ISSN 1831-9424

European Commission

# An ontology of health impacts and value chain enablers of digital health solutions

*Towards a toolbox for characterising cyber incidents in health*

Reina, V., Griesinger, C.B.

2024

Joint Research Centre

EUR 40160

**Contact information**
Name: Vittorio Reina
Address: Via E. Fermi, 2749 I – 21027 Ispra (VA) ITALY
Email: vittorio.reina@ec.europa.eu
Tel.: +39 0332 78 3638

**EU Science Hub**
https://joint-research-centre.ec.europa.eu

JRC139910

EUR 40160

PDF ISBN 978-92-68-23020-6 ISSN 1831-9424 doi:10.2760/7823548 KJ-01-24-213-EN-N

Luxembourg: Publications Office of the European Union, 2024



How to cite this report: European Commission: Joint Research Centre, Reina, V. and Griesinger, C.B., *An ontology of health impacts and value chain enablers of digital health solutions,* Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2760/7823548, JRC139910.

# Content

Abstract ..... 3
1 Introduction ..... 5
2 Specific context of this ontology: a toolbox for cyber incident characterisation ..... 10
3 An ontology of concepts supporting cyber incident characterisation: premises, methods and information sources ..... 13
4 The four ontology categories ..... 16
4.1 Ontology category 1: cybersecurity ..... 16
4.2 Ontology category 2: Enabling IT infrastructure ..... 32
4.3 Ontology category 3: Enabling technologies ..... 35
4.4 Ontology category 4: Health impacts ..... 45
4.5 Schematic illustration of categories and key concepts of the ontology ..... 52
5 Conclusion ..... 55
References ..... 56
List of abbreviations and definitions ..... 59
List of figures ..... 61
List of tables ..... 62
Annexes ..... 63
Annex 1. List of concepts in alphabetical order ..... 63

## Abstract

Cyber attacks on healthcare settings increase in frequency and magnitude. They cause significant damage to infrastructures, compromising both continuity and quality of services. Accordingly, policy makers recognise cyber attacks as a growing public health problem (e.g. von der Leyen, 2024). Its urgency will increase due to the accelerating digitisation of healthcare and roll-out of AI-enabled and connected devices. Apart from causing significant economic damage, cyber attacks can cause harm to patients by delaying diagnosis and treatment or interrupting emergency services, leading to adverse health outcomes, e.g. illness, impairment or death. Yet, the severity of this problem is presently not fully known: available data are sparse or contradictory. There is currently no comprehensive and consistent framework for generating reliable data on cyber incident characteristics that would enable collaboration across the value chain. Here we propose a foundational ontology of categories of concepts that we consider part of the value chain of digital and AI-enabled health solutions. This ontology is part of a forthcoming framework for cyber incident characterisation including causal links to adverse health outcomes. The ontology consists of a systematic structure of concepts on 1) general cybersecurity, 2) IT infrastructure, 3) enabling technologies. As a fourth category we include health impacts in order to support causality inquiries between cyber attacks and what happened to the most vulnerable party of a cyber attack, the patients.

## Acknowledgements

We gratefully acknowledge the contribution of Igor Nai-Fovino (EC Joint Research Centre, Cybersecurity and Digital Technologies Unit) who provided valuable advice on general cybersecurity aspects and issues of terminology and wording.

We would also like to express our gratitude to the colleagues of the International Medical Device Regulators Forum (IMDRF) Adverse Event Working Group and in particular Nancy Pressly for agreeing to use Annex F of the IMDRF adverse event terminology as the basis for capturing relevant health impacts that may result from cyber security incidents in health settings.

***Authors***

Vittorio Reina

Claudius Griesinger

# 1 Introduction

***Cyber incidents in healthcare: an increasing public health problem***

The healthcare sector is experiencing an increasing number of cyber attacks: various data sources reveal the alarming trend of healthcare being one of the most vulnerable industries to cyber attacks, with a drastic surge in the rate of cyber incidents over a short span of years. Our recent study screening the frequency and nature of cyber attacks over one year, with a particular focus on reporting of health effects, confirmed this trend (Reina and Griesinger, 2024). Similar findings were presented by ENISA in 2023. Importantly, the increasing digitisation of healthcare and the expected increasing rollout of AI-enabled solutions (AI-enabled medical devices software either as software *as* or *in* a medical device), will only exacerbate this considerable public health problem. This has been recognised by policy makers. For instance, the EU's Commission president indicated that a plan would be swiftly developed for enhancing cyber resilience of healthcare settings (von der Leyen, 2024).

***Specific healthcare-related dimensions: data, multitude of connected devices, health impacts***

Typically, cyber attacks (e.g. ransomware) lead to the temporary suspension and deterioration of healthcare services by relevant settings (e.g. hospitals, clinics). They require high human and financial resources to restore healthcare delivery to its pre-attack levels and to investigate causes, vulnerabilities and whether and to which extent digital infrastructure has been damaged.

However, additional to service interruptions, cyber attacks can have serious health effects due to the specifics of the healthcare sector. Healthcare heavily depends on and deals with sensitive personal data and employs a great number of individual devices and products connected to each other as well as to cloud services, hospitals and other networks. This leads to a multitude of 'entry points' and possible vulnerabilities for attacks, thus creating a complex risk landscape that is difficult to control. The use of legacy products with outdated security features (e.g. US FBI, 2022) coupled to the arrival of novel products, some with insufficient cyber security patches, further complicates this situation. Cyber attacks may lead to the leakage of sensitive personal health data or data theft. With increasing use of AI in healthcare, cyber attacks may cause the 'poisoning' of models or data, thus inflicting deterioration and longer-lasting damage with significant economic cost.

All these effects may affect patient health, including delayed diagnostic procedures or delayed surgery, deteriorated device performance or even the tampering of individual devices, e.g. via remote wireless access. Cyber attacks against health settings (e.g. WannaCry attack on the UK's National Health Service in May 2017, Trautman and Ormerod, 2018; Health Service Executive of Ireland in May 2021, PwC, 2021) forced hospitals to send patients to other facilities, redirecting ambulances to different hospitals, thus slowing clinical care. This puts many patients at risk, especially those who need urgent attention or surgeries. The main lesson is that patients are the ones who are most at risk from cyber attacks. They are the ones whose safety and private information are put in danger when medical equipment or treatments are disrupted (Wasserman and Wasserman, 2022).

***Cyber incidents in health have an ethical and legal dimension***

From a perspective of ethics in healthcare (Council of Europe, 1997: Oviedo Convention on human rights and biomedicine), cyber attacks are a serious issue for healthcare providers, since they may affect some of their obligations, rooted in conventions or specific legislations, i.e. to protect patients' safety and health as well as their dignity. Relevant aspects include: a) the capacity to respond to emergency situations (Article 8 of said convention), b) the protection of private life and personal and

sensitive information (Article 10) and c) equitable access to health care (Article 3). Importantly, cyber attacks could also lead to litigation, i.e. patients or their relatives challenging healthcare providers in regard to negligence or in regard to fulfilling their responsibilities to sufficiently protect their services and hence patients from the adversity caused by cyber attacks.

***Improving cyber resilience requires a better understanding of cyber attacks***

To protect public and private healthcare providers, the increasing health cyber risk will need to be tackled from different angles: clearly enhancing awareness, competences and operational capacities at healthcare settings is crucial. This could be achieved through dedicated cyber units with sufficient cross-cutting expertise on basic infrastructure as well as on medical devices employed in that setting.

However, a more fundamental prerequisite is to understand, and characterise cyber attacks in regard to common, consistent categories that facilitate the understanding of root causes, vulnerabilities and enhance information exchange between facilities (without the need to disclose sensitive information). This would help to learn from experiences and establish a code of best practices and key vulnerabilities, of "do's and do not's".

In short, without the necessary tools grounded in common concepts, the increasing digitalisation of the healthcare sector and the complexity of the governance of cyber security in healthcare will remain unmonitored and under-researched in regard to its cyber security related risks.

***Cybersecurity as part of the digital and AI value chain in health: concepts and methods***

An important hurdle currently is the lack of clear common understanding of key concepts and risks (see for instance: Dart & Ahmed, 2023). While there have been recently efforts in regard to developing frameworks (e.g. Dart & Ahmed, 2023), a systematic approach to organising relevant concepts in this area has been missing so far. A key shortcoming from our perspective is a conceptual one: cyber security appears rather separate from value chain-related aspects (e.g. data, models, AI systems, devices etc.) and there appear different communities dealing with cybersecurity and value chain aspects. However, cyber security is essential to preserve the elements of the value chain which may be threatened in their integrity and hence value by a cyber attack.

Second, estimating health impacts caused by cyber incidents remains problematic. The ENISA study *Threat landscape: health sector* (ENISA, 2023), reported that from January 2021 to March 2023 the European health sector faced 215 cyber incidents with a greater variety of type of attacks. Despite this large number of cyber incidents, ENISA stated that with the information collected it is not possible to «*measure accurately the impact of delayed treatment and care to a patient's health*». That suggests that there is no conclusive evidence on adverse health outcomes: they might or might not have occurred. This lack of robust evidence is clearly an unsatisfactory situation from a public health perspective. Thus, evaluating potential adverse health outcomes in patients remains a key challenge and such outcomes are much harder to quantify than financial costs associated with cyber incidents: they require appropriate medical monitoring, root cause reasoning and sufficiently long follow up. This clearly would cause costs and efforts. However, if not tackled, the human cost of cyber attacks in health may remain a blind spot of public health management and public health policies.

At the root of this shortcoming is a lack of data, clear reporting criteria and consistent characterisation methodologies allowing to describe and measure all effects of cyber attacks on healthcare organisations – not only those on infrastructure and cost. This is particularly important when considering the pace of technological advancements and the growing interconnectedness of organisations, which introduces new complexities (Portela et al., 2023).

As a solution, we propose a comprehensive toolbox for characterising cyber incidents in the health sector, capable of assessing potential causal connections between cyber incidents and adverse health effects (see section 2).

This toolbox requires, as a first prerequisite, a clear systematic approach to relevant concepts and their understanding. With the present ontology of "value chain enablers" and relevant health impact concepts we aim to deliver on this first requirement.

We propose that cybersecurity is an integral part of the value chain of digital and AI-enabled health solutions. More specifically, we consider cybersecurity a "value-preserving enabler" of value chain elements (**Figure 1**): cyber attacks can lead to the deterioration or destruction of assets of the value chain, e.g. data (including sensitive personal health data), machine learning (ML) and/ or statistical models, AI systems (containing ML models) or services, for instance those required for the use of digital health solutions (e.g. wearables under supervision of a health setting). Cyber security is hence fundamental for protecting and preserving those assets.

Other enablers are a) IT infrastructure and b) specific technologies. With enablers we mean prerequisites for capitalising on and realising value in digital and AI-enabled health. The concept of the value chain is discussed in more detail in a forthcoming publication on ontologies for AI in health (Griesinger et al., in preparation).

The three boxes coloured in green in **Figure 1** are the categories of the ontology focused on the value chain of digital health solutions, specifically the essential assets and enablers required for creating value, such as telemedicine and remote care, AI applications, digital therapeutics and treatment, personal health and wellness. Notably, cybersecurity plays a vital role as a value-preserving enabler, safeguarding all other components within the value chain.

The fourth category of the ontology, the health impacts (boxes coloured in brown), is not part of the value chain, but provides to the toolbox the necessary terminology to identify adverse health events caused by cyber incidents.

***Clarification of the concept of 'ontology'***

The term ontology, originally used only in philosophy, has been entering various other disciplines, notably data science and artificial intelligence. Below we outline the two main meanings of 'ontology':

- **Philosophy:**

  The term ontology refers to a branch of philosophy that "is the science of what is, of the kinds and structures of objects, properties, events, processes, and relations in every area of reality" (Smith, 2003). Ontologies are at the intersection of epistemology and logic and provide, in a more specific sense, an overview of 'entities' and their interrelationship and categorisation in relation to a specific problem of field[1]. In this sense, ontologies are related to terminologies but provide a more systematic overview of concepts.

[1] Originally, the term ontology or (ontologia) was coined independently in 1613 by the two philosophers Rudolf Göckel (Goclenius) in his Lexicon philosophicum and Jacob Lorhard (Lorhardus) in his Theatrum philosophicum. In the original sense of the word, ontologies sought to establish a comprehensive and all-encompassing classification of entities across all domains of existence. This classification should be definitive, providing a complete account of the essential types of entities needed to describe and explain all phenomena in the universe. It should also be exhaustive, encompassing every type of entity, as well as the relationships that connect them, forming more complex structures.

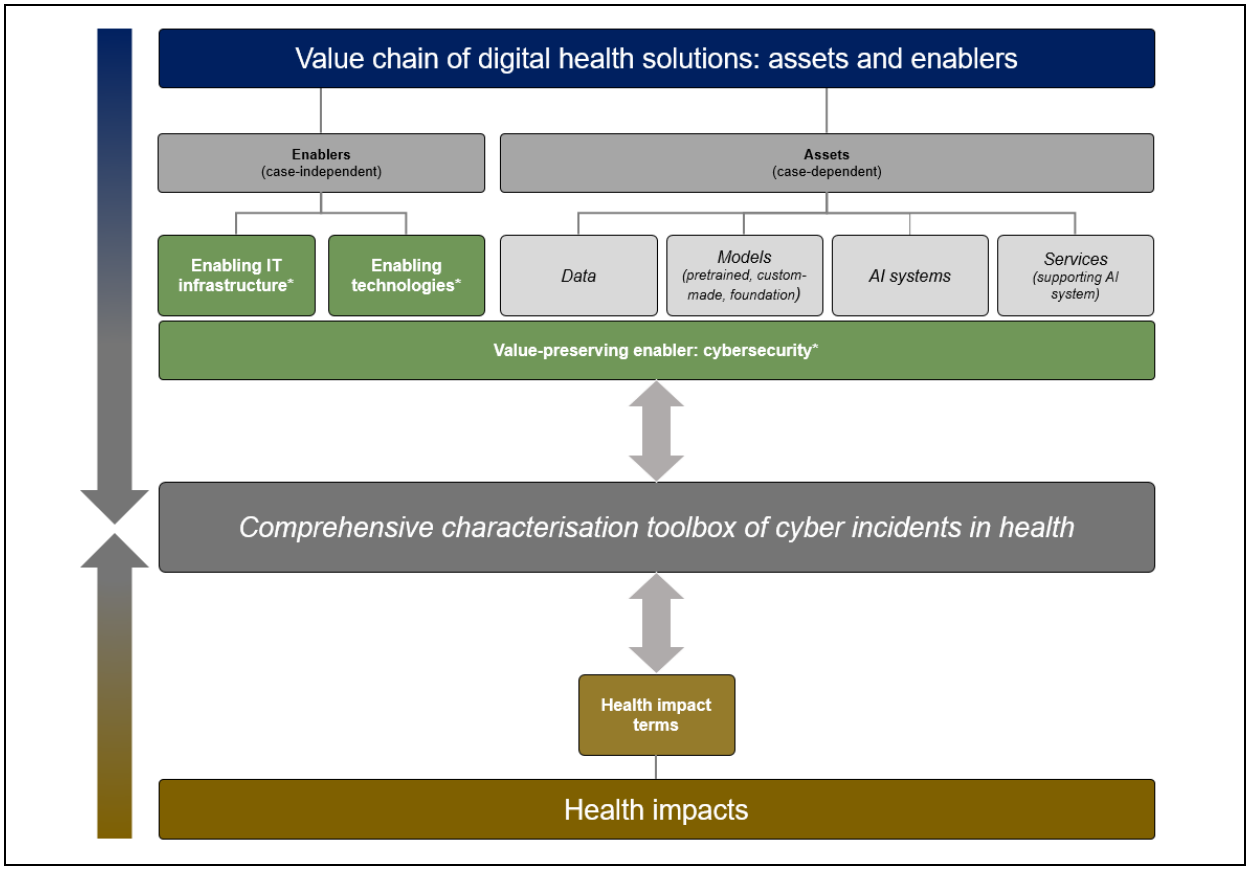
- **Data science and artificial intelligence**

  Since the mid of the 1970's the concept of ontologies has been adopted in the fields of data science and subsequently artificial intelligence. Researchers in these areas created so-called 'ontologies' that are machine readable and support computational models capable of enabling certain kinds of automated reasoning.

  Subsequently, in the AI community, the term ontology started to be referred to as both a theory of a modelled world and a component of knowledge-based systems. The seminal paper 'Toward Principles for the Design of Ontologies Used for Knowledge Sharing' (Gruber, 1993) offered a generally adopted definition of the term ontology to mean a 'specification of a conceptualization' that is, *"an ontology is a description (like a formal specification of a program) of the concepts and relationships that can exist for an agent or a community of agents"*. Felimayr modified Gruber's definition to describe ontology as *"a formal, explicit specification of a shared conceptualization that is characterised by high semantic expressiveness required for increased complexity"* (Felimayr et al., 2016).

  In computer science and data science, the development of an ontology is closely associated with specific methodologies, specific language and data model, which serve as essential tools for structuring knowledge within a domain. Typically, languages such as OWL (Web Ontology Language) or RDF (Resource Description Framework) are employed to encode these ontologies, ensuring that they can be processed by machines and understood by various stakeholders. Additionally, a data model defines how information is organised, facilitating the integration and retrieval of data across different applications. This structured approach on one hand enhances the clarity and consistency of information and on the other supports advanced functionalities such as reasoning and inference, which are vital for applications in fields like cybersecurity, particularly in complex environments like the health and medicine sector.

**Figure 1.** Schematic depiction of the four categories of this ontology (green and brown boxes) as fundamental element of a characterisation toolbox for cyber incidents in health. Green boxes: ontology categories of the value chain of digital and AI-enabled health solutions. Brown box: health impacts as a prerequisite for assessments of correlation and causality of cyber incidents and health impacts.




*Source: own production*

# 2 Specific context of this ontology: a toolbox for cyber incident characterisation

As outlined in the introduction, the present ontology is one key element of a comprehensive toolbox for the characterisation of cyber security incidents in healthcare settings. The toolbox responds to the growing threat of cyber incidents in the health. It is subject of a dedicated forthcoming publication (Reina and Griesinger, in preparation). It is designed to allow characterisation of cyber attacks that target general digital infrastructure (e.g. hospital servers, cloud services, network infrastructure etc.) as well as those targeting products and devices that, e.g. via the internet of things, are accessible to hackers and malicious actors. This concerns for instance digital healthcare solutions, irrespective of whether these are enabled by AI or not (e.g. robotic surgery suite, wearable devices etc.). However, we expect that AI-enabled products in healthcare may introduce novel vulnerabilities over time.

Briefly, the four elements of the toolbox are:

- Toolbox element 1 (this publication): **Ontology of concepts supporting cyber incident characterisation**

  The ontology is the foundational element of the toolbox and provides a common collection of concepts and vocabulary used by the other elements of the toolbox in order to characterise cyber incidents in health. The ontology is structured in two parts:

  a. The ontology of value chain enablers of digital health solutions that includes three categories of concepts:
     i. cybersecurity,
     ii. enabling IT infrastructure,
     iii. enabling technologies
  b. Health impact concepts

- Toolbox element 2: **Cyber incident characterization**

  The function of this element is to associate each cyber incident with a specific type, enabling healthcare organisations to rapidly identify and categorise the nature of the incident. This characterization process facilitates the implementation of targeted response strategies, ensuring that the organisation's response is proportionate to the severity and type of incident.

- Toolbox element 3**: Magnitude estimation**

  The function of this element is to estimate the magnitude of the incident based on a model comprising three dimensions. This multi-dimensional approach provides a comprehensive understanding of the incident, allowing healthcare organisations to allocate resources effectively and prioritise response efforts.

- Toolbox element 4: **Health impact assessment**

  The function of this element is to establish a plausible correlation between cyber incidents and patient health impacts included in the ontology subject of this report. By analysing the potential consequences of a cyber incident on patient care and health outcomes, healthcare organisations can take proactive measures to mitigate harm and ensure the continued delivery of high-quality care.

**Figure 2** is a schematic depiction of the toolbox and its constituent elements. The figure shows that the information related to cyber incidents is the input of the toolbox and it also illustrates the interlink between the present ontology and the other three elements. For example, the element 3 of the toolbox, Magnitude estimation, uses concepts of the categories enabled IT infrastructure and health impacts to evaluate respectively scope and seriousness of a cyber incident.

These four elements will provide a consistent understanding of relevant concepts, thus facilitating collaboration and information exchange when characterising incidents in the health sector. It will help describe the magnitude of incidents in regard to the affected organisation and its stakeholders. Finally, it will provide tools for exploring potential causal links between cyber incidents and patient health effects and, most importantly, adverse health outcomes. A better understanding of the key properties of a given cyber incident will facilitate the implementation of adequate mitigation measures and to improve responsiveness to cyber incidents that may affect patient health.

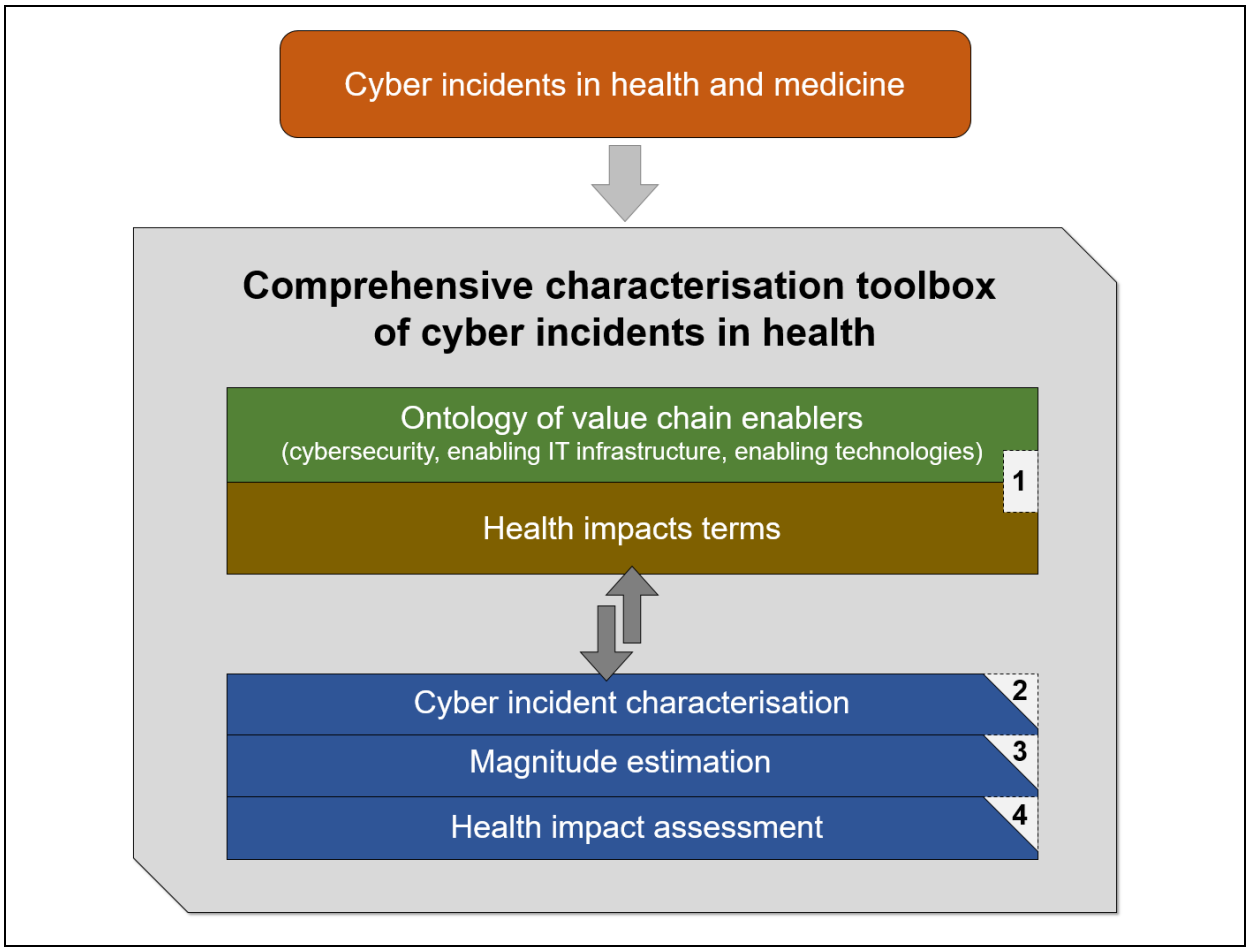
We note in this context that some examples of cybersecurity ontologies for the health sectors have been proposed. However, these either are not aimed at the specifics of the healthcare sector, or are highly focused in scope or do not address health effects of patients.

The approach and ontology suggested by Dart and Ahmed (2023) focuses on general data breaches and data disclosures. The approach by Hannou et al. (2021) focuses on incidents caused by attacks combining cyber and physical threats against healthcare infrastructures. Both approaches are valuable contributions to tackle cyber vulnerabilities in healthcare settings, but do not address health impacts.

A recent publication presents an ontology for cybersecurity in internet of medical things focused on remote patient monitoring (Bughio et al., 2024). A scoping review of cybersecurity ontologies applied to health, well-being and similar aspects of care addressed the topic of structuring the meaning of well-being and health data and structuring the meaning of cybersecurity approaches, measures, techniques, etc. to protect such data (Belani et al., 2023).

Other cybersecurity ontologies have been developed in the past years (Borja Rivadeneira et al., 2020 and Farooq et al., 2023) without being specific to healthcare, but taking into consideration aspects such as networking, software or human factors.

**Figure 2.** Schematic depiction of the toolbox and its constituting elements for characterising cyber incidents in healthcare settings




*Source: own production*

# 3 An ontology of concepts supporting cyber incident characterisation: premises, methods and information sources

The ontology presented here is based on the following premises:

1. **The ontology is rooted in the traditional philosophical concept[2] of an ontology and not a machine readable ontology** (see Introduction). It should not be mistaken as an ontology for implementing a programmable model of concepts for purposes of data sciences (e.g. organizing complex data sets) or AI (e.g. creating algorithms based on a concept model).
2. **The ontology is not a regulatory document.** However, it may, from a scientific and technical perspective, inform work towards regulatory templates and requirements for cyber incident reporting, in particular in the healthcare context.
3. The ontology should be tailored to the **health sector and applicable to both healthcare settings or to specific health applications**, products, devices and services. This concerns medical devices used in healthcare (e.g. diagnostics, clinical decision making), AI systems for healthcare management (e.g. patient flow management, emergency triaging) as well as services needed for deploying and running healthcare products (e.g. telemedicine services for AI-enabled wearable closed loop systems for managing specific diseases such as diabetes).
4. The ontology should outline important **general cybersecurity concepts** that relate to health care independent aspects but are generally applicable due to use of common infrastructure.
5. The ontology must include concepts related to the **IT infrastructure** (e.g. servers, databases, cloud services) **and technologies** (e.g. code libraries, software repositories), necessary to implement information systems and AI solutions in health.
6. The ontology should be embedded in a **value chain perspective** so as to facilitate the collaboration between different communities and agents involved in protecting relevant assets and services from cyber attacks.
7. The ontology should include concepts related to **health impacts** caused by cyber incidents so as to create a foundation for the evidence-based assessment of possible causal connections between cyber incidents and health impacts (e.g. delayed surgery), including adverse health outcomes (e.g. serious harm, illness; death; deterioration of health status).

We translated these premises into an ontology that describes a set of concepts related to cybersecurity and healthcare domains. The current ontology which we propose is aimed at providing a clear and consistent set of concepts that are required for the comprehensive characterisation of cyber incidents in health. The ontology itself is one of four elements of the forthcoming cyber incident characterisation toolbox briefly outlined in the previous chapter and it is intended as knowledge base used by the other three elements of this toolbox.

The ontology is composed of four categories. Categories 1 to 3 relate to the value chain of digital health solutions, i.e. assets and enablers that are prerequisites for value creation (e.g. AI models, telemedical solutions etc.). We consider categories 1 to 3 as value chain enablers (i.e. in contrast to

[2] See definition by Oxford Languages: *"Ontology: a set of concepts and categories in a subject area or domain that shows their properties and the relations between them"*. Online: https://www.oxfordlearnersdictionaries.com/definition/american_english/ontology#:~:text=ontology-,noun,with%20the%20nature%20of%20existence

assets), with cybersecurity being a value-preserving enabler for all other value chain elements (see forthcoming publication on an ontology of AI in health and medicine: ethical principles, translational and fundamental concepts; Griesinger et al., in preparation).

1. Ontology category 1: **Cybersecurity**

   This deals with key concepts of cybersecurity, e.g. threats, vulnerabilities, attacks, incidents.

2. Ontology category 2: **Enabling IT infrastructure**

   This category addresses the components necessary to operate and manage IT environments of organisations. This includes for instance various IT hardware, computer software, network and storage infrastructure.

3. Ontology category 3: **Enabling technologies**

   This category outlines platforms, frameworks and applications employed for the development, implementation and operation of AI systems. This includes for instance containerization and virtualization solutions, data pipelining applications or libraries, code repositories or software products.

4. Ontology category 4: **Health impacts**

   This category provides a set of relevant health impacts that may result from cyber incidents (e.g. delay to treatment/therapy, death, hospitalisation or prolonged hospitalisation, disruption of subsequent medical procedure).

For each of these categories, relevant entities (i.e. concepts) are described ("concept description"). Relationship between concepts in the ontology are indicated

The concepts in the four categories of the ontology are compiled from a diverse range of sources produced by various organisations and authors, representing a comprehensive overview of the field. The ontology's four categories drew primarily on the following main sources and excellent reports:

**Cybersecurity**

- European Union Agency for Cybersecurity (ENISA) (e.g. ENISA threat landscape: health sector, 2023)
- National Institute of Standards and Technology (NIST) (e.g. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, 2024)
- EU Directives (i.e. NIS2) and Regulation (i.e. EU Cyber Resilience Act)
- EU Commission (e.g. Nai-Fovino et al., 2018)[3]
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework

**Enabling IT infrastructure and Enabling technologies**

- 'Creation of a taxonomy for the European AI ecosystem' of the European Institute of Innovation and Technology (EIT, 2021)

[3] The cybersecurity taxonomy proposed by Nai-Fovino et al. (2018), tries to cluster a complex and multifaceted discipline as cybersecurity adopting a multiple dimensions structure, capturing three dimensions (i) Cybersecurity domains (e.g. cryptology, education and training, identity management) (ii) Sectors (e.g. defence, energy and health) (iii) Applications and technologies (e.g. cloud and virtualisation, hardware technology, artificial intelligence).

The proposed cybersecurity taxonomy, conceived to facilitate the categorisation of EU cybersecurity competencies, is not limited to the traditional academic research domain, but captures competencies, concepts and definitions of existing concepts and terminologies. This resulting three-dimensional taxonomy is not static, but it is open to modifications and must be understood as a living semantic structure, which will change to keep the pace of the fast evolution of the digital world.

**Health impacts**

- 'Annex F: Health Effects - Health Impact' of the adverse event (AE) terminology developed by the International Medical Device Regulators Forum (IMDRF)

# 4 The four ontology categories

For each concept within the four categories, the following information is provided:

- **Concept description**: provides an explication of the concept with a focus, where appropriate, on health.
- **Explanatory note**: provides further technical or scientific explanations as well as synonyms
- **Concept relationships**: indicates relations with other categories and other concepts of the ontology. For example,

  Threat actors [*carry out*] **Cybersecurity: Attacks**

  indicates that the concept "Threat actors" is related with "Cybersecurity: Attacks" (i.e. category: concept) through the action indicated in parenthesis (i.e. carry out). Non-bold font indicates the current concept, while bold font indicates another concept in the ontology, to which the current concept relates. The full list of relationships is available in **Table 1**.
- **References and further reading**: list of related/relevant references (e.g. publications, websites) which were used for developing the concept description and/or explanatory note or which provide additional relevant information.

In case, the concept description or explanatory note make use of and refer to concepts that are contained in this ontology, the concepts (preceded by their category) are highlighted in red font and preceded by an arrow, e.g. -> cybersecurity: attacks.

**Annex 1** contains the full list of concepts in alphabetical order.

## 4.1 Ontology category 1: cybersecurity

We consider cybersecurity as part of the value chain of AI and, more specifically, as a horizontal *value-preserving enabler* of all other value chain elements since cyber attacks can lead to the significant deterioration or even destruction of assets and enabling technologies and IT infrastructure. Examples are data theft, data destruction, the leakage of personal health information, model poisoning, model theft.

A cybersecurity ontology providing clarity on cybersecurity-related concepts and their relationship serves as a foundation for describing the complex relationships between cybersecurity and information systems in the healthcare domain, with a view of preserving the value chain including sensitive personal health information. This category also covers security measures and concepts for assessing the magnitude of cyber incidents in health.

Cybersecurity: Health sector cybersecurity

| Concept description |
| --- |
| Health sector cybersecurity refers to the measures and strategies put in place to avoid -> cybersecurity: attacks in the health sector.<br><br>To be effective, cybersecurity in health needs to consider the specific -> cybersecurity: risks and -> cybersecurity: vulnerabilities that result from significant variability of infrastructures in various health care settings, the heterogeneity of design of relevant services, interoperability issues of hardware. The complexity of the value chain including the high number of different agents involved |

can pose difficulties in rendering effective cybersecurity, including under variable use conditions, use contexts and use environments (keyword 'robustness').

Health cybersecurity aims at ensuring (continuity of) best patient care, e.g. through uninterrupted availability of services, un-deteriorated operation of equipment, preservation of confidentiality and integrity of patient data.

There are several challenges for realising health cybersecurity:

- healthcare providers (e.g. hospitals, primary care providers, socio-sanitary and dental care providers, emergency services, mental health institutions, care homes for elderly etc.),
- companies providing IT services to healthcare providers (e.g. cloud services),
- laboratories carrying out testing and R&D activities concerning medicinal products, medical devices and in vitro diagnostic medical devices,
- entities and organisations conducting research and development in the health sector (including pharmaceutical companies, medical device manufacturers, public research institutes etc.),
- pharmaceutical companies and companies producing medical devices and in vitro diagnostic devices,
- biotechnology manufacturers,
- health data providers for AI developers,
- algorithm providers and platforms,
- health authorities on regional, national or supranational level,
- health insurance organisations.

Explanatory note

The health sector, i.e. healthcare and underpinning research in life and health sciences, is of critical importance for modern societies. The healthcare sector is particularly attractive for -> cybersecurity: threat actors and hence at high risk of -> cybersecurity: attacks due to a variety of factors. These include its unique vulnerability to disruptions (with potential severe -> health impacts on the health of patients), its overall sise (consider for instance the attack on Ireland in 2021), the fact that it is wide-spread, its dependency on interconnected information technology and the sensitivity of the data being produced, handled and stored. The existence of -> cybersecurity: vulnerabilities at healthcare providers provides an opportunity for -> cybersecurity: attacks and these are consequently on the rise in the sector. The increasing use of AI systems in the health sector opens up additional -> cybersecurity: threats and -> cybersecurity: risks from a cybersecurity perspective.

Concept relationships:

Health sector cybersecurity [*tries to avoid*] **Cybersecurity: Attacks**

Health sector cybersecurity [*tries to avoid*] **Health impacts**

**Cybersecurity: Cyber resilience** [*enhances*] Health sector cybersecurity

References and further reading


- ENISA (2023) ENISA threat landscape: health sector. Online: https://www.enisa.europa.eu/publications/health-threat-landscape

- Cyberark (2024) website. Online: https://www.cyberark.com/what-is/healthcare-cybersecurity/
- US administration for strategic preparedness - US Department of health and human services (2023) Healthcare sector cybersecurity. Online: https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

## Cybersecurity: Cyber resilience

| Concept description |
| --- |
| Cyber resilience refers to all aspects aimed at enhancing cyber security in products vulnerable to -> cybersecurity: attacks. This includes cyber secure design, relevant mitigation and preparedness measures, processes of continuous security monitoring in the post-deployment stage as well as regular provision of security updates that are reflecting novel -> cybersecurity: vulnerabilities and attack types, including those that exploit lack of awareness of users ("social engineering"). Cyber resilience thus encompasses a technological dimension as well as a societal dimension, referring also to user awareness of vulnerabilities and measures to train users on the importance of cyber security, including for purchasing or procurement decisions (e.g. at healthcare settings). Importantly, cyber resilience measures at user facilities may need to be tailored to the specifics of a use environment, since some settings (e.g. hospitals) may have very specific vulnerabilities, e.g. based on past procurement decision, legacy products in use etc. |
| Explanatory note |
| Given the complexity of the value chain in healthcare involving a multitude of actors (with different legal status, technical competence and varying levels of financial resources available), cyber resilience of healthcare settings (e.g. hospitals, care homes) but also more complex ecosystems such as telemedicine, are a key consideration for healthcare products with a digital dimension. This is even more relevant for AI-enabled products due to the additional risks of data breaches, data poisoning etc. |
| Concept relationships: |
| Cyber resilience [*enhances*] **Cybersecurity: Health sector cybersecurity** |

References and further reading

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (EU Cyber Resilience Act). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

## Cybersecurity: AI specific cybersecurity threats

| Concept description |
| --- |
| AI specific -> cybersecurity: attacks are often identified as Adversarial Machine Learning and can be categorised according to the three main types of security violations considered when analysing |

| |
|---|
| the security of a system and strictly related to -> cybersecurity: motivations of threat actors: availability, integrity, and confidentiality. |
| Explanatory note |
| AI specific -> cybersecurity: attacks can be classified as:<br>• Availability attacks can be carried-out via data poisoning, when the -> cybersecurity: threat actors control a fraction of the training set; via model poisoning, when the attacker controls the model parameters; or as energy-latency attacks via query access.<br>• Integrity attacks target the integrity of models' output, resulting in incorrect predictions performed by a model. -> cybersecurity: threat actors can cause an integrity violation by carrying-out evasion attacks at testing/deployment time or a poisoning attack at training time.<br>• -> cybersecurity: threat actors might compromise confidentiality in two ways: learning information about the training data (inference attacks) or about the model (model extraction). |
| Concept relationships: |
| **Cybersecurity: Threats** [*incorporate*] AI specific cybersecurity threats |

References and further reading


- National Institute of Standards and Technology (NIST) (2024) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2 E2023 Online: https://doi.org/10.6028/NIST.AI.100-2e2023


## Cybersecurity: Threat actors

| |
|---|
| Concept description |
| Individuals or groups that pose a -> cybersecurity: threat to organisations or individuals operating IT systems that are connected via computer networks, most commonly the internet, by intentionally causing harm to digital devices or systems, exploiting -> cybersecurity: vulnerabilities in computer systems, networks, and software. |
| Explanatory note |
| Five main categories can be discerned (ENISA):<br>1) Cybercriminals (main objective is financial gain, data theft or demanding ransom),<br>2) Hackers-for-hire (individuals or groups that offer their cyber skills to various other actors),<br>3) State-sponsored actors (individuals or groups that are affiliated with a nation state and conduct attacks for political reasons, e.g. to interrupt supply chains, steal information etc.),<br>4) 'Hacktivists' (politically, ideologically motivated actors),<br>5) Insiders with malicious or non-malicious intent (e.g. current or former employees or members of an organisation with either a personal agenda of mal-intent or, in case of non-malicious insiders, people that commit errors, misconfigurations etc. which lead to critical and easily exploitable vulnerabilities). |

Synonyms:

- Cyber threat actors
- Malicious actors
- Bad actors
- Cybercriminals
- Hackers

Concept relationships:

Threat actors [*carry out*] **Cybersecurity: Attacks**

Threat actors [*have*] **Cybersecurity: Motivations of threat actors**

Threat actors [*intend to realise*] **Cybersecurity: Threats**

References and further reading


- ENISA (2021) ENISA Threat Landscape 2021. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- ENISA (2023) ENISA Threat Landscape 2023. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- ENISA (2023) ENISA threat landscape: health sector. Online: https://www.enisa.europa.eu/publications/health-threat-landscape


## Cybersecurity: Threats

Concept description

As defined by ENISA: "any circumstance or event with the potential to adversely impact a -> cybersecurity: asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service".

Explanatory note

Main threat categories are:

- Ransomware
- Threats against data
- Denial of service attacks
- Malware
- Social engineering threats
- Supply chain attacks
- Misconfigurations, errors and poor security practices.

Concept relationship:

Threats [*define*] **Cybersecurity: Attack scenario**

Threats [*incorporate*] **Cybersecurity: AI specific cybersecurity threats**

**Cybersecurity: Threat actors** [*intend to realise*] Threats

References and further reading

- ENISA Risk Management Glossary. Online: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

## Cybersecurity: Assets

Concept description

As defined by NIST: "An item of value to stakeholders. The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns".

Explanatory note

Examples of tangible assets are:

- physical item such as hardware
- firmware
- computing platform
- network device, or other technology component

Examples of intangible assets are:

- humans
- data and information
- software
- service
- trademark, copyright, patent, intellectual property
- image and/or reputation

Concept relationships:

Assets [*incorporate*] **Enabling IT infrastructure**

**Cybersecurity: Attacks** [*target*] Assets

References and further reading

- National Institute of Standards and Technology (NIST) (2021), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Volume 2. Online: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

## Cybersecurity: Motivations of threat actors

Concept description

The particular objective, reason or goal for a threat actors to carry-out a particular -> cybersecurity: attack.

| Explanatory note |
| --- |
| Examples of motivation of threats actors are:<br>• espionage<br>• financial gain<br>• sabotage<br>• ideology<br>• causing reputational damage<br><br>Synonyms:<br>• Intentions<br>• Objectives<br>• Aims<br>• Goal |
| Concept relationships: |
| **Cybersecurity: Threat actors** [*have*] Motivations of threat actors |

References and further reading


- ENISA (2023) ENISA threat landscape: health sector. Online: https://www.enisa.europa.eu/publications/health-threat-landscape


## Cybersecurity: Attacks

| Concept description |
| --- |
| Any kind of malicious cyber activity carried-out by -> cybersecurity: threat actors that attempts to realise some specific -> cybersecurity: threat that impacts confidentiality, integrity, accountability of some -> cybersecurity: assets of the entity targeted. |
| Explanatory note |
| A cybersecurity attack is a deliberate and often targeted attempt carry-out by -> cybersecurity: threat actors to exploit -> cybersecurity: vulnerabilities or breach the security of a system or network. It is a manifestation of a -> cybersecurity: threat and involves specific methods or tools to achieve its objective. |
| Concept relationships: |
| Attacks [*target*] **Cybersecurity: Assets**<br><br>Attacks [*implement*] **Cybersecurity: Attack scenario**<br><br>Attacks [*may cause*] **Cybersecurity: Cyber incident**<br><br>Attacks [*exploit*] **Cybersecurity: Vulnerabilities**<br><br>**Cybersecurity: Health sector cybersecurity** [*tries to avoid*] Attacks<br><br>**Cybersecurity: Monitoring tools** [*may identify*] Attacks |

**Cybersecurity: Threat actors** [*carry out*] Attacks

References and further reading

- Cyberark (2024) website. Online: https://www.cyberark.com/what-is/healthcare-cybersecurity/

## Cybersecurity: Vulnerabilities

### Concept description

As defined by the Common Vulnerabilities and Exposures (CVE) Program Glossary: "A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components".

### Explanatory note

Vulnerabilities refer to weaknesses or gaps in a system, network, or application that can be exploited by attackers to gain unauthorised access, steal data, or cause damage. These vulnerabilities can be the result of software or hardware flaws, inadequate security configurations, or human error.

Some examples of vulnerabilities are:

1. Software bugs
2. Unpatched systems
3. Weak passwords
4. Misconfigured systems
5. Social engineering
6. Unsecured network protocols

### Concept relationships:

Vulnerabilities [*define*] **Cybersecurity: Attacks scenario**

**Cybersecurity: Attack** [*exploit*] Vulnerabilities

**Cybersecurity: Measures for AI system IT infrastructure** [*mitigate*] Vulnerabilities

**Cybersecurity: Measures for IT environment** [*mitigate*] Vulnerabilities

**Cybersecurity: Monitoring tools** [*may identify*] Vulnerabilities

**Enabling technologies** [*have*] Vulnerabilities

**Enabling IT infrastructure** [*have*] Vulnerabilities

References and further reading

- Common Vulnerabilities and Exposures (CVE) Program Glossary. Online https://www.cve.org/ResourcesSupport/Glossary

## Cybersecurity: Attack scenario

| Concept description |
| --- |
| Steps and ways the -> cybersecurity: threat actor may realise -> cybersecurity: threats in order to exploit -> cybersecurity: vulnerabilities. An attack scenario occurs when a -> cybersecurity: threat actor takes action (-> cybersecurity: attacks) against a -> cybersecurity: asset by exploiting vulnerabilities within the system. |
| Explanatory note |
| Two examples of attack scenario in the health sector are:<br>• A healthcare organisation experiences a ransomware attack, which encrypts critical patient data and disables access to essential systems, such as electronic health records (EHRs), medical imaging systems, and scheduling software. The attackers demand a ransom payment in exchange for the decryption key to restore access to the data and systems.<br>• A healthcare organisation relies heavily on an AI-powered diagnostic system to analyze medical images, such as X-rays, CT scans, and MRIs. The attackers gain access to the system and manipulate the AI algorithms, causing incorrect diagnoses and delayed treatment for patients.<br><br>Synonyms:<br>• Threat scenario |
| Concept relationships: |
| Attack scenario [*have*] **Cybersecurity: Attack Likelihood**<br>Attack scenario [*have*] **Cybersecurity: Potential harm**<br>**Cybersecurity: Attacks** [*implement*] Attack scenario<br>**Cybersecurity: Threats** [*define*] Attack scenario<br>**Cybersecurity: Vulnerabilities** [*define*] Attack scenario |

References and further reading


- National Institute of Standards and Technology (NIST), Glossary of the Computer Security Resource Center (CSRC). Online: https://csrc.nist.gov/glossary
- Izosimov V., Törngren M. (2019) Security Awareness in the Internet of Everything (2019). DOI: 10.4018/978-1-5225-7332-6.ch012
- Mansourov N.; Campara D. (2010) System Assurance: Beyond Detecting Vulnerabilities. Morgan Kaufmann Publishers Inc.340 Pine Street, Sixth Floor, San Francisco CA, United States


## Cybersecurity: Attack likelihood

| Concept description |
| --- |
| As defined by ENISA: “The chance of a -> cybersecurity: attack to happen”. |

| Concept relationships: |
| --- |
| Attack likelihood [*determines*] **Cybersecurity: Security risks**<br><br>**Cybersecurity: Attack scenario** [*have*] Attack likelihood |

References and further reading

- ENISA Business Continuity Management Glossary. Online: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary/i-p

## Cybersecurity: Potential harm

| Concept description |
| --- |
| Potential negative consequence resulting from a -> cybersecurity: attacks. |
| **Explanatory note** |
| Examples of potential harm in the health and medicine sectors are:<br>• Medical device tampering<br>• Disruption of healthcare services<br>• Data breaches<br>• Compromised research data<br>• Reputational damage |
| **Concept relationships:** |
| Potential harm [*determines*] **Cybersecurity: Security risks**<br><br>**Cybersecurity: Attack scenario** [*have*] Potential harm |

References and further reading

- ENISA Risk Management Glossary. Online: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

## Cybersecurity: Security risks

| Concept description |
| --- |
| The chance of something happening that will have an impact upon objectives. In cybersecurity, it is associated with the potential that -> cybersecurity: threats will exploit -> cybersecurity: vulnerabilities of a -> cybersecurity: asset or group of assets of the targeted entity and the likelihood of a -> cybersecurity: attack scenario. |
| **Explanatory note** |
| Security risks can be classified in the following 16 categories:<br>1) Privacy-unauthorised contact or disclosure,<br>2) Privacy-unauthorised data collection, |

3) Data-physically lost or stolen,
4) Data-malicious breach,
5) Data-unintentional disclosure,
6) Identity-fraudulent use/account access,
7) Industrial controls and operations,
8) Network/website disruption,
9) Phishing, spoofing, social engineering,
10) Skimming, physical tampering,
11) IT-configuration/implementation errors,
12) IT-processing errors,
13) Cyber extortion,
14) Denial of service (DDOS)/system disruption,
15) Digital breach/identity theft and
16) Undetermined/other.

Concept relationships:

Security risks [*influence*] **Cybersecurity: Measures for AI system**

Security risks [*influence*] **Cybersecurity: Measures for IT environment**

**Cybersecurity: Likelihood** [*determines*] Security risks

**Cybersecurity: Potential harm** [*determines*] Security risks

References and further reading


- Nai-Fovino, I. et al (2018) European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. EUR 29332 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-92956-4, doi:10.2760/622400, JRC111441
- ENISA business Continuity Management Glossary. Online: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary/p-z
- Pavel V Shevchenko et al. (2023), The nature of losses from cyber-related events: risk categories and business sectors, Journal of Cybersecurity, Volume 9, Issue 1, 2023, tyac016, https://doi.org/10.1093/cybsec/tyac016
- Advisen Cyber Loss Data. Online: https://www.advisenltd.com/data/cyber-loss-data/


## Cybersecurity: Cyber incident

Concept description

An occurrence, resulting from the successful accomplishment of a -> cybersecurity: attack scenario, that actually or potentially jeopardises the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Explanatory note

A cyber incident refers to a security event or occurrence that negatively impacts the confidentiality, integrity, or availability of an organisation's information technology systems, networks, or data. A

cyber incident can result from a successful -> cybersecurity: attack scenario, which is a deliberate attempt to breach or exploit the security of a system or network.

A cyber incident can manifest in various forms, including:

- Data breaches
- Malware infections
- Denial-of-Service (DoS) attacks
- Social engineering
- Insider threats

When a -> cybersecurity: attack scenario is successful, it can lead to one or more -> cybersecurity: potential harm(s).

Concept relationships:

Cyber incident [*have*] **Cybersecurity: Scale**

Cyber incident [*have*] **Cybersecurity: Scope**

Cyber incident [*have*] **Cybersecurity: Seriousness**

Cyber incident [*may cause*] **Health impacts**

**Cybersecurity: Attacks** [*may cause*] Cyber incident

References and further reading


- National Institute of Standards and Technology (NIST), Glossary of the Computer Security Resource Center (CSRC). Online: https://csrc.nist.gov/glossary/term/incident


## Cybersecurity: Scale

Concept description

First of three concepts proposed for monitoring and characterising -> cybersecurity: attacks as a basis for potential -> cybersecurity: incidents reporting (depending on reporting thresholds set by regulators). **With "scale" we mean the extent and severity of the impacts ('adverse/negative effects') at the entity targeted by the attack** (e.g. a provider of cloud storage solutions, a company developing AI systems, a hospital).

Scale includes the following seven aspects:

1. damages of -> cybersecurity: assets (e.g. data loss/leaks; damage of an AI model, compromised networks etc.);
2. duration of the adverse effects caused by the attack;
3. the recovery time and internal/external resources required to resume normal and secure operations;
4. the level of deterioration of the operations of the entity (up to a complete outage);
5. financial and/or reputational damages suffered by the affected entity;
6. type of attack underlying the attack (e.g. phishing versus ransomware);
7. threat actor (e.g. organised crime or state sponsored crime versus teenage hackers).

Explanatory note

With scale we refer to the totality of adverse effects experienced by the entity targeted by a -> cybersecurity: attacks, including their extent and severity.

The concept of 'scale' encompasses both, 'impact' and 'damage' as widely used in the cybersecurity community. For instance the OCTAVE framework (Alberts et al., 1999) which provides guidance on evaluations of operationally critical -> cybersecurity: threats, -> cybersecurity: assets and -> cybersecurity: vulnerabilities, uses the term 'impact' to characterise a wide variety of adverse effects on the -> cybersecurity: assets (e.g. network, physical infrastructure) required for the entity's IT operations. Also the EU's NIS2 Directive (network and information security Directive, second iteration) uses both the terms damage and also impact in the context of adverse effects on the targeted entity (including severe operational disruption) as well as on other legal or natural persons (see for instance Article 23 on criteria for 'significant' cybersecurity incidents).

Synonyms:

- Impacts and damages at the entity targeted by the attack (e.g. OCTAVE framework)
- Severity of the incident for the entity targeted (e.g. NIS2 Directive)

Concept relationships:

**Cybersecurity: Cyber incidents** [*have*] Scale

References and further reading


- Christopher A. J.; Behrens S.; Pethia R. D.; Wilson W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. Carnegie Mellon University. DOI: 10.1184/R1/6575906.v1
- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Online: https://eur-lex.europa.eu/eli/dir/2022/2555
- ENISA (2023) Health Threat Landscape. Online: https://www.enisa.europa.eu/publications/health-threat-landscape


## Cybersecurity: Scope

Concept description

Second of three concepts proposed for monitoring and characterising -> cybersecurity: attacks as a basis for potential -> cybersecurity: incidents reporting. **With "scope" we mean the "breadth" or "latitude" of the incident impact** when looking at the stakeholders of the affected entity. Stakeholders can be individual users or entities (e.g. companies, hospitals, research organisations). Scope is characterised by:

1. the number of affected stakeholders of the primarily affected entity
2. the geographical spread of stakeholders
3. cumulative sise of all stakeholder organisations affected by the incident

Explanatory note

We dissect the concept of 'impact' experienced by stakeholders (including affected individuals) into two distinct notions: a) the scope of the stakeholder landscape affected and b) the seriousness of

the impacts experienced by the stakeholders. The scope relates to the number, geographical spread and cumulative sise of stakeholders. The latter can be described by various aspects: e.g. number of people employed, number of users, turnover rate etc. -> cybersecurity: seriousness (see below) relates to the severity of the impacts experienced by stakeholders.

Synonyms:

- Impact and damages at stakeholders including individuals (e.g. NIS2)

Concept relationships:

**Cybersecurity: Cyber incidents** [*have*] Scope

References and further reading


- Christopher A. J.; Behrens S.; Pethia R. D.; Wilson W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. Carnegie Mellon University. DOI: 10.1184/R1/6575906.v1
- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Online: https://eur-lex.europa.eu/eli/dir/2022/2555


## Cybersecurity: Seriousness

Concept description

Third of three concepts used for monitoring and characterising -> cybersecurity: attacks as a basis for potential -> cybersecurity: incidents reporting. **With seriousness we mean the gravity of adverse impacts/damages experienced by the stakeholders (including individuals such as patients)** of the entity affected. Seriousness concerns:

1. time period during which the incident caused a deterioration (up to a complete outage) of the stakeholder's operations or services
2. financial and/or reputational damages suffered by the stakeholders
3. in case of healthcare providers: the adverse health effects/impacts on individuals/patients, e.g. delayed treatment, wrong treatment, prolonged hospitalisation etc.

Explanatory note

Note that for characterising adverse health impacts for patients, we provide a set of -> health impacts adapted from the IMDRF health impacts/effects terminology. These terms capture high-level downstream impacts such as prolonged hospitalisation or delayed treatment that may be relevant in the present context.

Synonyms:

- Impact and damages at stakeholders including individuals (e.g. NIS2 Directive, Article 23 mentions the words impact and damage in the context of reporting obligations of essential and important entities)

| Concept relationships: |
| --- |
| Seriousness [*draws on*] **Health impacts**<br>**Cybersecurity: Cyber incidents** [*have*] Seriousness |

References and further reading


- Christopher A. J.; Behrens S.; Pethia R. D.; Wilson W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. Carnegie Mellon University. DOI: 10.1184/R1/6575906.v1
- Agrafiotis I., Nurse J. R. C., Goldsmith M., Creese S., Upton D. (2018), A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006
- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Online: https://eur-lex.europa.eu/eli/dir/2022/2555
- IMDRF adverse event terminology. See the web-browser originally developed by JRC: https://www.imdrf.org/working-groups/adverse-event-terminology


## Cybersecurity: Monitoring tools

| Concept description |
| --- |
| Cybersecurity monitoring tools are software applications used to detect, analyse, and respond to -> cybersecurity: attacks and -> cybersecurity: incidents in real-time. These tools help organisations identify potential -> cybersecurity: threats, -> cybersecurity: vulnerabilities, and anomalies in their systems, applications and -> enabling IT infrastructure. Cybersecurity monitoring tools support the implementation of continuous security monitoring (CSM) strategies by automatising tasks such as the monitoring of information security controls (->cybersecurity: measures for IT environment and -> cybersecurity: measures for AI system), -> cybersecurity: vulnerabilities and other -> cybersecurity: threats. |
| Explanatory note |
| Some common types of cybersecurity monitoring tools are:<br>• Intrusion Detection Systems (IDS)<br>• Security Information and Event Management (SIEM) Systems<br>• Endpoint Detection and Response (EDR) Tools<br>• Network Traffic Analysis (NTA) Tools<br>• Vulnerability assessment tools<br>• Penetration testing tools |
| Concept relationships: |
| Monitoring tools [*may identify*] **Cybersecurity: Attacks**<br>Monitoring tools [*may identify*] **Cybersecurity: Vulnerabilities** |

References and further reading


- Types of cybersecurity monitoring tools: NetAlly explains. Online: https://cyberscope.netally.com/blog/types-of-cybersecurity-monitoring-tools (Last accessed: 2024.09.12)
- The Importance of Continuous Security Monitoring for a Robust Cybersecurity Strategy. Online: https://thehackernews.com/2023/11/the-importance-of-continuous-security.html (Last accessed: 2024.09.12)
- National Institute of Standards and Technology (NIST) (2011), Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations, NIST Special Publication 800-137. Online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf


## Cybersecurity: Measures for IT environment

### Concept description

Actions implemented at level of IT infrastructure/enabling technologies used to develop/deploy an AI system, taken to reduce the -> cybersecurity: security risk caused by a -> cybersecurity: attack. They may reduce the "value" of the affected -> cybersecurity: assets, the -> cybersecurity: threats facing the asset or the -> cybersecurity: vulnerabilities of that asset to those -> cybersecurity: threats.

### Explanatory note

Some key security measures that can be implemented to protect the overall IT environment from potential -> cybersecurity: attacks are:

1. Network segmentation
2. Firewalls and secure gateways
3. Endpoint security
4. Intrusion detection and prevention
5. Access controls
6. Data encryption
7. Regular software updates and patching
8. Security monitoring and logging

Synonyms:

- Mitigation measures
- Preventive actions
- Countermeasures

### Concept relationships:

Measures for IT environment [*mitigate*] **Cybersecurity: Vulnerabilities**

Measures for IT environment [depends on] **Enabling IT infrastructure**

**Cybersecurity: Security risks** [*influence*] Measures for IT environment

**Enabling IT infrastructure** [depends on] Measures for IT environment

References and further reading

- ENISA Business Continuity Management Glossary. Online: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary/c-d

### Cybersecurity: Measures for information/AI system

| Concept description |
| --- |
| Actions implemented at level of the information/AI systems (e.g. algorithms) taken to reduce the -> cybersecurity: security risk caused by a -> cybersecurity: attack. They may reduce the "value" of the affected -> cybersecurity: assets, the threats facing the asset or the -> cybersecurity: vulnerability of that asset to those -> cybersecurity: threats. |
| **Explanatory note** |
| Some key security measures that can be specifically implemented to protect AI systems from potential -> cybersecurity: attacks are:<br>1. Model encryption<br>2. Model versioning and backups<br>3. Model testing and validation<br>4. Model hardening<br>5. Model monitoring and logging<br>6. Access controls<br>7. Model watermarking<br><br>Synonyms:<br>• Mitigation measures<br>• Preventive actions<br>• Countermeasures |
| **Term relationship:** |
| Measures for information/AI system [*mitigate*] **Cybersecurity: Vulnerabilities**<br><br>**Cybersecurity: Security risks** [*influence*] Measures for information/AI system |

References and further reading

- ENISA Business Continuity Management Glossary. Online: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary/c-d

## 4.2 Ontology category 2: Enabling IT infrastructure

The enabling IT infrastructure category of concepts is based on the comprehensive report 'Creation of a taxonomy for the European AI ecosystem' of the European Institute of Innovation and Technology (EIT, 2021). This category captures the fundamental IT technologies and infrastructure that enable organisations to develop, deploy or use AI systems.

It encompasses the hardware, software, and network components that support the storage, processing, and transmission of data. This category of concepts, including technologies that provide basic technologies for computation, data storage as well as networking, is, in the EIT report, considered part of a broader category called 'enabling technology types'.

However, given the relevance and transversal characteristics of these concepts for both AI and non AI applications, we decided to create a separate category for these concepts.

All the concepts of this category have relationships with the following concepts of this ontology:

Enabling IT infrastructure [*have*] --> **Cybersecurity: Vulnerabilities**
**Cybersecurity: Asset** [*incorporate*] --> Enabling IT infrastructure
**Cybersecurity: Measures for IT environment** [*depend on*] --> Enabling IT infrastructure
**Enabling technologies** [*lean on*] --> Enabling IT infrastructure

References and further reading relevant for all the concepts of this category

- The European Institute of Innovation and Technology (EIT) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem

### Enabling IT infrastructure: Computing - algorithms run on local computers

| Concept description |
| --- |
| As defined by EIT: "*All hardware that is being used to run program code, meaning servers that house, for example, CPU or GPU based compute hardware*". |

### Enabling IT infrastructure: Computing - algorithms run on cloud-based computers

| Concept description |
| --- |
| A model of delivering computing resources, such as servers, storage, databases, networking, software, analytics, and intelligence, over the Internet ("the cloud"). |

### Enabling IT infrastructure: Storage - direct attached storage

| Concept description |
| --- |
| As defined by EIT: "*Hardware that is providing storage for data. This category comprises various different storage technologies like hard disk drives, flash drives or others*". |

### Enabling IT infrastructure: Storage - network-based storage

| Concept description |
| --- |
| Data storage infrastructure that is connected to the network and shared among multiple users or devices. It can be implemented using various technologies, such as Storage Area Networks (SANs), Network-Attached Storage (NAS). |

### Enabling IT infrastructure: Storage - cloud storage (remote storage)

| Concept description |
| --- |
| A type of network-based storage that is delivered as a service over the Internet. It allows organisations to store, manage, and access their data on remote servers maintained by a cloud storage provider. |

### Enabling IT infrastructure: Networking - Local Area Network (LAN) wired

| Concept description |
| --- |
| A wired LAN is a type of local area network that uses physical network cables, such as Ethernet, to connect devices and share resources within a limited geographical area, typically within a single building or campus. |

### Enabling IT infrastructure: Networking - Local Area Network (LAN) wireless

| Concept description |
| --- |
| A wireless LAN is a type of local area network that uses wireless technologies, such as Wi-Fi or Bluetooth, to connect devices and share resources within a limited geographical area, typically within a single building or campus. |

### Enabling IT infrastructure: Networking - Wide Area Network (LAN) wired

| Concept description |
| --- |
| A wired WAN is a type of wide area network that uses physical network cables, such as fiber-optic, copper, or satellite connections, to connect devices and share resources across long distances, typically spanning multiple cities, states, or countries. |

### Enabling IT infrastructure: Networking - Wide Area Network (WAN) wireless

| Concept description |
| --- |
| A wireless WAN is a type of wide area network that uses wireless technologies, such as cellular networks (e.g., 4G, 5G) or satellite connections, to connect devices and share resources across long distances, typically spanning multiple cities, states, or countries. |

### Enabling IT infrastructure: Direct networks

| Concept description |
| --- |
| Direct networks are short-range, ad-hoc communication technologies that enable devices to connect and share data without the need for a centralised network infrastructure (e.g. Bluetooth, NFC). |

Enabling IT infrastructure: Sensors

| Concept description |
| --- |
| As defined by EIT: "*Sensors refer to physical devices that allow capturing information about the real world. Examples are radar appliances, cameras for image capturing*". |

## 4.3 Ontology category 3: Enabling technologies

The category 'enabling technologies' capture concepts relating to platforms, frameworks and applications that facilitate and support the development, implementation, and operation of information systems and more specifically of AI systems.

This category is divided in three sub-categories of concepts taken from the 'Creation of a taxonomy for the European AI ecosystem' of the European Institute of Innovation and Technology (EIT, 2021).

These three sub-categories are understood as follows:

**Platforms**:

Software platforms used to manage AI model training or operation, maintain data assets or steer the development process of machine learning applications.

**Frameworks**:

Libraries, code repositories or technical resources that can be built upon in AI or ML development and that provide certain necessary functionalities, of which the goal is often to facilitate AI development and reduce effort of redundant implementation of the same functionalities.

**Applications**:

Software products commonly used during development or operation of AI systems, for example, to facilitate the setup of infrastructure, integrated development environment (IDE), data visualization or monitoring applications.

All the concepts of this category have relationships with the following concepts of this ontology:

Enabling technologies [*have*] **Cybersecurity: Vulnerabilities**
Enabling technologies [*lean on*] **Enabling IT infrastructure**

Enabling technologies: Platforms

| Concept description |
| --- |
| As defined by EIT: "*A platform describes some standardised layer of software that provides unified interfaces and functionalities to build application software on top of it*". |
| Explanatory note |
| Software platforms are used to manage AI model training or operations, maintain data assets or pipelines or steer the development process of machine learning applications. |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem

## Enabling technologies: Platforms - *Virtualization*

| Concept description |
| --- |
| As defined by EIT: "*Virtualization solutions allow abstracting from physical hardware infrastructure, by simulating hardware assets via software solutions and therefore increasing flexibility*". |
| **Explanatory note** |
| By using virtualization solutions, AI developers can create flexible, scalable, and secure environments that enable the efficient development, testing, and deployment of AI solutions.<br>Examples of popular virtualization platforms are:<br>• VMware vSphere<br>• Microsoft Hyper-V<br>• KVM (Kernel-based Virtual Machine)<br>• Xen<br>• Proxmox Virtual Environment (Proxmox VE)<br>• Citrix Hypervisor<br>• Oracle VM VirtualBox<br>• Red Hat Virtualization (RHV) |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://hostomise.com/blog/server-virtualization-popular-platforms/

## Enabling technologies: Platforms - Containerization

| Concept description |
| --- |
| As defined by EIT: "*Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system. A container is essentially a fully packaged and portable computing environment*". |
| **Explanatory note** |
| Containerization enables the efficient deployment of models across different environments. This involves packaging the AI/ML model, its dependencies, and the necessary runtime components into a single container image. The container image can then be deployed on a chosen host, ensuring that the AI/ML model runs consistently and reliably. By adopting containerization, AI/ML developers can streamline the deployment process, reduce complexity, and ensure consistency across different environments.<br>Popular open-source containerization tools and technologies include: |

- Docker
- Kubernetes
- Apache Mesos
- OKD
- Operator Hub

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://techbeacon.com/enterprise-it/how-containerization-brings-ai-your-devops-pipeline
- https://bito.ai/blog/containerization-a-beginners-guide-to-its-impact-on-software-development/
- https://www.teraflow.ai/simplifying-ml-model-deployment-with-containerization/

## Enabling technologies: Platforms - Orchestration

### Concept description

As defined by EIT: "*Orchestration describes the automatic assignment of hardware resources to software solutions. These solutions allow to abstract from actual hardware and resource requirements, which are handled automatically*".

### Explanatory note

Orchestration enables the automated management and coordination of multiple containers across different environments. Orchestration platforms provide a comprehensive set of features to simplify the deployment, scaling, and management of containerised AI/ML workloads. This involves defining the desired state of the AI/ML workload, such as the number of replicas, resource requirements, and networking configurations, and letting the orchestration platform handle the actual deployment and management.

Tasks performed using container orchestration tools include:

- Allocating resources among containers
- Scaling containers up and down based on workloads
- Routing traffic and balancing loads
- Assigning services and applications to specific containers
- Deployment and Provisioning

Popular orchestration platforms for AI/ML include:

- Kubernetes
- Red Hat OpenShift
- Mirantis Kubernetes Engine
- Helios
- Amazon Elastic Container Service (Amazon ECS)
- Google Kubernetes Engine (GKE)
- Azure Service Fabric
- Amazon Elastic Kubernetes Service (EKS)
- Docker Swarm

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://techbeacon.com/enterprise-it/how-containerization-brings-ai-your-devops-pipeline
- https://enterprisersproject.com/article/2021/7/aiml-workloads-containers-6-things-to-know
- https://gcore.com/blog/top-10-container-orchestration-tools/

## Enabling technologies: Frameworks

| Concept description |
| --- |
| As defined by EIT: "*A framework is a collection of software modules that are not a usable end-user-software themselves, but allow programmers to build upon them by using them as apart of their final software solutions*". |
| **Explanatory note** |
| Frameworks are libraries, code repositories or technical resources that can be built upon in AI or ML development and that provide certain necessary functionality, of which the goal is often to facilitate AI development and reduce effort of redundant implementation of the same functionality. |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem

## Enabling technologies: Frameworks - Machine learning libraries

| Concept description |
| --- |
| As defined by EIT: "*Machine learning libraries provide functionalities for training machine learning models. Machine learning libraries provide, for examples, languages to describe and handle statistical models and implement optimization approaches to train such statistical models based on some data*". |
| **Explanatory note** |
| Machine learning libraries provide a wide range of functionalities for training machine learning models, simplifying the development process and accelerating model building.<br>Some examples are:<br>• Scikit-learn: a Python library for traditional machine learning tasks, offering tools for data preprocessing, model selection, and evaluation<br>• TensorFlow: a library for building and training deep learning models, widely used for numerical computation and large-scale supervised and unsupervised learning<br>• PyTorch: a deep learning library suitable for research, known for its ease of use and customization options |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://neptune.ai/blog/visualization-in-machine-learning
- https://www.samarpaninfotech.com/blog/best-ai-development-tools-frameworks/

## Enabling technologies: Frameworks - Data visualization

| Concept description |
| --- |
| As defined by EIT: "*Data visualization frameworks provide functionality to plot graphs and other means of data visualization*". |
| **Explanatory note** |
| Data visualization frameworks provide functionality to plot graphs and visualise data, aiding in the exploration and communication of insights from datasets.<br>Some examples are:<br>• Matplotlib: a plotting library for creating static, animated, and interactive visualizations in Python<br>• Seaborn: Built on top of Matplotlib, Seaborn provides a high-level interface for creating attractive and informative statistical graphics<br>• Plotly: A JavaScript graphing library that offers interactive plots and dashboards for data visualization in Python, R, and other programming languages |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://www.projectpro.io/article/machine-learning-frameworks/509

## Enabling technologies: Frameworks - Data preparation and transformation

| Concept description |
| --- |
| As defined by EIT: "*Data preparation and transformation libraries allow handling of large data resources, transforming them and running simple analyses to derive insights about a dataset that are relevant in the later machine learning phase*". |
| **Explanatory note** |
| Some examples are of data preparation and transformation libraries are:<br>• Pandas<br>• OpenRefine<br>• Trifacta Wrangler<br>• DataRobot Paxata<br>• Rapid Miner<br>• KNIME Analytics Platform |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://neptune.ai/blog/packaging-ml-models
- https://skillupwards.com/blog/ai-tools-for-data-preprocessing-and-cleaning

## Enabling technologies: Frameworks - Model management

| Concept description |
| --- |
| As defined by EIT: "*Model management frameworks allow to track training of models and handle models in production (i.e. storing and loading them, deploying vs. undeploying them)*". |
| **Explanatory note** |
| Model management frameworks enable the tracking, deployment, and maintenance of machine learning models in production, ensuring their reliability and performance.<br>Some examples are:<br>• MLflow: an open-source platform for managing the end-to-end machine learning lifecycle, including experiment tracking, model packaging, and deployment<br>• Kubeflow: an open-source machine learning toolkit for Kubernetes, providing tools for building, deploying, and managing machine learning workflows at scale<br>• DVC (Data Version Control): a version control system for machine learning projects that support in track changes to data, models, and experiments. |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://www.projectpro.io/article/machine-learning-frameworks/509
- https://deepchecks.com/top-10-machine-learning-model-management-tools-for-businesses-in-2024/

## Enabling technologies: Frameworks - Other frameworks

| Concept description |
| --- |
| As defined by EIT: "*This category covers all other frameworks that focus on more general tasks, but in the end are also being used in the development of machine learning applications (e.g., to develop user interfaces)*". |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem

## Enabling technologies**:** Applications

| Concept description |
| --- |
| As defined by EIT: "*Applications are software artefacts that are designed and being used by end-users, that are not programmers themselves*". |
| **Explanatory note** |
| Software products that are commonly used during AI development or operations, for example to facilitate the setup of infrastructure, IDEs, data Visualization or monitoring applications. |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem

## Enabling technologies: Applications - Data Management

| Concept description |
| --- |
| As defined by EIT: "*Data management applications support users in handling and working with large datasets. They provide a graphical user interface to run basic data transformation and transferring*". |
| **Explanatory note** |
| Data management applications encompass tools and platforms that facilitate the organisation, processing, and utilization of data for various AI-related tasks. These applications leverage artificial intelligence to automate tasks, enhance data quality, streamline governance, improve cataloguing, and facilitate integration of diverse data sources. They play an important role in ensuring that data is clean, accurate, and readily available for analysis, model training, and decision-making in AI projects. |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://www.akkio.com/post/ai-use-cases-for-data-manager
- https://sloanreview.mit.edu/article/how-ai-is-improving-data-management/

## Enabling technologies: Applications - Data pipelining

| Concept description |
| --- |
| As defined by EIT: "*Data pipelining applications allow to define the flow of data between different applications and software solutions across the organisation*". |
| **Explanatory note** |
| These applications automate the process of extracting, transforming, and loading (ETL) data, ensuring that it is clean, relevant, and in the right format for analysis or model training. Data pipelining applications are used for ensuring that machine learning models are trained on high-quality data, leading to accurate predictions and optimal performance. |

Examples of data pipelining applications in AI include:

- Apache Airflow
- Apache Kafka
- AWS Glue
- Google Cloud Dataflow
- Microsoft Azure Data Factory

References and further reading


- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://flyaps.com/blog/how-to-build-a-data-pipeline-fast-for-ai-and-llm-projects-comparing-top-three-choices/
- https://www.chatgptguide.ai/2024/03/21/what-is-data-pipeline-python-for-ai-explained/
- https://www.informatica.com/blogs/with-ai-for-ai-8-top-steps-to-get-started-with-a-data-pipeline.html
- https://www.linkedin.com/pulse/feb-2024-gen-ai-applications-data-pipelines-quality-luke-dunlap-0cd8e
- https://www.projectpro.io/article/data-pipeline-tools/946


## Enabling technologies: Applications - Labelling (AME*: labeling)

Concept description

As defined by EIT: "*Labelling applications support users during data labelling, meaning they provide an easy and GUI-based approach to annotate data and might also support data annotation by pre-labelling functionalities*".

Explanatory note

These applications provide a user-friendly interface for annotating various types of data, such as images, text, and audio, to create labelled datasets for training machine learning models. In this way, AI developers can efficiently create high-quality labelled datasets, which are essential for training accurate and reliable machine learning models.

References and further reading


- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://keylabs.ai/blog/automated-data-labeling-revolutionizing-ai-development/
- https://www.labellerr.com/blog/how-ai-powered-data-labeling-tools-help-faster-development/
- https://www.superannotate.com/blog/best-data-labeling-tools


*) AME = American English, i.e. English as spoken and written in the US.

## Enabling technologies: Applications - Integrated development environments (IDEs)

| Concept description |
| --- |
| As defined by EIT: "*IDEs (Integrated Development Environments) are software solutions that are being used to program software. They provide text editor functionalities including support for software testing etc.*" |
| **Explanatory note** |
| IDEs play a significant role in simplifying the software development process, especially when working with complex AI projects that involve virtual environments, multiple API calls, and various libraries or packages.<br><br>IDEs streamline coding with AI tools by offering features like syntax highlighting, AI-driven code completion, and build automation systems that automatically manage dependencies and compile code, saving developers from manual setup tasks. IDEs also provide debugging tools that allow developers to examine variables, step through code execution, and quickly identify and correct issues in AI models. |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://www.dataquest.io/blog/what-is-an-ide-and-how-will-it-be-used-in-working-with-ai-in-2024/
- https://azumo.com/insights/integrated-development-environments-ides
- https://codesubmit.io/blog/ai-code-tools/

## Enabling technologies: Applications - Data visualization

| Concept description |
| --- |
| Data visualization applications allow users to create graphs and plots in a GUI-based fashion. |
| **Explanatory note** |
| These applications provide a user-friendly interface for users to easily visualise data without needing to write code.<br><br>Some popular examples of such applications are:<br><br>• Tableau<br>• Microsoft Power-BI<br>• Qlik<br>• Looker<br>• Sisense<br>• Polymer |

References and further reading

- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://www.geeksforgeeks.org/ai-tools-for-data-visualization/

## Enabling technologies: Applications - Monitoring

| Concept description |
| --- |
| As defined by EIT: "*Monitoring applications help users to track the outputs of their machine learning models and keep track of model quality*". |
| **Explanatory note** |
| Monitoring applications enable users to track the outputs of their machine learning models and maintain model quality. These applications provide continuous evaluation of models deployed in production to identify issues that may impact results. Some examples of metrics that monitoring applications help users track include memory use, latency, CPU/GPU use, data pipeline monitoring and model pipeline monitoring and cost tracking. Tools like Prometheus and Grafana are commonly used for monitoring machine learning systems. |

References and further reading


- EIT (the European Institute of Innovation and Technology) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem
- https://developer.nvidia.com/blog/a-guide-to-monitoring-machine-learning-models-in-production/
- https://learn.microsoft.com/en-us/azure/machine-learning/concept-model-monitoring?view=azureml-api-2
- https://www.evidentlyai.com/ml-in-production/model-monitoring

## 4.4 Ontology category 4: Health impacts

As outlined in the introduction, this ontology is intended to be one pillar of a forthcoming toolbox for characterising cyber incidents in health and, in particular, in healthcare settings, such as hospitals.

A complete characterisation of cyber incidents in healthcare requires an analysis of whether and to which extent patients have been harmed as a consequence of cyber attacks.

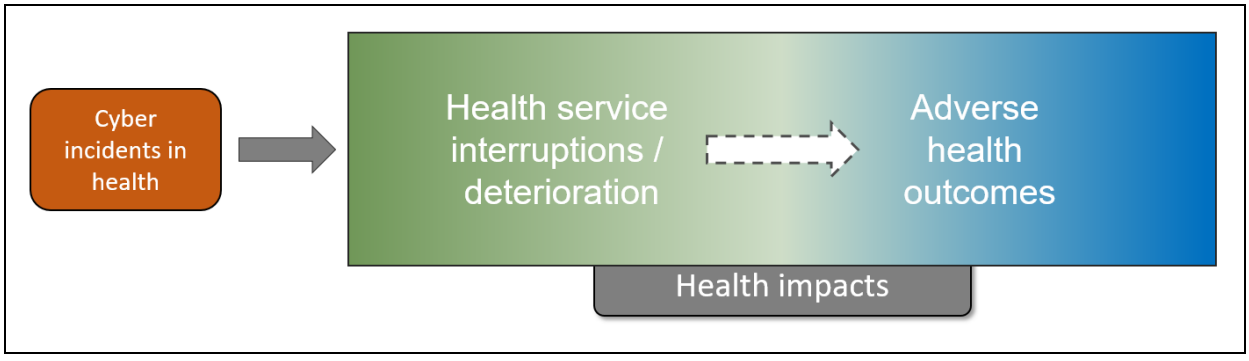
Primarily such attacks may result in, for instance, interruption or deterioration of services (e.g. patient scheduling), impaired infrastructure (e.g. diagnostic equipment) or inaccessibility of critical infrastructure (cloud-based radiological image storage).

As a secondary consequence, these primary effects may lead to delay of diagnosis, prolonged hospitalisation and other impacts on patients and their health status. We call these secondary consequences involving patients "health impacts".

The category health impacts, includes both concepts related to interruption / deterioration of health services (e.g. delay therapy / treatment) and adverse health outcomes directly affecting patients' health (e.g. serious injury / illness). As shown in **Figure 3**, under certain circumstances health service interruption / deterioration may lead to adverse health outcomes. Even if it would have been possible to subcategorise heath impacts concepts to further specify their effects, in some cases this distinction cannot be easily applied. For example, an additional surgery that was not planned does not influence the health status of the interested patient per se but, based on the health conditions of the individual, may induce unexpected adverse health outcomes.

For this reason, in order to facilitate, in the context of the forthcoming toolbox, a high-level characterisation of possible health impacts caused by cybersecurity incidents related to (AI-enabled) digital solutions, we propose a concise list of health impact concepts deemed most relevant in the context of cybersecurity incidents.

**Figure 3.** Category health impacts of the ontology




*Source: own production*

The concepts are based on the adverse event (AE) terminology (https://www.imdrf.org/working-groups/adverse-event-terminology) which were developed in a dedicated working group of the International Medical Device Regulators Forum (IMDRF), the 'Adverse Event Working Group' of which the European Commission (via JRC) was an active member.

The IMDRF AE terminology was developed with the objective of reporting problems with medical devices once on the market (i.e. incidents in EU / "adverse events" in US) and, potentially, also for

reporting problems occurring in the context of clinical trials in the pre-market space. The IMDRF AE terminology is provided in Excel format or via a web browser developed by the JRC which ensures user-friendly searching capabilities. The terminology consists of 7 sets of terms:

- Annex A: Medical Device Problem
- Annex B: Cause Investigation - Type of Investigation
- Annex C: Cause Investigation - Investigation Findings
- Annex D: Cause Investigation – Investigation Conclusion
- Annex E: Health Effects - Clinical Signs and Symptoms or Conditions
- Annex F: Health Effects - Health Impact
- Annex G: Medical Device Component

The list of health impacts in the current ontology is based on Annex F. The definitions of concepts were adapted to cyber security incidents - as opposed to the more specialised focus on medical devices of the original IMDRF health impact terms. The codes associated to each concept have the following syntax:

[IMDRF code] – CS

For clear traceability of term origin, the original IMDRF codes for each concept are provided.

All the concepts of this category have relationships with the following concepts of this ontology:

**Cybersecurity: Cyber incidents** [*may cause*] Health impacts
**Cybersecurity: Seriousness** [*draws on*] Health impacts
**Cybersecurity: Health sector cybersecurity** [*tries to avoid*] Health impacts

### Health impacts: Death

| Concept description |
| --- |
| Cyber incident caused or demonstrably contributed to death in patient(s). |
| Codes |
| Code: F02-CS<br>*Original IMDRF code: F02* |

### Health impacts: Delay to Diagnosis

| Concept description |
| --- |
| Cyber incident caused a clinically significant delay of patient diagnosis. |
| Codes |
| Code: F04-CS<br>*Original IMDRF code: F04* |

## Health impacts: Delay to Treatment / Therapy

| Concept description |
| --- |
| Patient treatment was delayed as a consequence of the cyber incident. |
| **Codes** |
| Code: F05-CS<br>*Original IMDRF code: F05* |

## Health impacts: Disruption of Subsequent Medical Procedure

| Concept description |
| --- |
| Situation in which the cyber incident impeded or affected a subsequent medical procedure or the use of a medicine or medical device. |
| **Codes** |
| Code: F06-CS<br>*Original IMDRF code: F06* |

## Health impacts: Hospitalization or prolonged hospitalization

| Concept description |
| --- |
| Hospitalization or prolonged hospitalization due deteriorated patient health resulting from the cyber incident. |
| **Codes** |
| Code: F08-CS<br>*Original IMDRF code: F08* |

## Health impacts: Inadequate / Inappropriate treatment or diagnostic exposure

| Concept description |
| --- |
| Patient did not receive intended treatment or received inadequate treatment as a consequence of the cyber incident. |
| **Codes** |
| Code: F10-CS<br>*Original IMDRF code: F10* |

## Health impacts: Minor Injury / Illness / Impairment

| Concept description |
| --- |
| The cyber incident caused a mild injury, illness or impairment which can be treated with minimal or no intervention, including monitoring only. |
| **Codes** |
| Code: F11-CS<br>*Original IMDRF code: F11* |

## Health impacts: Serious Injury / Illness / Impairment

| Concept description |
| --- |
| The cyber incident caused a severe injury, illness or impairment which requires medical intervention including hospitalization. |
| **Codes** |
| Code: F12-CS<br>*Original IMDRF code: F12* |

## Health impacts: Misdiagnosis / Misclassification

| Concept description |
| --- |
| The cyber incident caused an incorrect diagnosis or incorrect classification of an illness or other problem. |
| **Codes** |
| Code: F13-CS<br>*Original IMDRF code: F13* |

## Health impacts: Prolonged Episode of Care

| Concept description |
| --- |
| The cyber incident caused clinically significant extended treatment time or procedural time. Not to be used for prolonged hospitalization or prolonged surgery. |
| **Codes** |
| Code: F14-CS<br>*Original IMDRF code: F14* |

## Health impacts: Additional Surgery

| Concept description |
| --- |
| The cyber incident led to a surgical intervention that was not planned, but needed to be performed in addition to other interventions including surgical ones. |
| **Codes** |
| Code: F1901-CS<br>*Original IMDRF code: F1901* |

## Health impacts: Modified Surgical Procedure

| Concept description |
| --- |
| The cyber incident led to a change of surgical procedures from the original plan. |
| **Codes** |
| Code: F1906-CS<br>*Original IMDRF code: F1906* |

## Health impacts: More Complex Surgery

| Concept description |
| --- |
| The cyber incident led to surgery that is more complicated, more comprehensive or more extensive than planned (e.g. percutaneous to open surgery). |
| **Codes** |
| Code: F1907-CS<br>*Original IMDRF code: F1907* |

## Health impacts: Prolonged surgery

| Concept description |
| --- |
| The cyber incident caused surgery of a patient to be prolonged when compared to the originally anticipated duration. |
| **Codes** |
| Code: F1908-CS<br>*Original IMDRF code: F1908* |

## Health impacts: Surgical Procedure Delayed

| Concept description |
| --- |
| The cyber incident caused a delay of the surgical procedure which could not be completed when originally scheduled and put off until sometime in the future. |
| **Codes** |
| Code: F1909-CS<br>*Original IMDRF code: F1909* |

## Health impacts: Serious Public Health Threat

| Concept description |
| --- |
| The cyber incident caused a serious public health threat, i.e. the imminent risk of death, serious injury, or serious illness to more than one individual that required prompt remedial action. |
| **Codes** |
| Code: F20-CS<br>*Original IMDRF code: F20* |

## Health impacts: Unexpected Deterioration

| Concept description |
| --- |
| The cyber incident caused an unexpected clinical deterioration of the patient. |
| **Codes** |
| Code: F21-CS<br>*Original IMDRF code: F21* |

## Health impacts: Unexpected Diagnostic Intervention

| Concept description |
| --- |
| The cyber incident caused an unexpected diagnostic intervention (e.g. biopsy, endoscopic diagnostic procedure, imaging, IVD testing) that was not originally planned. |
| **Codes** |
| Code: F22-CS<br>*Original IMDRF code: F22* |

## Health impacts: Unexpected Medical Intervention

| Concept description |
| --- |
| As a consequence of the cyber incident, the patient required an unforeseen medical intervention (e.g. medication, resuscitation, blood transfusion but excluding surgery), which was not on the original treatment plan. |
| **Codes** |
| Code: F23-CS<br>*Original IMDRF code: F23* |

## Health impacts: Insufficient Information

| Concept description |
| --- |
| There is insufficient information to conclude whether or not the cyber incident has caused any serious health impact. |
| **Codes** |
| Code: F24-CS<br>*Original IMDRF code: F24* |

## Health impacts: No Health Consequences or Impact

| Concept description |
| --- |
| It can be excluded with a high degree of certainty, that the cyber incident caused any health consequences or impact. |
| **Codes** |
| Code: F26-CS<br>Original IMDRF code: F26 |

## Health impacts: No Patient Involvement

| Concept description |
| --- |
| No patient involvement when the cyber incident occurred (e.g. happened during set-up or cleaning). |
| **Codes** |
| Code: F27-CS<br>*Original IMDRF code: F27* |

## 4.5 Schematic illustration of categories and key concepts of the ontology

In order to visualise the relationships of the four ontology categories and, where appropriate, some of their constituent concepts, we prepared an ontology chart with relational arrows accompanied by a brief text outlining the type of relationship.

**Figure 4** shows a schematic illustration of categories and selected key concepts of the ontology. It does not reflect the entire ontology as presented in sections 4.1 to 4.4. Colour coding used in the figure is as follows:

- Light green: concepts associated with the category cybersecurity.
- Dark green: categories enabling IT infrastructure and enabling technologies. We decided to include in the figure only one box for each of allowing to detect patterns these two categories as all their concepts relate to the same categories or concepts.
- Brown: category health impacts. Also for this category we decided to include only one box as all its concepts relate to the same categories or concepts.

Other colours refer to concepts outlined in a forthcoming publication on an ontology for AI in health (Griesinger et al., in preparation).

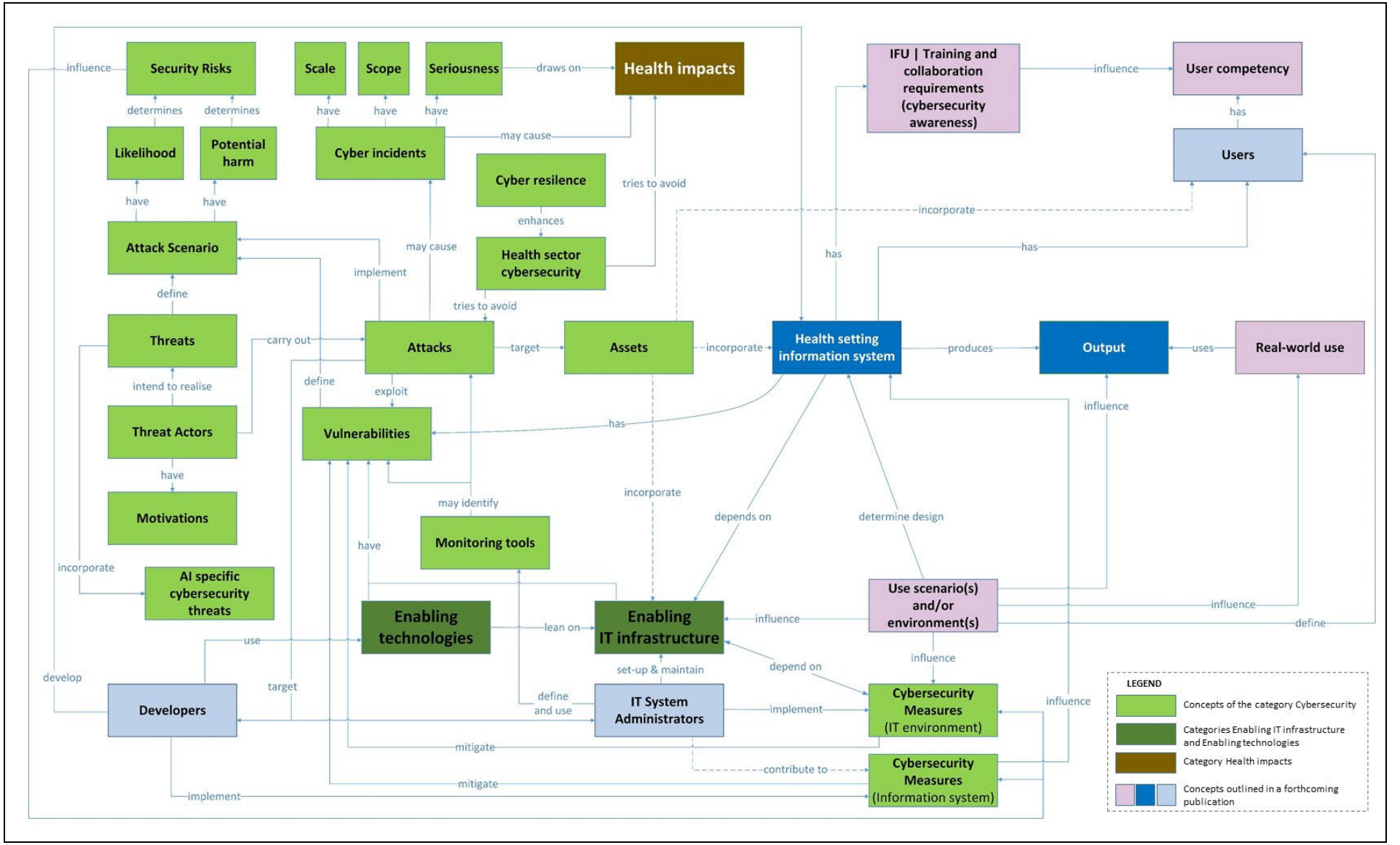
The same colour coding is used in **Table 1** where all the relations between categories and concepts of this ontology are listed.

**Table 1.** Relations between categories and key concepts of the ontology

| Category /Concept | Relation | Category /Concept |
|---|---|---|
| Assets | *incorporate* | Enabling IT infrastructure |
| Attack likelihood | *determines* | Security risks |
| Attack scenario | *have* | Likelihood |
| | *have* | Potential harm |
| Attacks | *may cause* | Cyber incident |
| | *target* | Assets |
| | *exploit* | Vulnerabilities |
| | *implement* | Attack scenario |
| Cyber incidents | *have* | Scale |
| | *have* | Scope |
| | *have* | Seriousness |
| | *may cause* | Health impacts |
| Cyber resilience | *enhances* | Health sector cybersecurity |

| Category /Concept | Relation | Category /Concept |
|---|---|---|
| Health sector cybersecurity | *tries to avoid* | Attacks |
| | *tries to avoid* | Health impacts |
| Measures for information/AI system | *mitigate* | Vulnerabilities |
| Measures for IT environment | *mitigate* | Vulnerabilities |
| | *depend on* | Enabling IT infrastructure |
| Monitoring tools | *may identify* | Attacks |
| | *may identify* | Vulnerabilities |
| Potential harm | *determines* | Security risks |
| Security risks | *influence* | Measures for information/AI system |
| | *influence* | Measures for IT environment |
| Seriousness | *draws on* | Health impacts |
| Threat actors | *have* | Motivations |
| | *carry out* | Attacks |
| Threats | *define* | Attack scenario |
| | *incorporate* | AI specific cybersecurity threats |
| Vulnerabilities | *define* | Attack scenario |
| Enabling IT infrastructure | *have* | Vulnerabilities |
| | *depends on* | Cybersecurity measures |
| Enabling technologies | *lean on* | Enabling IT infrastructure |
| | *have* | Vulnerabilities |

**Figure 4.** Schematic illustration of categories and selected key concepts of the ontology




*Source: own production*

# 5 Conclusion

The lack of a consistent framework for characterising cyber incidents in health complicates the estimation of patient health impacts of such incidents (EC JRC, 2024). It should enable the consistent characterisation of incidents in terms of their magnitude and type of incident (e.g. data breach versus ransomware), allowing the detection of patterns of technical deficiencies and vulnerabilities which would support forward-looking countermeasures ("cybersecurity by design"). Importantly, It should also be able to assess the link between cyber incident-caused health service impairments and health impacts as well as adverse health outcomes in patients. However, before being able to build such a framework, it is necessary to create the conceptual foundations, i.e. a common understanding of relevant concepts and how these relate to each other. This would also enhance clarity during collaboration and information exchange between industry and health settings on the one hand and, on the other hand, networks of health settings wishing to share experiences and best practices.

To this end, we have proposed here an ontology of relevant concepts. The ontology outlines key concepts, organises these in a logical structure and points to relevant references of important scientific and technical publications. Relevant concepts in this ontology relate to three 'enabling' elements of the value chain: i) cybersecurity (which can be considered an element of the value chain, protecting other value chain elements), ii) general enabling IT infrastructure, iii) enabling technologies. These three elements help realise health digitisation values such as a) *digital health products* and, specifically, *artificial intelligence-enabled health products* ('AI systems'), *data* (including health data generated during the post-market phase in a given health setting) and *services* needed to properly use specific digital health solutions. In addition, to facilitate assessments of potential causal links between health service deterioration or interruption and adversity in patients, we propose an essential set of health impact concepts, based on the IMDRF's adverse event terminology.

On the basis of the ontology, we will now continue to elaborate a comprehensive framework or 'toolbox' for characterising cyber incidents in health and assessing potential causal connections between these and adverse health outcomes in patients.

## References


Agrafiotis I., Nurse J. R. C., Goldsmith M., Creese S., Upton D. (2018), A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006

Belani H., Šolić P., Perković T. and Zovko K. (2023) "Ontology-Based Cybersecurity for Well-Being, Aging and Health: A Scoping Review," *2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, Dubrovnik, Croatia, 2023, pp. 50-55, doi: 10.1109/MeditCom58224.2023.10266600

Borja Rivadeneira W. F., Gómez O. S. (2020) Cybersecurity Ontologies: A Systematic Literature Review. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, vol. 9, núm. 2, 2020, Noviembre-, pp. 1-18. Online: https://www.redalyc.org/articulo.oa?id=512267931002

Bughio K.S., Cook D.M., Shah S.A.A. (2024) Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring. Sensors 2024, 24, 2804. https://doi.org/10.3390/s24092804

Christopher A. J.; Behrens S.; Pethia R. D.; Wilson W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. Carnegie Mellon University. DOI: 10.1184/R1/6575906.v1

Council of Europe (1997) Oviedo convention on human rights and biomedicine (ETS No 164). Online: https://www.coe.int/en/web/bioethics/oviedo-convention

Dart M and Ahmed M. (2023) CYBER-AIDD: A novel approach to implementing improved cyber security resilience for large Australian healthcare providers using a Unified Modelling Language ontology. Digit Health. 2023 Jul 30;9:20552076231191095. doi: 10.1177/20552076231191095

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Online: https://eur-lex.europa.eu/eli/dir/2022/2555

Farooq M. S. and Waseem M. T. (2023). Developing and Building Ontologies in Cyber Security. DOI: 10.48550/arXiv.2306.00377

ENISA (2021) ENISA Threat Landscape 2021. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2023) ENISA Threat Landscape 2023. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA (2023) ENISA threat landscape: health sector. Online: https://www.enisa.europa.eu/publications/health-threat-landscape

ENISA (2023) Health Threat Landscape. Online: https://www.enisa.europa.eu/publications/health-threat-landscape

Feilmayr C., Wöß W. (2016). "An analysis of ontologies and their success factors for application to business". Data & Knowledge Engineering. 101: 1–23. doi:10.1016/j.datak.2015.11.003

Gruber T. (1993) "Toward Principles for the Design of Ontologies Used for Knowledge Sharing". International Journal of Human-Computer Studies. 43 (5–6): 907–928. doi:10.1006/ijhc.1995.1081

Hannou F., Atigui F., Lammari N., Cherfi S. (2021). SafecareOnto: A Cyber-Physical Security Ontology for Healthcare Systems. 10.1007/978-3-030-86475-0_3.

International medical device regulators forum (IMDRF) Adverse event terminology. Annex F: Health Effects - Health Impact. Online: https://www.imdrf.org/working-groups/adverse-event-terminology

Izosimov V., Törngren M. (2019) Security Awareness in the Internet of Everything (2019). DOI: 10.4018/978-1-5225-7332-6.ch012

Mansourov N., Campara D. (2010) System Assurance: Beyond Detecting Vulnerabilities. Morgan Kaufmann Publishers Inc.340 Pine Street, Sixth Floor, San Francisco CA, United States

Nai-Fovino I. et al (2018) European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. EUR 29332 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-92956-4, doi:10.2760/622400, JRC111441

National Institute of Standards and Technology (NIST) (2011), Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations, NIST Special Publication 800-137. Online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

National Institute of Standards and Technology (NIST) (2021), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Volume 2. Online: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

National Institute of Standards and Technology (NIST) (2024) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2 E2023. Online: https://doi.org/10.6028/NIST.AI.100-2e2023

NIS2 Directive, Article 23 mentions the words impact and damage in the context of reporting obligations of essential and important entities

Noy N., Mcguinness D. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. Knowledge Systems Laboratory. 32. Online: https://www.researchgate.net/publication/243772462_Ontology_Development_101_A_Guide_to_Creating_Your_First_Ontology

Portela D., Nogueira-Leite D., Almeida R., Cruz-Correia R. (2023) Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study. JMIR Form Res 2023; 7:e41738 URL: https://formative.jmir.org/2023/1/e41738 doi: 10.2196/41738

PricewaterhouseCoopers (PwC) (2021) Conti cyber attack on the HSE: Independent Post Incident Review. Online: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (EU Cyber Resilience Act). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

Reina V. and Griesinger C. (2024) Cyber security in the health and medicine sector: a study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, European Commission, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2760/693487 , JRC13869

Shevchenko P. et al. (2023), The nature of losses from cyber-related events: risk categories and business sectors, Journal of Cybersecurity, Volume 9, Issue 1, 2023, tyac016, https://doi.org/10.1093/cybsec/tyac016

Smith B. (2003) Ontology. In The Blackwell Guide to Philosophy of Computing and Information, L. Floridi, ed., pp. 155-166, Blackwell, 2004. Online: https://philarchive.org/rec/SMIO-11

von der Leyen U. (2024) Political guidelines for the next European Commission 2024-2029. Online: https://commission.europa.eu/about-european-commission/towards-new-commission-2024-2029/president-elect-ursula-von-der-leyen_en

The European Institute of Innovation and Technology (EIT) (2021), Creation of a taxonomy for the European AI ecosystem. Online: https://eit.europa.eu/library/creation-taxonomy-european-ai-ecosystem

Trautman L. J. and Ormerod P. (2018), Wannacry, Ransomware, and the Emerging Threat to Corporations. 86 Tennessee Law Review 503 (2019), Available at SSRN: https://ssrn.com/abstract=3238293 or http://dx.doi.org/10.2139/ssrn.3238293

US administration for strategic preparedness - US Department of health and human services (2023) Healthcare sector cybersecurity. Online: https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

United States Federal Bureau of Investigation – cyber division. Private industry notification: Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities. Online: https://www.ic3.gov/CSA/2022/220912.pdf

Wasserman L. and Wasserman Y. (2022), Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Front. Digit. Health 4:862221. doi: 10.3389/fdgth.2022.862221

## List of abbreviations and definitions

| Abbreviations | Definitions |
|---|---|
| **AE** | Adverse Event |
| **AI** | Artificial intelligence |
| **API** | Application Programming Interface |
| **CPU** | Central Processing Unit |
| **CSM** | Continuous Security Monitoring |
| **CT scan** | Computed Tomography scan |
| **CVE** | Common Vulnerabilities and Exposures |
| **DVC** | Data Version Control |
| **EC** | European Commission |
| **EHR** | Electronic Health Record |
| **EIT** | European Institute of Innovation and Technology |
| **ENISA** | European Union Agency for Cybersecurity |
| **ETL** | Extracting, Transforming and Loading |
| **EU** | European Union |
| **FDA** | Food and Drug Administration |
| **GPU** | Graphics Processing Unit |
| **GUI** | Graphical User Interface |
| **IDE** | Integrated Development Environment |
| **IMDRF** | International Medical Device Regulators Forum |
| **IT** | Information Technology |
| **JRC** | Joint Research Centre |
| **LAN** | Local Area Network |
| **ML** | Machine Learning |

| | |
|---|---|
| **MRI** | Magnetic Resonance Imaging |
| **NAS** | Network-Attached Storage |
| **NFC** | Near Field Communication |
| **NIS (Directive)** | Directive on security of network and information systems |
| **OCTAVE** | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| **OES** | Operators of Essential Services |
| **OWL** | Web Ontology Language |
| **RDF** | Resource Description Framework |
| **SAN** | Storage Area Network |
| **US** | United States |
| **WAN** | Wide Area Networks |

# List of figures

**Figure 1.** Schematic depiction of the four categories of this ontology (green and brown boxes) as fundamental element of a characterisation toolbox for cyber incidents in health. Green boxes: ontology categories of the value chain of digital and AI-enabled health solutions. Brown box: health impacts as a prerequisite for assessments of correlation and causality of cyber incidents and health impacts. ..... 9

**Figure 2.** Schematic depiction of the toolbox and its constituting elements for characterising cyber incidents in healthcare settings ..... 12

**Figure 3.** Category health impacts of the ontology ..... 45

**Figure 4.** Schematic illustration of categories and key concepts of the ontology ..... 54

# List of tables

**Table 1.** Relations between categories and key concepts of the ontology..... 52

# Annexes

## Annex 1. List of concepts in alphabetical order


Cybersecurity: AI specific cybersecurity threats 18
Cybersecurity: Assets 21
Cybersecurity: Attacks 22
Cybersecurity: Attack likelihood 24
Cybersecurity: Attack scenario 24
Cybersecurity: Cyber incident 26
Cybersecurity: Cyber resilience 18
Cybersecurity: Health sector cybersecurity 16
Cybersecurity: Measures for IT environment 31
Cybersecurity: Measures for information/AI system 32
Cybersecurity: Monitoring tools 30
Cybersecurity: Motivations of threat actors 21
Cybersecurity: Potential harm 25
Cybersecurity: Security risks 25
Cybersecurity: Scale 27
Cybersecurity: Scope 28
Cybersecurity: Seriousness 29
Cybersecurity: Threats 20
Cybersecurity: Threat actors 19
Cybersecurity: Vulnerabilities 23
Enabling IT infrastructure: Computing - algorithms run on cloud-based computers 33
Enabling IT infrastructure: Computing - algorithms run on local computers 33
Enabling IT infrastructure: Direct networks 34
Enabling IT infrastructure: Sensors 35
Enabling IT infrastructure: Networking - Local Area Network (LAN) wired 34
Enabling IT infrastructure: Networking - Local Area Network (LAN) wireless 34
Enabling IT infrastructure: Networking - Wide Area Network (LAN) wired 34
Enabling IT infrastructure: Networking - Wide Area Network (WAN) wireless 34
Enabling IT infrastructure: Storage - cloud storage (remote storage) 34
Enabling IT infrastructure: Storage - direct attached storage 33
Enabling IT infrastructure: Storage - network-based storage 33
Enabling technologies**:** Frameworks 38
Enabling technologies: Frameworks - Data preparation and transformation 39
Enabling technologies: Frameworks - Data visualization 39
Enabling technologies: Frameworks - Machine learning libraries 38
Enabling technologies: Frameworks - Model management 40

Enabling technologies: Frameworks - Other frameworks....40
Enabling technologies: Platforms....35
Enabling technologies: Platforms - Containerization....36
Enabling technologies: Platforms - Orchestration....37
Enabling technologies: Platforms - *Virtualization*....36
Enabling technologies**:** Applications....41
Enabling technologies: Applications - Data Management....41
Enabling technologies: Applications - Data pipelining....41
Enabling technologies: Applications - Data visualization....43
Enabling technologies: Applications - Integrated development environments (IDEs)....43
Enabling technologies: Applications - Labelling (AME*: labeling)....42
Enabling technologies: Applications - Monitoring....44
Health impacts: Additional Surgery....49
Health impacts: Death....46
Health impacts: Delay to Diagnosis....46
Health impacts: Delay to Treatment / Therapy....47
Health impacts: Disruption of Subsequent Medical Procedure....47
Health impacts: Hospitalization or prolonged hospitalization....47
Health impacts: Inadequate / Inappropriate treatment or diagnostic exposure....47
Health impacts: Insufficient Information....51
Health impacts: Minor Injury / Illness / Impairment....48
Health impacts: Misdiagnosis / Misclassification....48
Health impacts: Modified Surgical Procedure....49
Health impacts: More Complex Surgery....49
Health impacts: No Health Consequences or Impact....51
Health impacts: No Patient Involvement....51
Health impacts: Prolonged Episode of Care....48
Health impacts: Prolonged Surgery....49
Health impacts: Serious Injury / Illness / Impairment....48
Health impacts: Serious Public Health Threat....50
Health impacts: Surgical Procedure Delayed....50
Health impacts: Unexpected Deterioration....50
Health impacts: Unexpected Diagnostic Intervention....50
Health impacts: Unexpected Medical Intervention....51

## Getting in touch with the EU

### In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

### On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

## Finding information about the EU

### Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

### EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

### EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

### EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

**EU Science Hub**
Joint-research-centre.ec.europa.eu

Publications Office
of the European Union