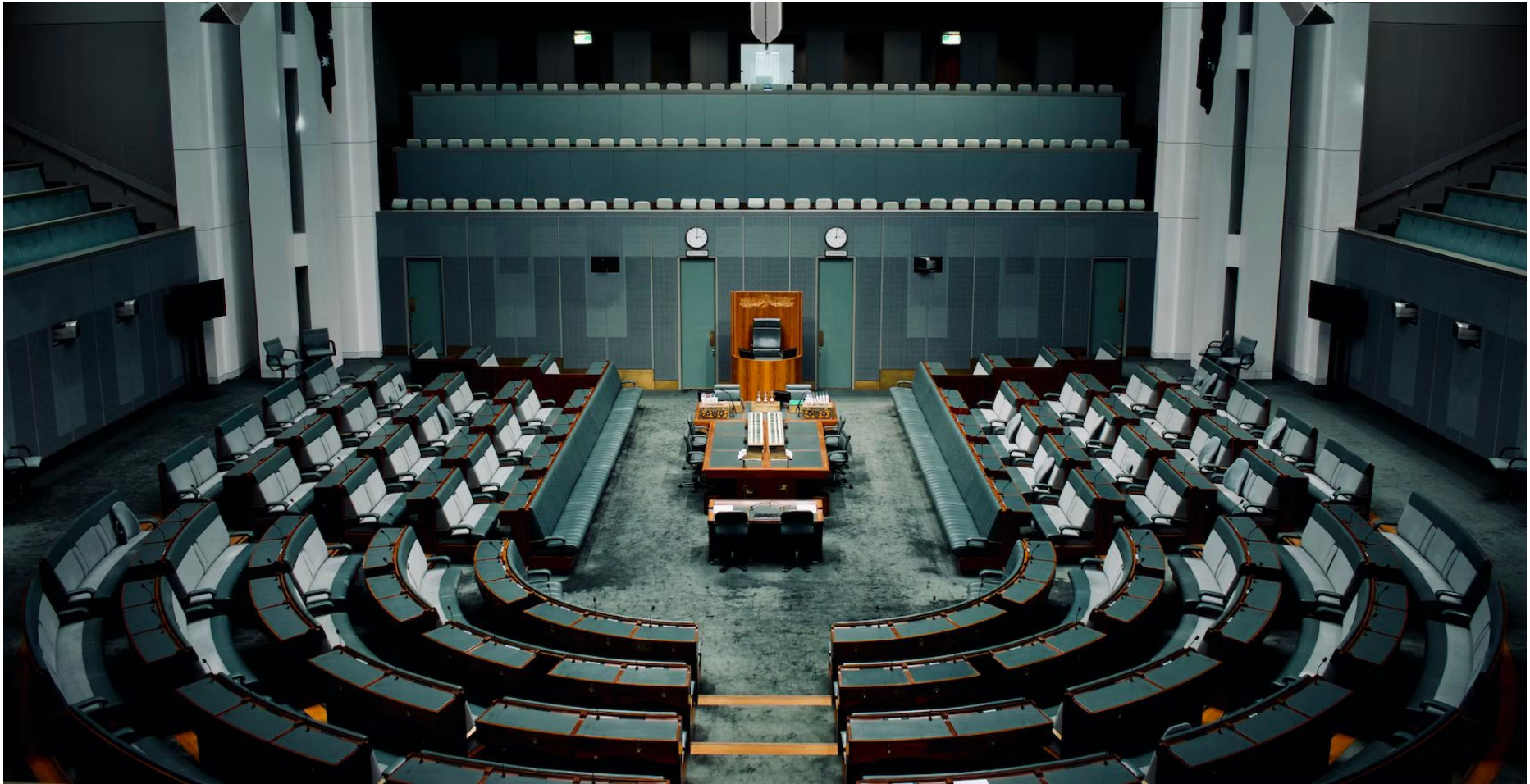
Question: Is the current bad situation the fault of our hardware, software, protocols, algorithms and services? Or are we innocent bystanders?

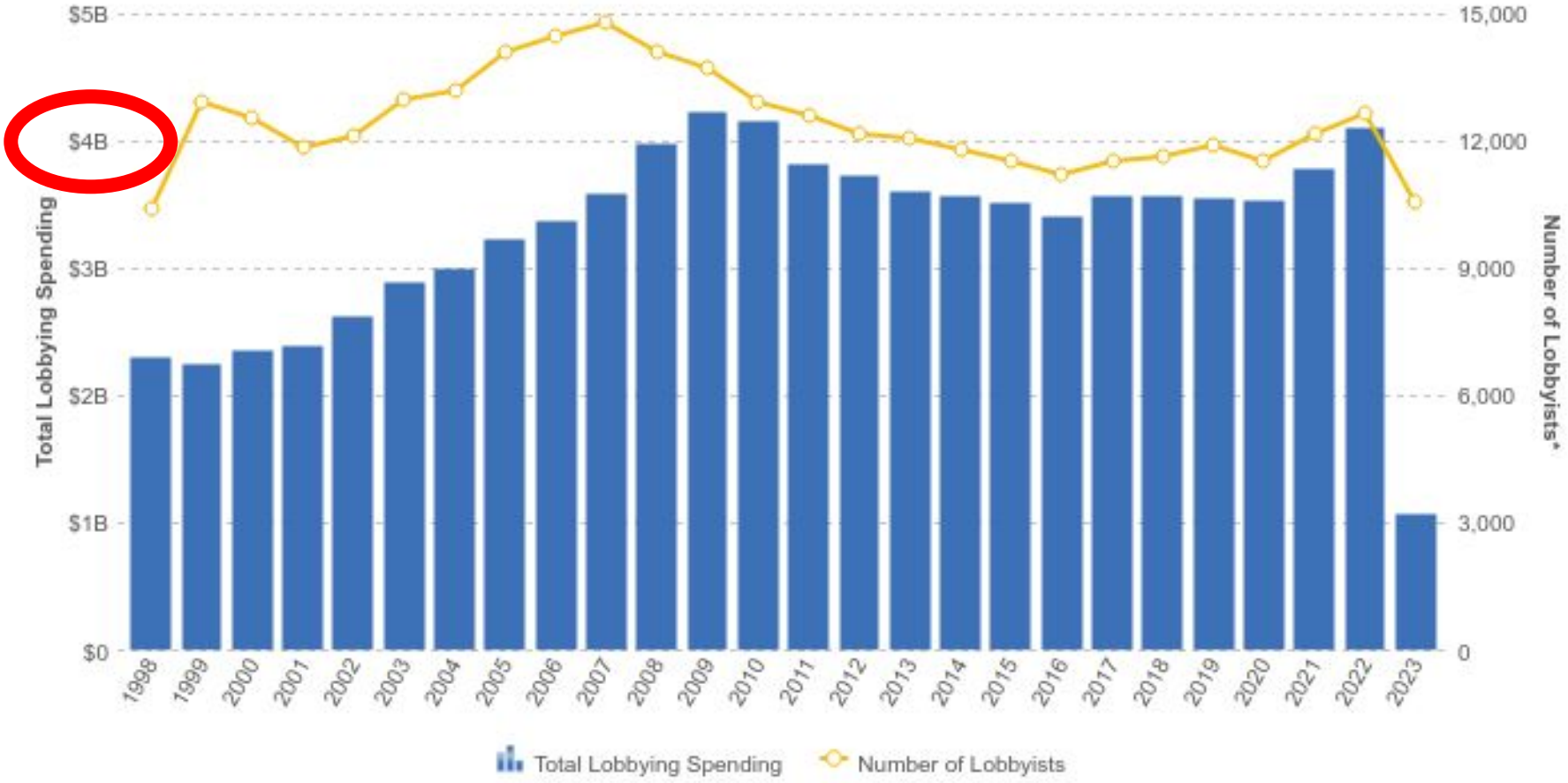
Nevertheless, governments are going to act. “You are supplying flammable materials”

“Get ready for mandatory Rust coding sessions”


RoHS

It isn’t that easy being in government…




$5B
$4B
$3B
$2B
$1B
$0
Total Lobbying Spending
15,000
12,000
9,000
6,000
3,000
0
Number of Lobbyists*
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
Total Lobbying Spending
Number of Lobbyists

“Listen to us please, we know best!”

Regulation!

Known: Vertical regulation of cars, planes, healthcare, spaceflight etc

Current status is that being hacked or shipping incredibly badly protected stuff is somehow allowed

New: horizontal regulation of everything ‘cyber’ or ‘with digital elements’

Three kinds:

- EU Radio Equipment Directive, EU Cyber Resilience Act, UK act: Sorta product legislation, put requirements on hardware **and software**
- EU NIS2, EU Cyber Solidarity Act: Rules on services, continuity, preparedness
- GDPR, CCPA, HIPPA: Rules on data

Interaction!

- Existing vertical regulations get you presumption of conformity in EU CRA
  - Yay
- Complying with NIS2 continuity requirements means having to use EU CRA certified equipment/software
- EU CRA and UK law attempt to “bake in” GDPR into your hardware software: can only log and process data required for **actual operation**

- There may also be some mutual recognition internationally
  - But do not count on it
  - Think of the egg story

“The CLS will be launched as a voluntary scheme to allow time for the market and manufacturers to understand how the scheme benefits them. CSA will monitor the response to the scheme and consider when it will be suitable for the labelling scheme to be made mandatory for IoT consumer devices.”

Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)

The UK’s consumer connectable product security regime will come into effect on 29 April 2024.

From that date, the law will require manufacturers of UK consumer connectable products to comply with minimum security requirements.

These minimum security requirements are based on the UK’s Code of Practice for Consumer IoT security, the leading global standard for consumer IoT security **ETSI EN 303 645**, and on advice from the UK’s technical authority for cyber threats, the National Cyber Security Centre. The regime will also ensure other businesses in the supply chains of these products play their role in preventing insecure consumer products from being sold to UK consumers and businesses.

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimise exposed attack surfaces
7. Ensure software integrity
8. **Ensure that personal data is protected**
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

Question: Isn’t this what everyone should be doing anyhow?

Can we use this to help our management do these useful things?

US National Cybersecurity Strategy 2023
Very early days - broad initiative

Oh boy

What the EU Cyber Resilience Act covers

- Any connected piece of hardware, almost every piece of software sold for money
- Either the producer is compliant, or the importer/distributor/seller has to validate compliance
- Producer is 100% on the hook for its own code
- Must perform due-diligence on sourced components
  - Intensity of due-diligence is variable but now precisely known
- Critical products (definition is not very useful) most undergo third party audits by “notified bodies” (think Tüv etc)
- **Industry must write a standard for compliance, until that time ALL products must undergo third party audits**
  - **(in flux)**

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

GDPR

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

(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;

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

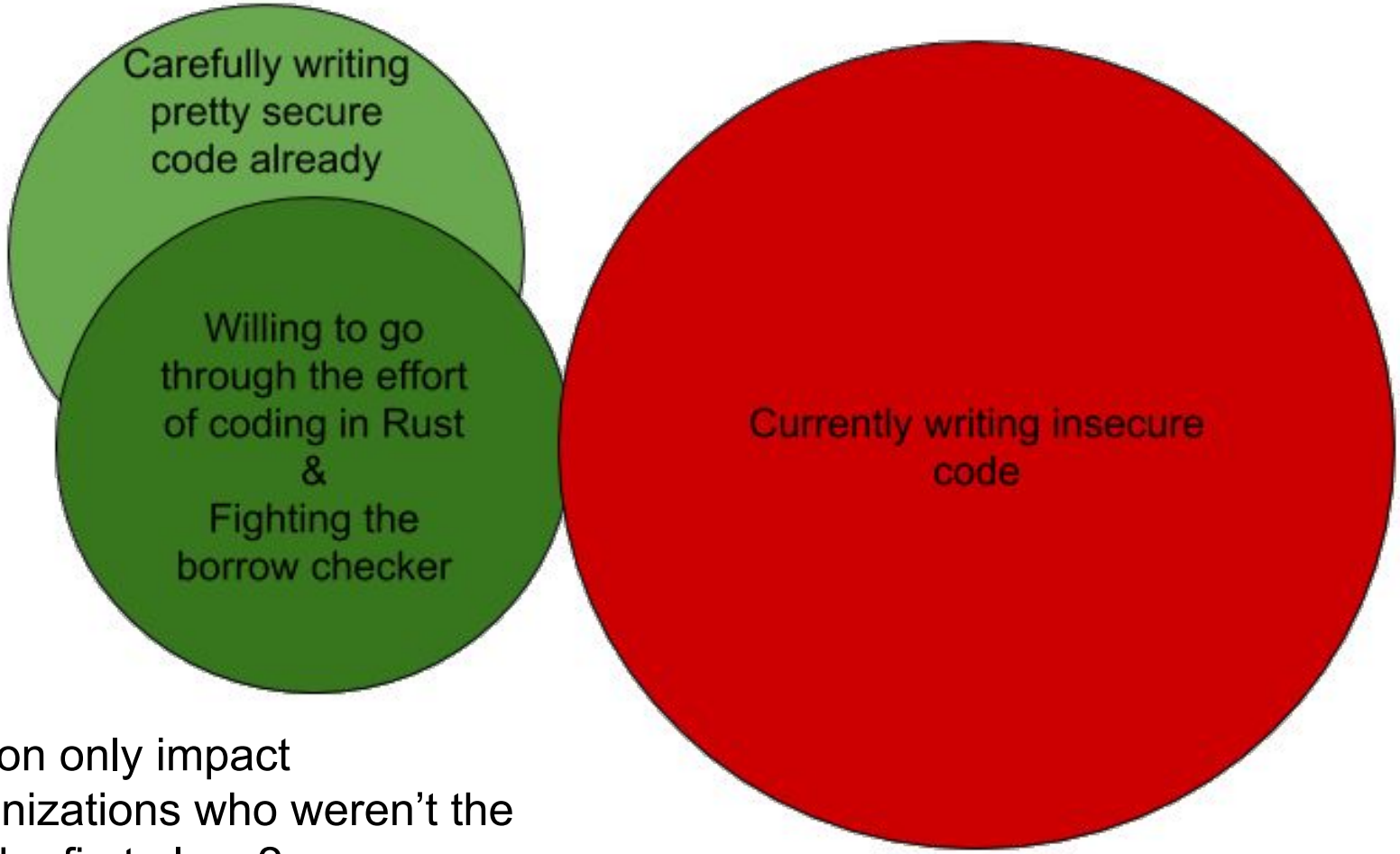
(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Thoughts please



Will regulation only impact people/organizations who weren't the problem in the first place?

Where to regulate?

Whole finished product (“end user SKU”)?

Physical components?

Units of code?

The Open Source Problem

Who does the certification for
OpenSSL? Linux? SQLite?

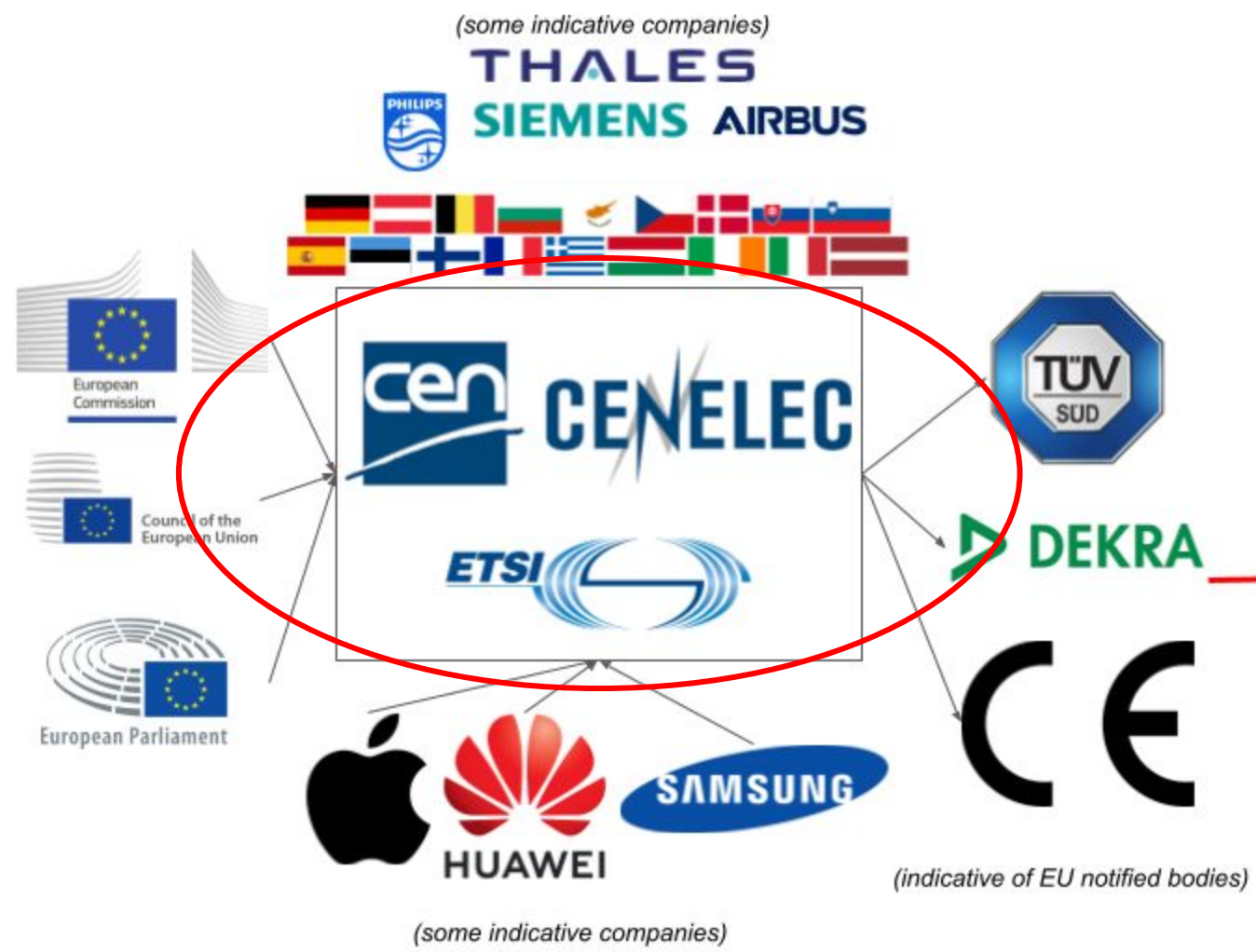
Electron? Android? Jquery? Angular?

Grub?

The Embedded Blob Problem

Would that ever get certified by anyone?

Question: What kind of requirements would make sense?

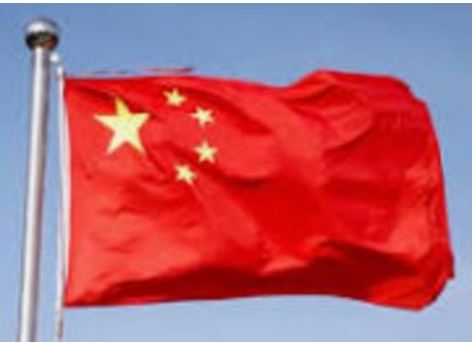


"And this is how you have to code, according to the EU and its harmonised standards organizations, to be checked by EU notified bodies."

International
Organization for
Standardization

Question: Automotive industry has lots of standards, which apply internationally. What can we learn from there in terms of deconfliction?

Question: Are standards organizations nimble enough to effectively regulate “cyber”?



“We are here”

1) Is it going to work?
2) Do we know what to do?
    a) Specifically, how are we as TECHNICAL PEOPLE going to contribute to this process?

Upcoming government regulation/certification of hardware, software and services

https://berthub.eu/qpss23.pdf

bert@hubertnet.nl / https://berthub.eu/