SAVONIA

Introduction to Cybersecurity

Cybersecurity Fundamentals

Markku Kellomäki

Jussi Nivamo

What is cybersecurity?

- Let us first define what we are studying in this course.
- Definition of cyber:
  - https://www.merriam-webster.com/dictionary/cyber

cyber

1 of 2 **adjective**

cy·ber ˈsī-bər
: of, relating to, or involving computers or computer networks (such as the Internet)
the *cyber* marketplace

cyber-

2 of 2 **combining form**

: computer : computer network
*cyber*space

What is cybersecurity?

- Definition of security:
  - https://www.merriam-webster.com/dictionary/security

¬Ž ¬]Ð

ť Ż¬ť

se·cu·ri·ty si-ˈkyu̇r-ə-tı -ˈkyər-

plural **securities**

Synonyms of *security*

1

: the quality or state of being secure: such as
a: freedom from danger : **SAFETY**
b: freedom from fear or anxiety
c: freedom from the prospect of being laid off *job security*

2

a: something given, deposited, or pledged to make certain the fulfillment of an obligation
b: **SURETY**

3

: an instrument of investment in the form of a document (such as a stock certificate or bond) providing evidence of its ownership

4

a: something that secures : **PROTECTION**
b(1): measures taken to guard against espionage or sabotage, crime, attack, or escape
(2): an organization or department whose task is security

Definition of cybersecurity

- There are several different definitions of this term used by different organizations.
- European Union Agency for Cybersecurity (ENISA) has published a paper on the different definitions: https://www.enisa.europa.eu/publications/definition-of-cybersecurity
- It appears that cybersecurity is an umbrella term which covers wide variety of organizations and measures taken against unauthorized or unintended usage, alteration or disclosure of information.

Definition of cybersecurity in dictionaries

3.2 Terminology as defined by dictionaries

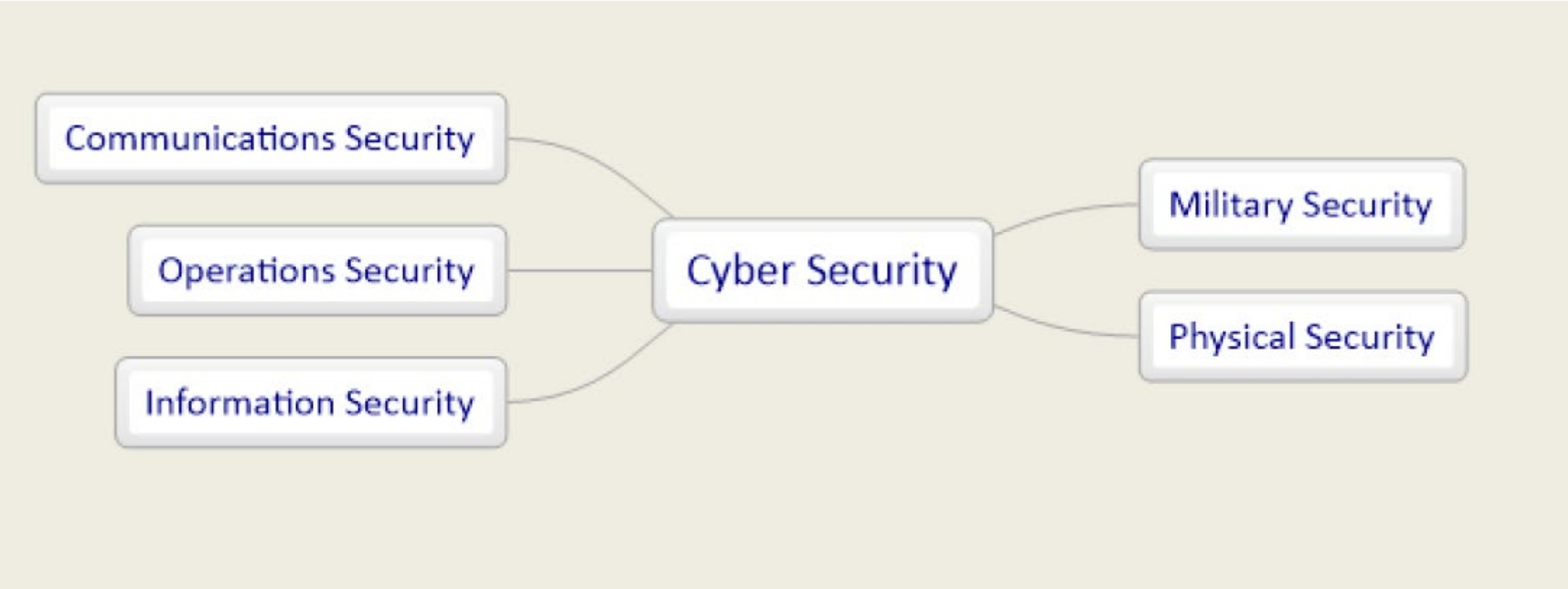
3.2.1 Oxford

The Oxford Dictionaries – Online[6] defines 'cybersecurity' as: *The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.*

3.2.2 Merriam Webster

The Merriam – Webster[7] defines 'cybersecurity' as: *Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*

Domains of cybersecurity



Source: ENISA 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Domains of cybersecurity

Communications Security	Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users.
Operations Security	Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users.
Information Security	Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system.
Physical Security	Protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families.
Public/National Security	Protection against a threat whose origin is from within cyberspace, but may threaten either physical or cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications financial system or other critical public or industrial infrastructures.

Source: ENISA 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Components of term "cybersecurity" for different organizations

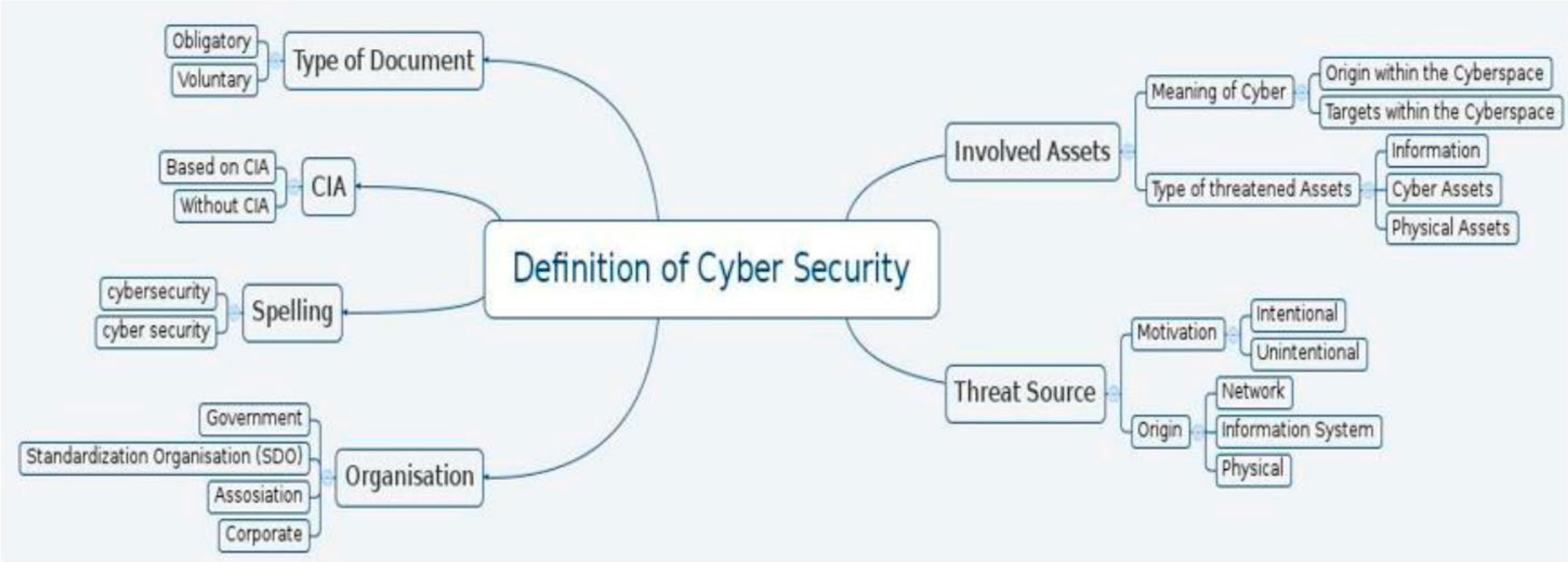
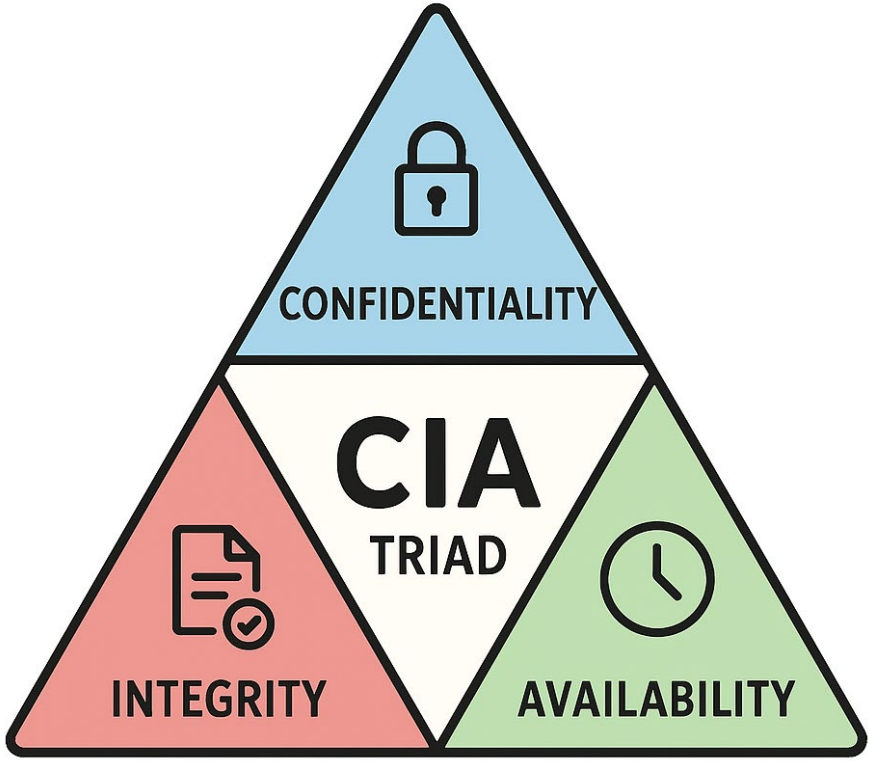


Figure 2: Components constituting the definition of Cybersecurity

Source: ENISA 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity

CIA triad



- **Confidentiality** involves the efforts of an organization to make sure data is kept secret or private
- **Integrity** involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.
- **Availability** involves making sure your data is available when you need it, and it does not take an inordinate amount of time to access it. This means that systems, networks, and applications must be functioning as they should and when they should.

Source: OpenAI (2025) ChatGPT (GPT-5) [Large language model]. https://chat.openai.com/chat

The CIA triad is a common model that forms the basis for the development of security systems.

Meaning of term "cybersecurity" for different organizations

Source: ENISA 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Origin	Document	Spelling	Organization	Type	CIA	Meaning	Motivation	Threat
ISO/IEC JTC1/SC27	27032	Cybersecurity	SDO	V	YES	Only assets intended for the Internet	No differentiation between malicious or unintentional	Only virtual assets connected to the Internet, no physical assets
ISO/IEC JTC1/SC27	27000	Information security	SDO	O[8]	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
ITU-T	X.1205	cybersecurity	Inter-gov	???	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
NIST	SP 800-39	cybersecurity	SDO	V	NO	Risk originating in the Cyber Space ONLY	Only covers malicious origins (cyber attacks)	Only virtual assets connected to the Internet, no physical assets
NATO	National Cyber Security Framework Manual	--	Military	V	NO	Any Risk origination in the Cyber Space (Cyber Threat)	Only covers malicious origins (cyber Threats)	Any asset
Committee on National Security Systems	CNSSI No. 4009	Cyber security	Govt	O	YES	Any Risk	No differentiation between malicious or unintentional	Any asset

Evolution of IoT attacts

- The age of eploration 2005 – 2009
  - Only new features mattered
  - Defence: belief in attacker's ignorance
- The age of eploration 2011 – 2019
  - Attack monetization emerges
  - New security technologies adopted, but inconsistently
- The age of protection 2020 –
  - Connected devices are everywhere ⇔ risks related to cyber incidents have rised
  - Rise of regulation and laws
  - Strong security controls into IoT devices using security frameworks and unified solutions

Evolution of IoT Attacks

- Study the infographic in this link to understand how IoT attacks have evolved: https://www.sectigo.com/uploads/resources/Evolution-of-IoT-Attacks-Interactive-IG_May2020.pdf
- Exercise: explore the type of targets and attacks in different eras of IoT atttacks.
  - How does this relate to your study field at the moment?
  - What do you think will happen in the future with increasing amount of IoT devices?

Focus of this course

- Understand basics of cybersecurity and all aspects having an effect on it.
- Recognize various threats to Internet of Things systems.
  - Labs for stdying attack / defence methods
- Regulatory cybersecurity requirements for products.
- Standards which guide to compliance to requirements.

SAVONIA

Cybersecurity Regulations in European Union

Legal and regulatory response to IoT attacks

- Governments, cybersecurity organizations and standardization bodies have increased creation of laws, regulations, standards and best practice frameworks to defend against cyberattacks
- Climate has changed: consumers, industries and governments demand secure-by-default products and solutions and processes to maintain and improve product security
- European Union has been very active in introducing new laws and regulations:
  - GDPR – date of implementation
  - Cyber Resilience Act – date of implementation
  - Data Act – date of implementation
  - Cybersecurity Act – date of implementation
  - NIS2 – date of implementation
  - RED2 – date of implementation

GDPR – General Data Protection Regulation

- General Data Protection Regulation (GDPR) is EU's main data protection law.
- GDPR protects personal data that relates to and identified or identifiable living individual (data subject) in EU.
- Examples of personal data to be protected (even if it is anonymized / encrypted in a reversible way):
  - a name and surname
  - a home address
  - an email address such as 'name.surname@company.com'
  - an Internet Protocol (IP) address
  - an identification card number
  - a cookie ID
  - the advertising identifier of your phone
  - data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

GDPR – General Data Protection Regulation

- Examples of data that is not considered personal data
  - a company registration number
  - an email address such as 'info@company.com'
  - anonymised data, if anonymisation is irreversible
- Data processing is any operation performed on personal data. It includes the **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination** or otherwise making available, **alignment or combination, restriction, erasure or destruction** of personal data.
- The GDPR protects personal data **regardless of the technology used for processing that data**. It is technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example in an alphabetical order). It also does not matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

GDPR – General Data Protection Regulation

- The principles of personal data processing under the GDPR
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Storage limitation
  - Accuracy
  - Integrity and confidentiality
  - Accountability
- The rights of individuals
  - Right to be informed
  - Right of access
  - Right to rectification
  - Right to erasure
  - Right to restriction of processing
  - Right to data portability
  - Right to object
  - Rights in relation to automated decision-making and profiling

GDPR – General Data Protection Regulation

- The GDPR applies to:
  - A controller or a processor, such as an individual or a private or public organisation, established in the EU which processes personal data as part of its activities, regardless of whether the data is processed in the EU; and
  - A controller or a processor, such as an individual or a private or public organisation, established outside the EU when it is offering goods/services (paid or for free) to individuals in the EU or monitoring the behaviour of individuals in the EU.
- Question for reflection: how does this apply to IoT embedded devices, edge layer and cloud computing?
- Explanation: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en
- Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

EU digital and data statutes

- https://www.traficom.fi/en/communications/data-economy-and-digital-services/eu-digital-and-data-statutes-nutshell

Data Governance Act (DGA)

Digital Services Act (DSA)

Digital Markets Act (DMA)

Data Act (DA)

Artificial Intelligence Act (AIA)

European Regulation on Terrorist Content Online (TCO)

European Data Governance Act: reuse of data

- The Data Governance Act (DGA) regulates the transfer and use of data between organisations. Goal: create value from the data in a safe manner.
- The objective is to promote the freedom of movement and practical use of data. GDPR puts boundaries, however.
- The DGA lays down the prerequisites for the reuse of protected data possessed by the public sector, the provision of data intermediation services, and the operations of ‘data altruism organisations.’ In addition, the DGA launches the operations of the European Data Innovation Board.
- Strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.
- Explanation: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained
- Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868

Data Act: data availability

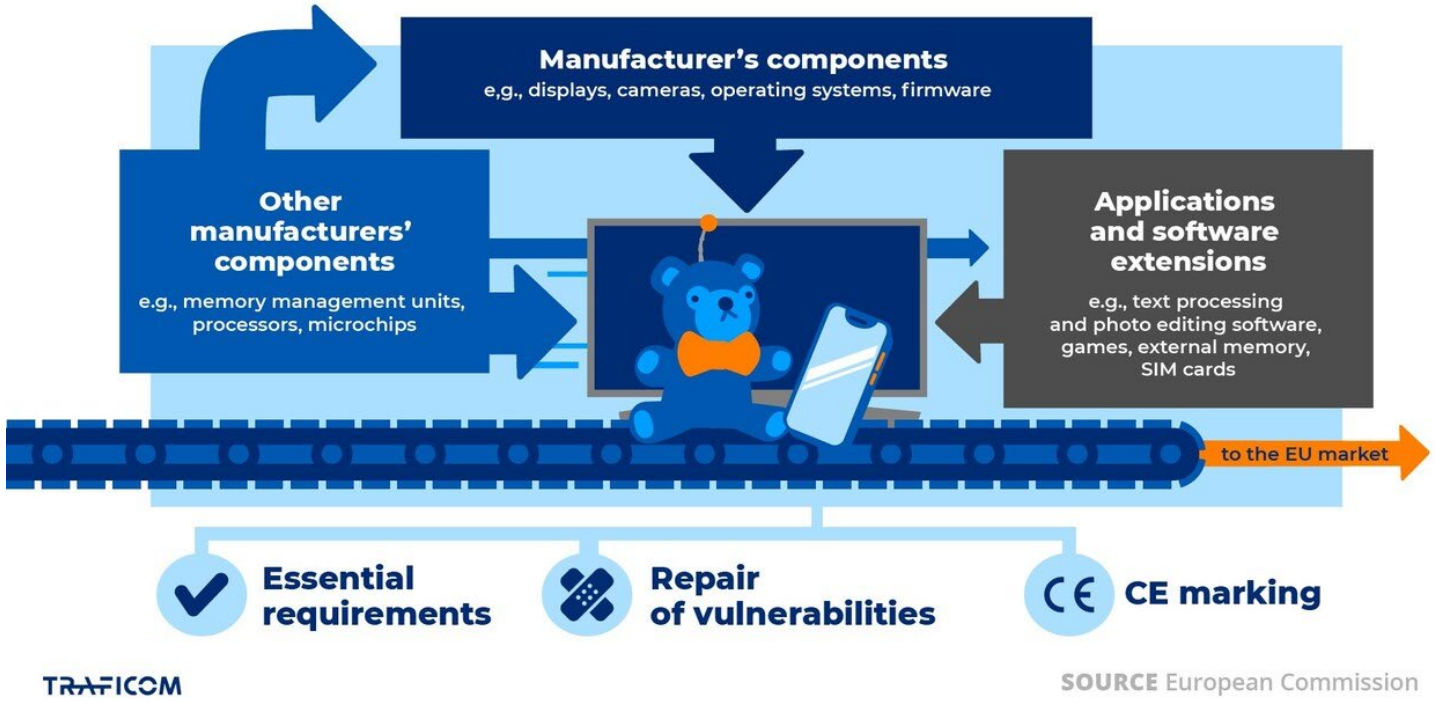
- The Data Act promotes higher data availability and use.
- The Data Act concerns data generated by IoT devices. Such devices include various sensors, smartwatches or even paper machines or airplanes.
- The Data Act obliges manufacturers to design devices in a way that ensures that the user has access to the data generated.
  - The manufacturer shall also disclose device data to a third party
  - In exceptional situations, on the request of a public sector entity.
- The Data Act also aims to make switching data processing services, such as cloud services, easier.
- Explained: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained
- Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854&qid=1740654142201

CRA - Cyber Resilience Act: cybersecurity requirements for products

- Cyber Resilience Act (CRA) explained: https://www.kyberturvallisuuskeskus.fi/en/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra
- CRA is a major shift in EU product requirements ⇔ The age of protection
  - Cybersecurity is now considered as part of CE mark.
  - No product without compliance to CRA is allowed to enter EU market.
  - Similar to EMC and health technology requirements.
  - Aims to stop, for example, spying through baby monitors and organizing DDoS attacks using home appliances.
  - Manufacturers will be responsible for cybersecurity for the entire lifecycle of the product.

CRA - Cyber Resilience Act

- Study the infographic on Traficom page: https://www.kyberturvallisuuskeskus.fi/en/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra



CRA - Cyber Resilience Act

- Applies to: devices or software containing a **digital element** that can be directly or indirectly **connected to another device or to a network**.
  - security cameras, televisions, toys, household routers, firewalls, and games and text processing and photo editing software.
  - operating systems, browsers, password management software and certain microprocessors and microcontrollers.
  - The CRA takes into account the special features of **IoT devices**. The control service typically linked to IoT devices, i.e., the remote data processing solution, which is under the responsibility of the manufacturer, is considered part of the product.
  - A cloud solution or a component used in it falls within the scope of the regulation if it meets the definition for a remote data processing solution laid down in the regulation and its development has been the responsibility of the product manufacturer.
- Does not apply to: medical devices, in vitro diagnostic medical devices, certain vehicles, marine equipment and aviation certified devices (cybersecurity already covered by other regulations), national security and defense.

CRA - Cyber Resilience Act

- Essential cybersecurity requirements: for example
  - Secure default settings and automatic security updates
  - Prevention of unauthorised access
  - Confidential storage of data and minimisation of data
  - Securing of key functionalities
- Reporting of vulnerabilities
  - Manufacturers of products placed on the EU market **must report any actively exploited vulnerabilities** contained in the product to the CSIRT and ENISA.
  - They must also inform the users of the products of possible vulnerabilities and of the ways of repairing them.
  - There are strict deadlines for reporting: within 24 hours of detecting vulnerability

CRA - Cyber Resilience Act

- Product categories: different requirements (source: https://www.kyberturvallisuuskeskus.fi/en/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra)

	Default category	Important products Class 1	Important products Class 2	Critical products ↓
Example products	Smart loudspeakers, hard disks, photo editing software, games	Routers, browsers, smart home products, wearable smart products, smart toys (Annex III)	Solutions for virtualisation, firewalls, tamper-resistant processors (Annex III)	Security box, smart meter gateway (Annex IV)

- Takes full effect in 12/2027
- Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

Cybersecurity Act

- The EU Cybersecurity Act grants a permanent mandate to ENISA (https://www.enisa.europa.eu/), the EU Agency for cybersecurity, and gives it more resources and new tasks.
  - European Union Agency for Network and Information Security (ENISA)
  - Helps to Member States in developing national CSIRTs (Computer Security Incident Response Team)
  - Finnish CSIRT: National Cyber Security Centre Finland https://www.kyberturvallisuuskeskus.fi/en
- The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes.
- Explanation: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

NIS2 directive

- Network and Information Security (NIS) directive was updated in 2022.
- The aim of the NIS2 Directive is to ensure a common level of cyber security in the whole European Union.
  - obligations that require Member States to adopt **national cybersecurity strategies** and to designate or establish competent **authorities**
  - cybersecurity risk-management measures and reporting obligations for **entities of critical sectors** ⇔ **sanctions for non-compliance!**
  - rules and obligations on cybersecurity **information sharing**
  - **supervisory and enforcement obligations** on Member States.
- Explanation:
  - https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/nis2-european-union-cybersecurity-directive
  - https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1740663270893

NIS2 directive affected sectors

- Essential Entities (Sectors of High Criticality)
  - Energy – Electricity, District Heating and Cooling, Oil, Gas, Hydrogen
  - Transport – Air, Rail, Water, Road
  - Banking
  - Financial Market Infrastructures
  - Health
  - Water – Drinking Water, Waste Water
  - Digital Infrastructure
  - ICT Service Management (B2B)
  - Public Administration
  - Space
- Important Entities (Other Critical Sectors)
  - Postal and Courier Services
  - Waste Management
  - Manufacture, Production and Distribution of Chemicals
  - Production, Processing and Distribution of Food
  - Manufacturing – Medical Devices, Computer Electronic or Optical Products, Machinery, Vehicles
  - Digital Providers
  - Research
- Companies of medium size or above are required to achieve NIS2 compliance

NIS2 directive measures

- Measures mandated by NIS2 for essential and important entities:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

- National cybersecurity organizations and cooperation
  - CSIRT (Kyberturvalllisuuskeskus), EU-wide CSIRT network, ENISA collaboration

RED – Radio Equipment Directive

- RED establishes a regulatory framework for placing radio equipment on the market.
  - essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum.
- New update: increase the level of cybersecurity, personal data protection and privacy.
- Explanation: https://huld.io/blog/the-radio-equipment-directive-red-update-everything-you-need-to-know/
- Updates coming in 2025: https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

SAVONIA

Finnish criminal code on cyber attacks and related criminal activities

Finnish Criminal code

- https://www.finlex.fi/en/legislation/translations/1889/eng/39-001
- Chapter 28
  - Section 7 (769/1990)

Unauthorised use

A person who without authorisation uses the movable property or the immovable machinery or equipment of another person shall be sentenced for unauthorised use to a fine or to imprisonment for at most one year.

An attempt is punishable.

The use of an internet connection through an unprotected wireless computer network is not deemed unauthorised use. (190/2011)

Finnish Criminal code

- Chapter 28
  - Section 8 (769/1990)

Aggravated unauthorised use

If, in unauthorised use,

1) considerable economic benefit is sought, or

2) particularly significant damage or harm is caused to the victim of the offence, taking into consideration the victim's circumstances,

and the unauthorised use is also aggravated when assessed as a whole, the perpetrator shall be sentenced for aggravated unauthorised use to a fine or to imprisonment for at most two years.

An attempt is punishable.

Finnish Criminal code

- Chapter 34
  - Section 9a (368/2015)

Endangerment of data processing

A person who, in order to cause harm or damage to data processing or to the functioning or security of an information system or a communications system,

1) imports, acquires for use, manufactures, sells or otherwise disseminates or makes available

a) a device, a computer programme or a set of programming instructions designed or modified to endanger or damage data processing or the functioning of an information system or a communications system or to decode or disable the technical protection of electronic communications or the protection of an information system, or

b) an information system password, access code or other equivalent information belonging to another, or

2) disseminates or makes available instructions for the manufacturing of a computer programme or a set of programming instructions referred to in paragraph 1

shall, unless an equally or more severe punishment for the act is provided elsewhere by law, be sentenced for endangerment

Finnish Criminal code

- Chapter 34
  - Section 9b (540/2007)

Possession of a data system offence device

A person who, in order to cause harm or damage to data processing or to the functioning or security of an information system or a communications system, possesses a device, a computer programme or a set of programming instructions referred to in section 9a, paragraph 1, subparagraph a, or a password, access code or other equivalent information referred to in subparagraph b shall be sentenced for possession of a data system offence device to a fine or to imprisonment for at most six months.

Finnish Criminal code

- Chapter 35
  - Section 3a (368/2015)

Criminal damage to data

A person who, to cause damage to another, unlawfully destroys, demolishes, hides, damages, alters, renders unusable or conceals data recorded on an information device or another recording or data contained in an information system, shall be sentenced for criminal damage to data to a fine or to imprisonment for at least two years.

An attempt is punishable.

Finnish Criminal code

- Chapter 35
  - Section 3b (368/2015)

Aggravated criminal damage to data

If criminal damage to data

1) causes particularly significant harm or economic loss,

2) is committed as part of the activities of an organised criminal group referred to in chapter 6, section 5, subsection 2, (564/2015)

3) is committed as part of activities that have affected a significant number of information systems, by using a device, a computer programme or a set of programming instructions referred to in chapter 34, section 9a, paragraph 1, subparagraph a, or a password, access code or other equivalent information referred to in subparagraph b, or

4) is directed at an information system, the damaging of which would endanger the energy supply, public healthcare, national defence, administration of justice or another comparable important societal function,

and the criminal damage to data is also aggravated when assessed as a whole, the perpetrator shall be sentenced for aggravated criminal damage to data to imprisonment for at least four months and at most five years.

An attempt is punishable.

Finnish Criminal code

- Chapter 38
  - Section 3 (368/2015)

Violation of the secrecy of communications

A person who unlawfully

1) opens a letter or another closed message addressed to another person or, by decoding the protection, obtains information on the contents of a message stored electronically or by other technical means that is protected against third parties, or

2) obtains information on the contents of a telephone call, a telegram, transmission of text, images or data, or another equivalent telecommunications message transmitted in a telecommunications network or an information system or on the transmission or reception of such a message

shall be sentenced for a violation of the secrecy of communications to a fine or to imprisonment for at most two years.

An attempt is punishable.

Finnish Criminal code

- Chapter 38
  - Section 4 (578/1995)

Aggravated violation of the secrecy of communications

If, in a violation of the secrecy of communications,

1) the perpetrator commits the offence by making use of his or her position in the service of a telecommunications operator referred in the Act on the Protection of Privacy in Electronic Communications (516/2004) or another special position of trust, (517/2004)

2) the perpetrator commits the offence by making use of a computer programme or special technical device designed or altered for such purpose, or otherwise in a particularly premeditated manner, or

3) the contents of the message that is the object of the offence are particularly confidential or the act constitutes a grave violation of the protection of privacy,

and the violation of the secrecy of communications is also aggravated when assessed as a whole, the perpetrator shall be sentenced for an aggravated violation of the secrecy of communications to imprisonment for at most three years.

An attempt is punishable.

Finnish Criminal code

- Chapter 38
  - Section 7a (368/2015)

Interference with an information system

A person who, in order to cause harm or economic loss to another person, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious disturbance to it shall be sentenced for interference with an information system to a fine or to imprisonment for at most two years.

Finnish Criminal code

- Chapter 38
  - Section 7b (368/2015)

Aggravated interference with an information system

If, in interference with an information system,

1) particularly significant harm or economic loss is caused,

2) the offence is committed in a particularly premeditated manner,

3) the offence is committed as part of activities that have affected a significant number of information systems through the use of a device, a computer programme or a set of programming instructions referred to in chapter 34, section 9a, paragraph 1, subparagraph a, or a password, access code or other equivalent information referred to in subparagraph b,

4) the offence is committed as part of the activities of an organised criminal group referred to in chapter 6, section 5, subsection 2, or (564/2015)

5) the offence is directed at an information system, the damaging of which would endanger the energy supply, public healthcare, national defence, administration of justice or another comparable important societal function,

and the interference with an information system is also aggravated when assessed as a whole, the perpetrator shall be sentenced for aggravated interference with an information system to imprisonment for at least four months and at most five years.

An attempt is punishable.

Finnish Criminal code

- Chapter 38
  - Section 8 (368/2015)

Unlawful access to an information system

A person who unlawfully, by using an access code that does not belong to him or her or by otherwise breaking the security system of an information system, accesses an information system where information or data is processed, stored or transmitted electronically or in another equivalent technical manner, or a separately protected part of such a system, shall be sentenced for unlawful access to an information system to a fine or to imprisonment for at most two years.

A person who, without accessing an information system or a part of it,

1) by using a special technical device or

2) by using other technical means to by-pass the security system, by taking advantage of a vulnerability in the information system, or otherwise by manifestly fraudulent means,

unlawfully obtains information or data contained in an information system referred to in subsection 1 shall also be sentenced for unlawful access to an information system.

An attempt is punishable.

This section only applies to acts for which an equally or more severe punishment is not provided elsewhere by law.

Finnish Criminal code

- Chapter 38
  - Section 8a (368/2015)

Aggravated unlawful access to an information system

If unlawful access to an information system is committed

1) as part of the activities of an organised criminal group referred to in chapter 6, section 5, subsection 2, or (564/2015)

2) in a particularly premeditated manner,

and the unlawful access to an information system is also aggravated when assessed as a whole, the perpetrator shall be sentenced for aggravated unlawful access to an information system to a fine or to imprisonment for at most three years.

An attempt is punishable.

Finnish Criminal code

- Chapter 38
  - Section 8b (919/2014)

Offence involving a protection decoding system

A person who, in violation of the prohibition laid down in section 269, subsection 2 of the Information Society Code (917/2014), for gain or so that the act is conducive to causing significant harm or damage to a provider of protected services, manufactures, imports, offers for sale, leases or distributes a protection decoding system, or advertises, installs or maintains one shall, unless a more or equally severe punishment for the act is provided elsewhere by law, be sentenced for an offence involving a protection decoding system to a fine or to imprisonment for at most one year.

Finnish Criminal code

- Chapter 38
  - Section 9 (1051/2018)

Data protection offence

A person who, in a capacity other than that of a controller or a processor referred to in Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the General Data Protection Regulation, intentionally or through gross negligence acquires personal data in a manner that is incompatible with their purpose, discloses personal data, or transfers personal data

in violation of a provision on the purpose limitation, disclosure or transfer of personal data laid down in

1) the General Data Protection Regulation,

2) the Data Protection Act (1050/2018),

3) the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018), or

4) another act concerning the processing of personal data,

and thus violates the protection of privacy of a data subject or causes a data subject other damage or essential harm, shall be sentenced for a data protection offence to a fine or to imprisonment for at most one year.

A person who intentionally or through gross negligence acts in violation of the provisions on the security of the processing of personal data laid down in the statutes referred to in subsection 1, paragraphs 1–4 shall also be sentenced for a data protection offence.

SAVONIA

Standards

Why we need standards for cybersecurity?

- Regulations set the expectations for cybersecurity, but they do not tell how to reach those expectations.
- Many regulations mention standards to be developed but EU officials do not develop them
  - Standardization organizations like ISO do them.
- As an example let us take a look at of Cyber Resilience Act (CRA) mapping to standards:
  - https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

CRA requirements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) Products with digital elements shall:

- (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;

CRA requirements

(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'**);

(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.

Mapping to standards

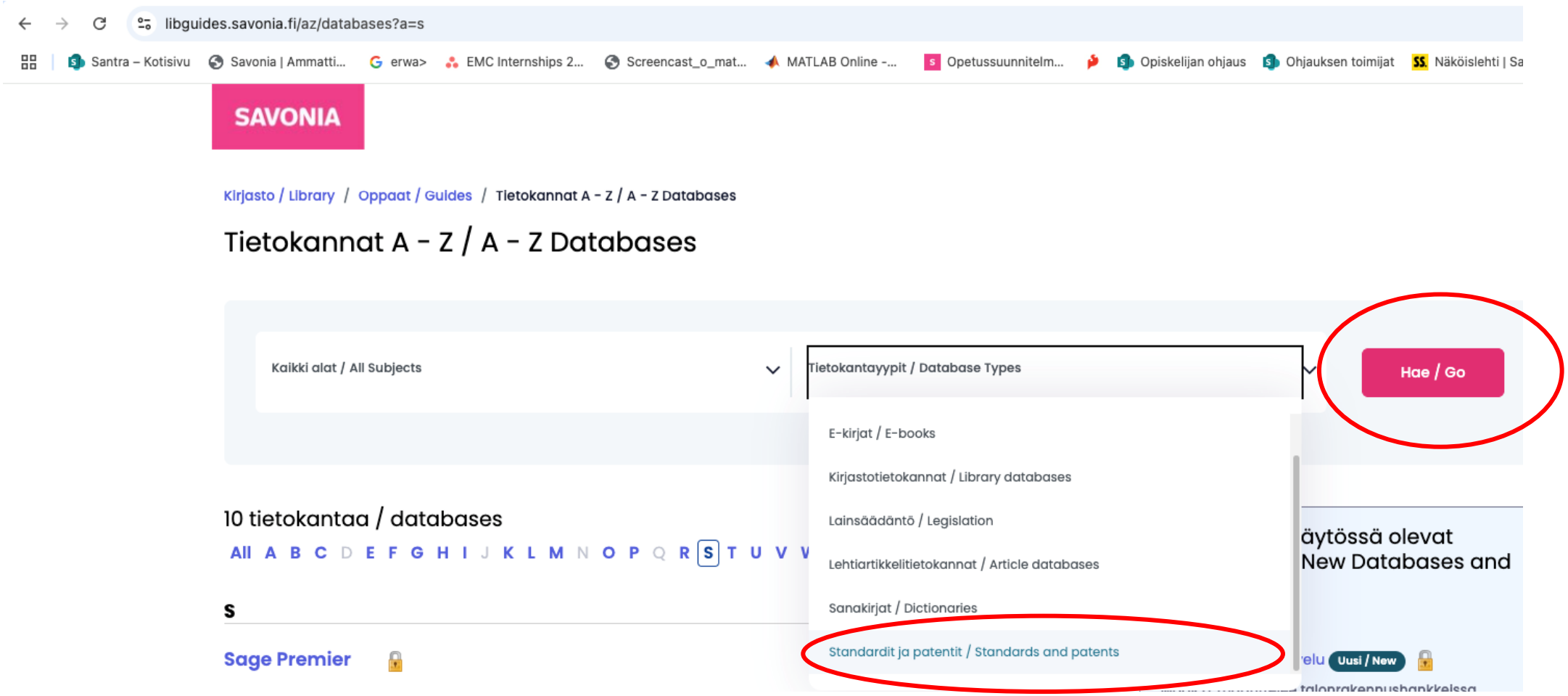
- Full tables available in the original document (source: https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping).
- This kind of mapping gives a starting point for studying and applying the standards.

	Security requirements relating to the properties of products with digital elements												
Standard	**1**	**2**	**3 a**	**3 b**	**3 c**	**3 d**	**3 e**	**3 f**	**3 g**	**3 h**	**3 i**	**3 j**	**3 k**
EN ISO/IEC 27002:2022	x		x					x			x	x	x
EN ISO/IEC 27005:2022	x												
EN IEC 62443-3-2:2020	x										x		
EN IEC 62443-4-1:2018	x	x											
ISO/IEC 18045:2022		x									x		
ITU-T X.1214 (03/2018)		x											
ETSI EN 303 645 V2.1.1 (2020-06)	x	x	x	x	x	x	x	x	x	x	x	x	x
ISO/IEC 18031:2011			x										
ISO/IEC 9798 Parts 1 to 6				x									

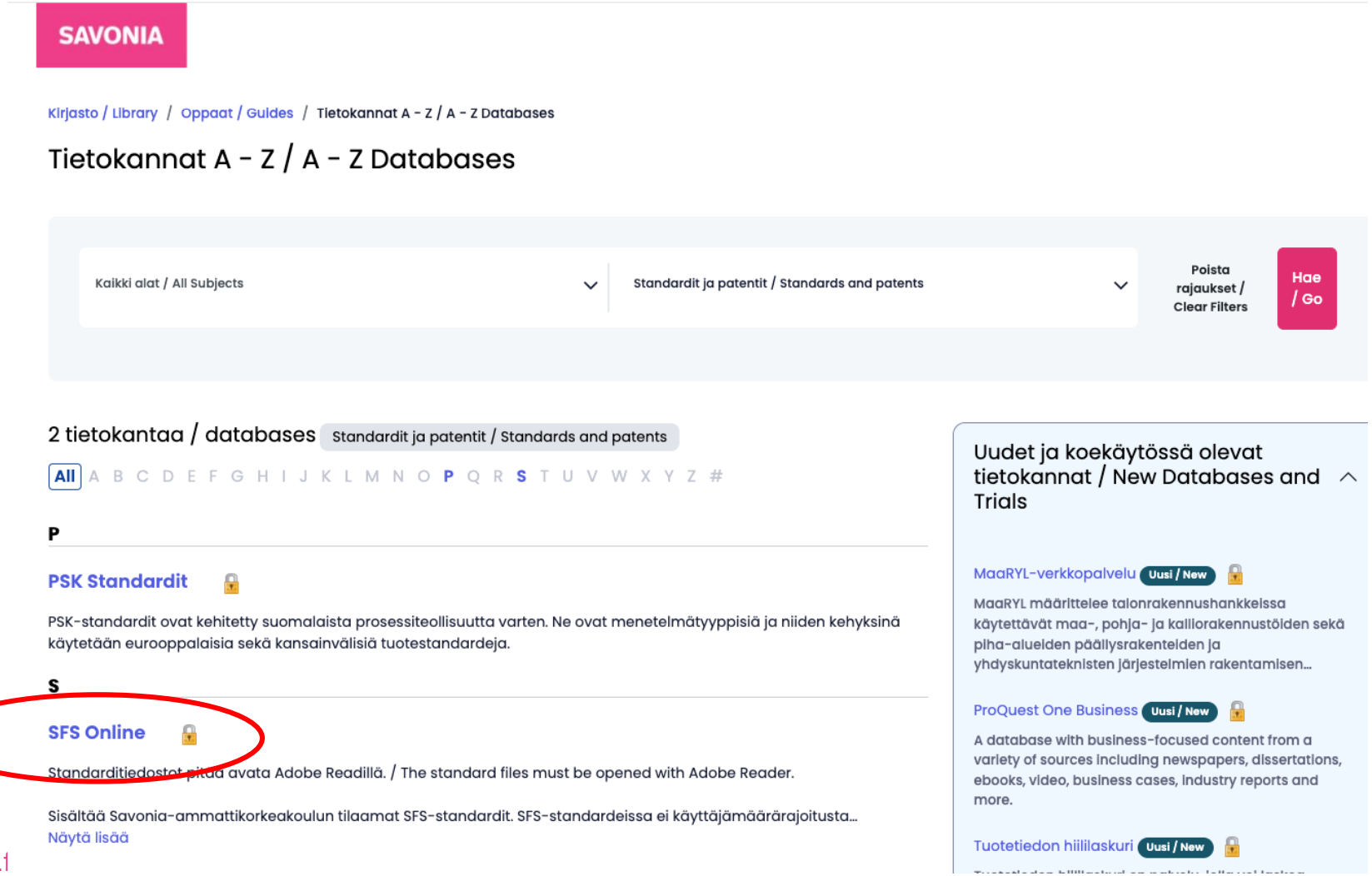
Links to standards relevant to CRA

- Standards available in Savonia library: https://libguides.savonia.fi/az/databases?a=s
  - EN ISO/IEC 27001: 2022
  - EN ISO/IEC 27002: 2022
  - EN ISO/IEC 27005: 2022
  - ISO/IEC TS 19249:2017
  - ISO/IEC 15408-2:2022
  - ISO/IEC 27036-1:2023
  - ISO/IEC 27036-2:2023
  - ISO/IEC 27036-3:2023
  - ISO/IEC 30111: 2020
- Links to other standards:
  - ETSI EN 303 645 V2.1.1 (2020-06): https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
  - ITU-T X.1214 (03/2018): https://www.itu.int/rec/T-REC-X.1214-201803-I/en

How to access standards in Savonia system



Access SFS Online



Search using number of ISO / IEC standard