A comprehensive characterisation toolbox for cyber incidents in health

Vittorio REINA, Claudius GRIESINGER (EU Commission Joint Research Centre)

9th ENISA eHealth Security Conference – 06.11.2024 Budapest

Outline

- Cyber incidents in health in Europe
- Comprehensive assessment and characterisation toolbox
    - Element 1 - Ontology
    - Element 2 - Cyber incident characterization
    - Element 3 - Magnitude estimation
    - Element 4 - Health impacts investigation
- Conclusions

Cyber incidents in health in Europe: EC JRC

Address the discrepancy and data gap in the literature and in media reports concerning whether and to which extent cyber incidents in healthcare settings may lead to adverse consequences on patients' health.

Cyber incidents in health in Europe: EC JRC

The Ponemon Institute reports:

- **2022**: 517 healthcare experts in US hospitals and healthcare facilities
- **2023**: 653 healthcare IT and security practitioners in the US

Results:

- cyberattacks resulted in **compromised patient care** (e.g. impacted healthcare services, inappropriate therapy or treatment deliveries)
- **increased mortality rate** as a consequence of cyberattacks

The Health Service Executive (HSE) in Ireland, in May 2021 was subject to huge cyber-attack.

Representatives from health services in sites most affected by the cyber-attack were invited to participate in focus groups to share their experiences and learning:

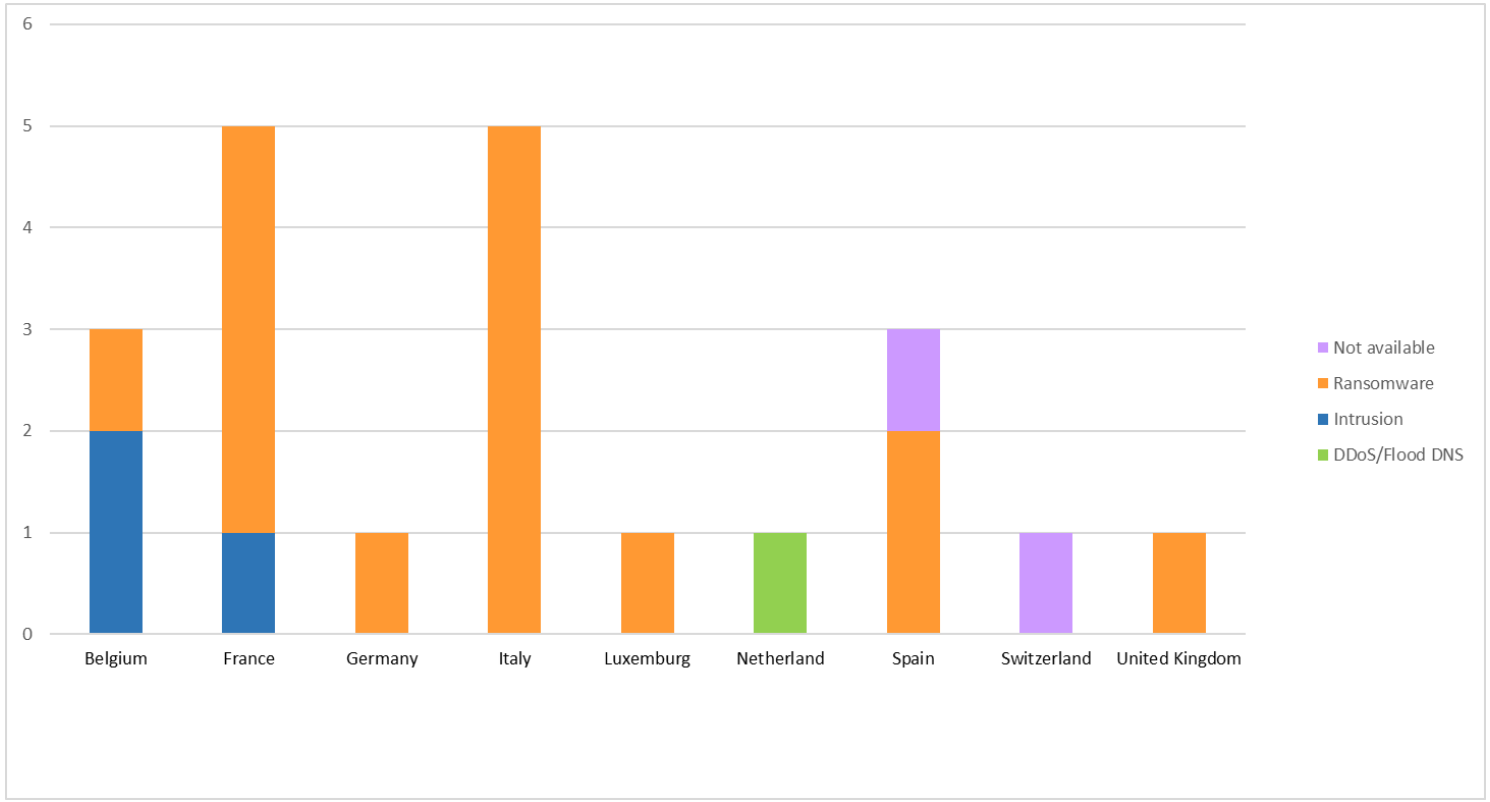
- **no evidence** that healthcare provision in the immediate aftermath of the attack has resulted in **harm to patients**
- **clinical staff** suspected that they will **not be fully aware of the impact of mitigations on patients** treated during this period for a long time to come

Ponemon Institute, Cynerio, The Insecurity of Connected Devices in Healthcare, 2022, https://www.cynerio.com/ponemon-survey-insecurity-of-connected-devices-in-healthcare-2022

Ponemon Institute, Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care 2023, https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Moore, G., Khurshid, Z., McDonnell, T. et al. A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Serv Res 23, 1112 (2023). https://doi.org/10.1186/s12913-023-10076-8

Cyber incidents in health in Europe: EC JRC



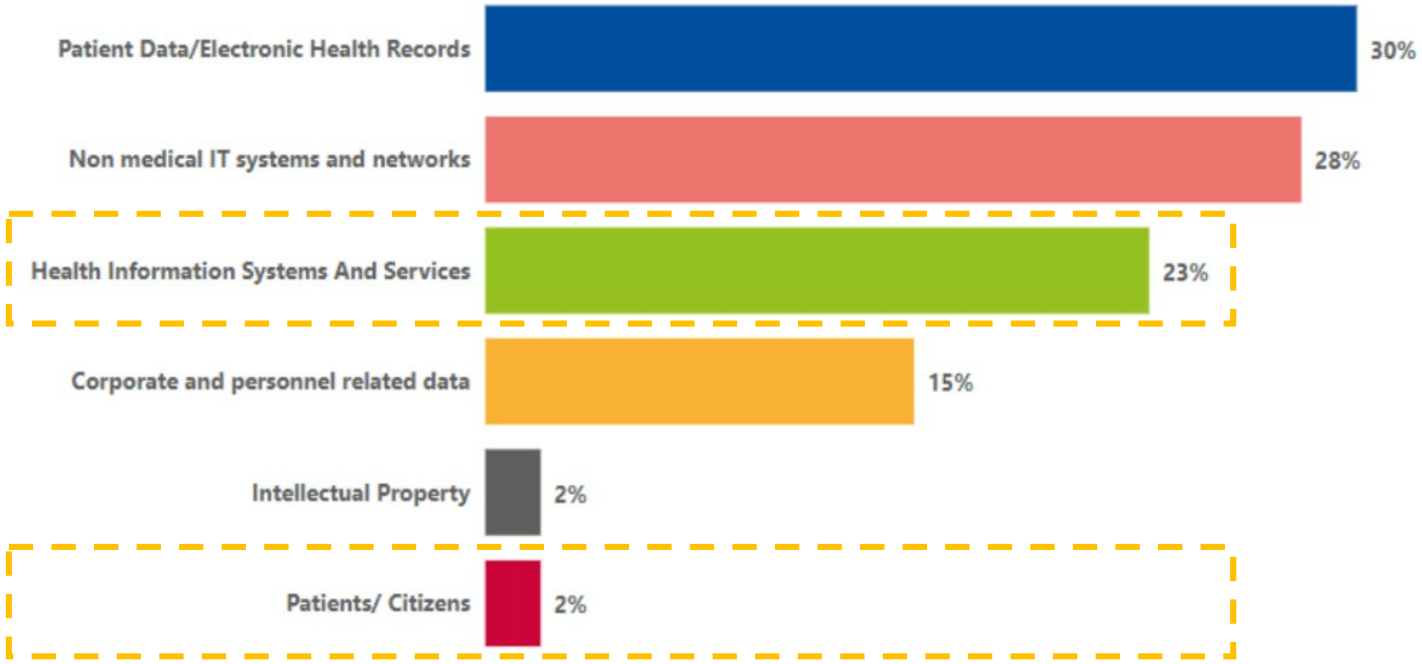
21 cyber incidents (from May 2022 to April 2023) that could potentially impact patients' health

English
Italian
French
Spanish
German

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

European Commission

Cyber incidents in health in Europe: ENISA



215 incidents from January 2021 to March 2023

(ca 100 incidents per year * 0.25)

«we cannot measure accurately the impact of delayed treatment and care to a patient's health»

ENISA THREAT LANDSCAPE: HEALTH SECTOR, July 2023, https://www.enisa.europa.eu/publications/health-threat-landscape

Comprehensive assessment and characterisation toolbox

The **lack of a consistent framework for characterising cyber incidents** in health **complicates the estimation of patient health impacts**.

Such framework should enable the consistent **characterisation** of **magnitude** and **type of incident** allowing to **detect patterns of technical deficiencies and vulnerabilities** which would support **forward-looking countermeasures**.

It should also allow to assess the **link between health service impairments caused by cyber incidents** and **health impacts** and **adverse health outcomes** in patients.

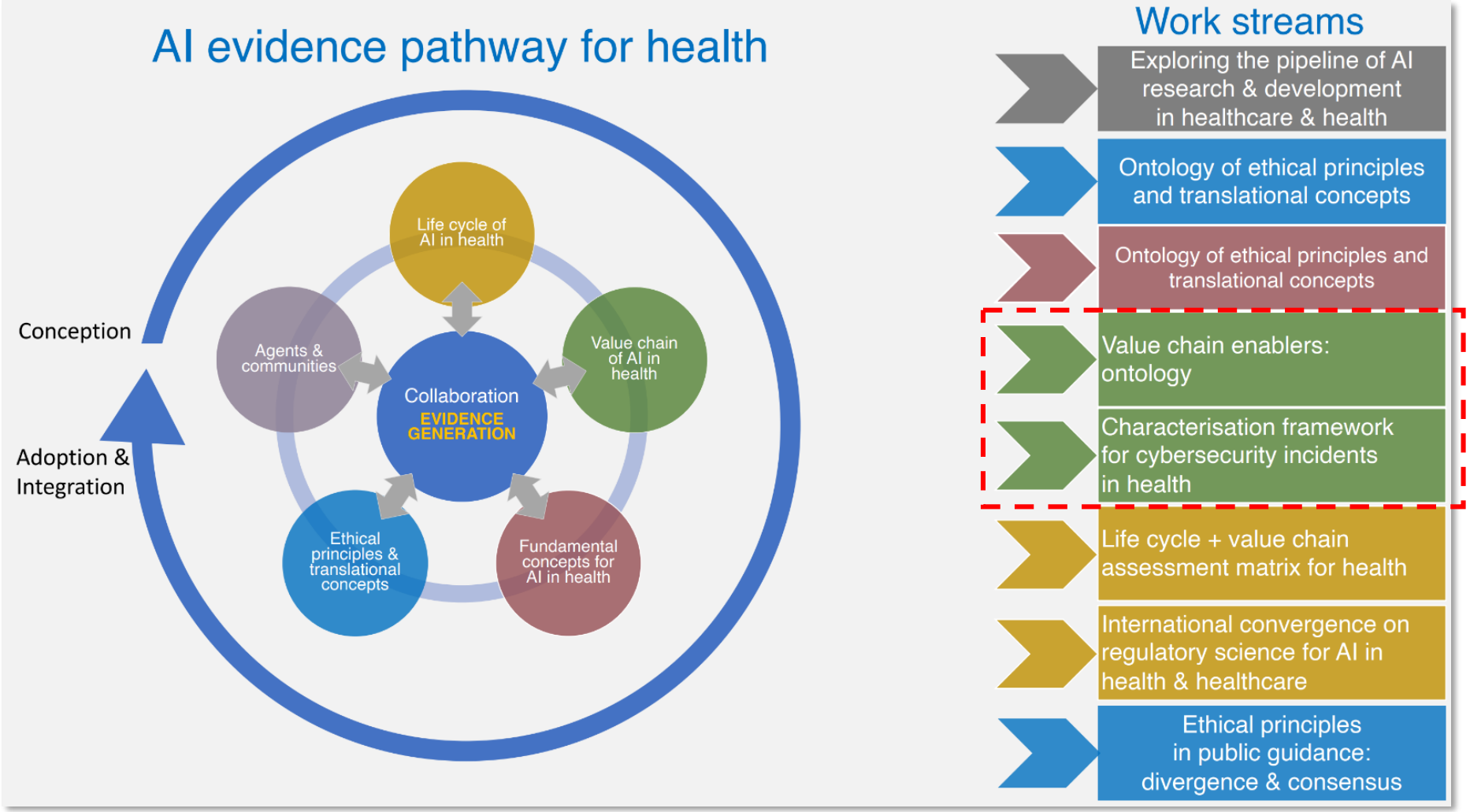
Comprehensive assessment and characterisation toolbox

It is necessary to create the **conceptual foundations**, a common understanding of relevant **terms and concepts** and how these relate to each other.

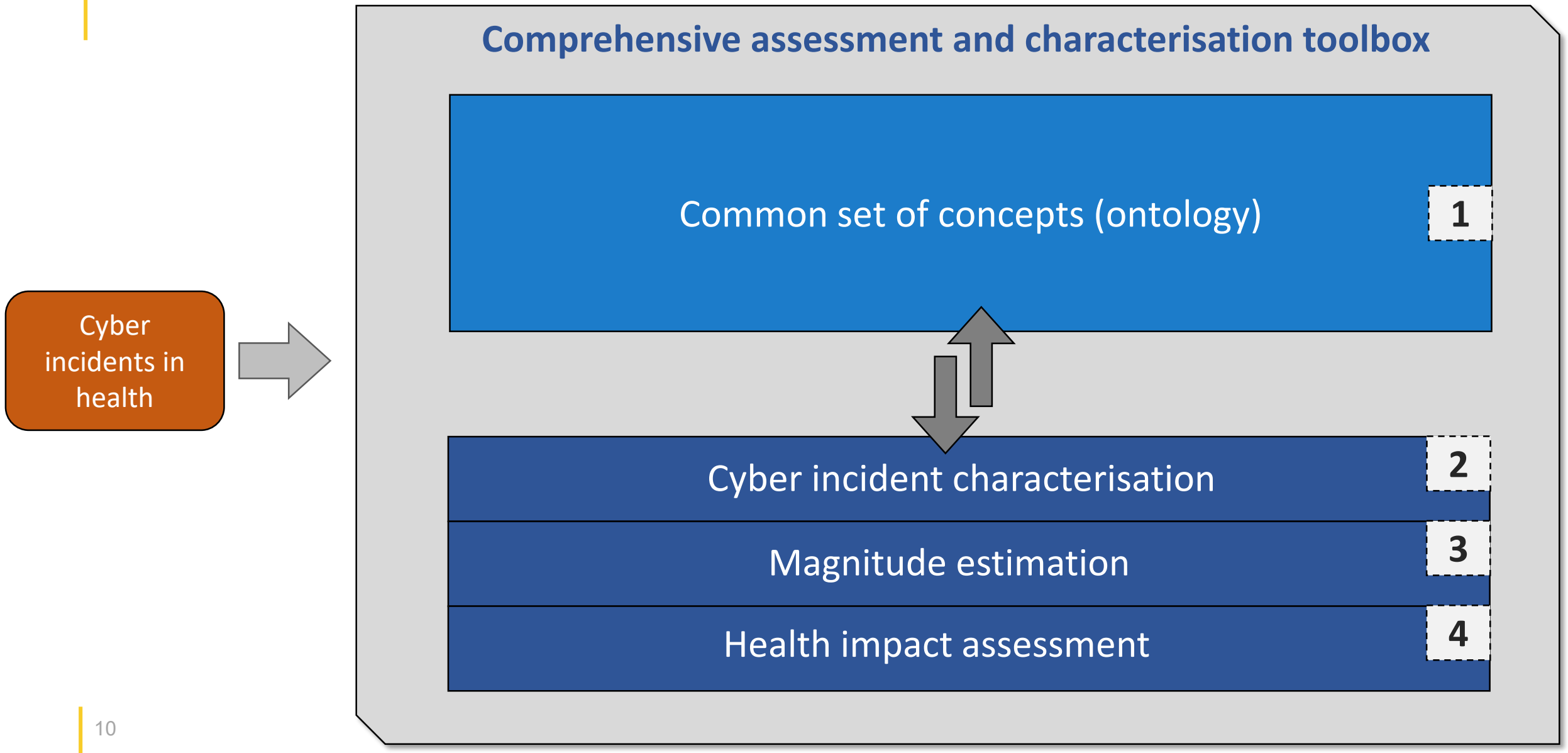
This would also enhance clarity during **collaboration and information exchange** between industry and networks of health settings wishing to share experiences and best practices.

Comprehensive assessment and characterisation toolbox

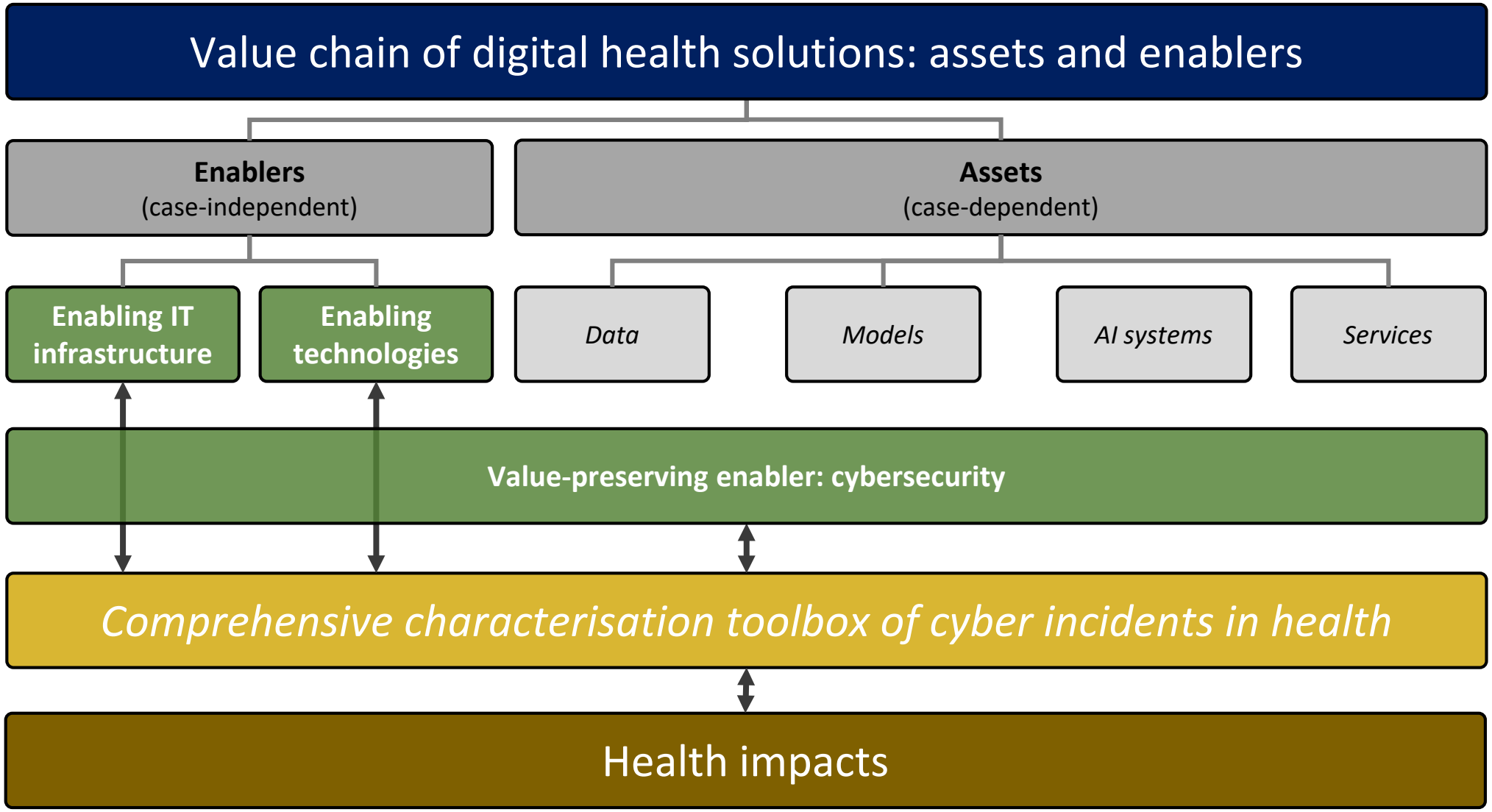
AI evidence pathway: collaboration across five domains
Our work streams to provide tools for bridging communities



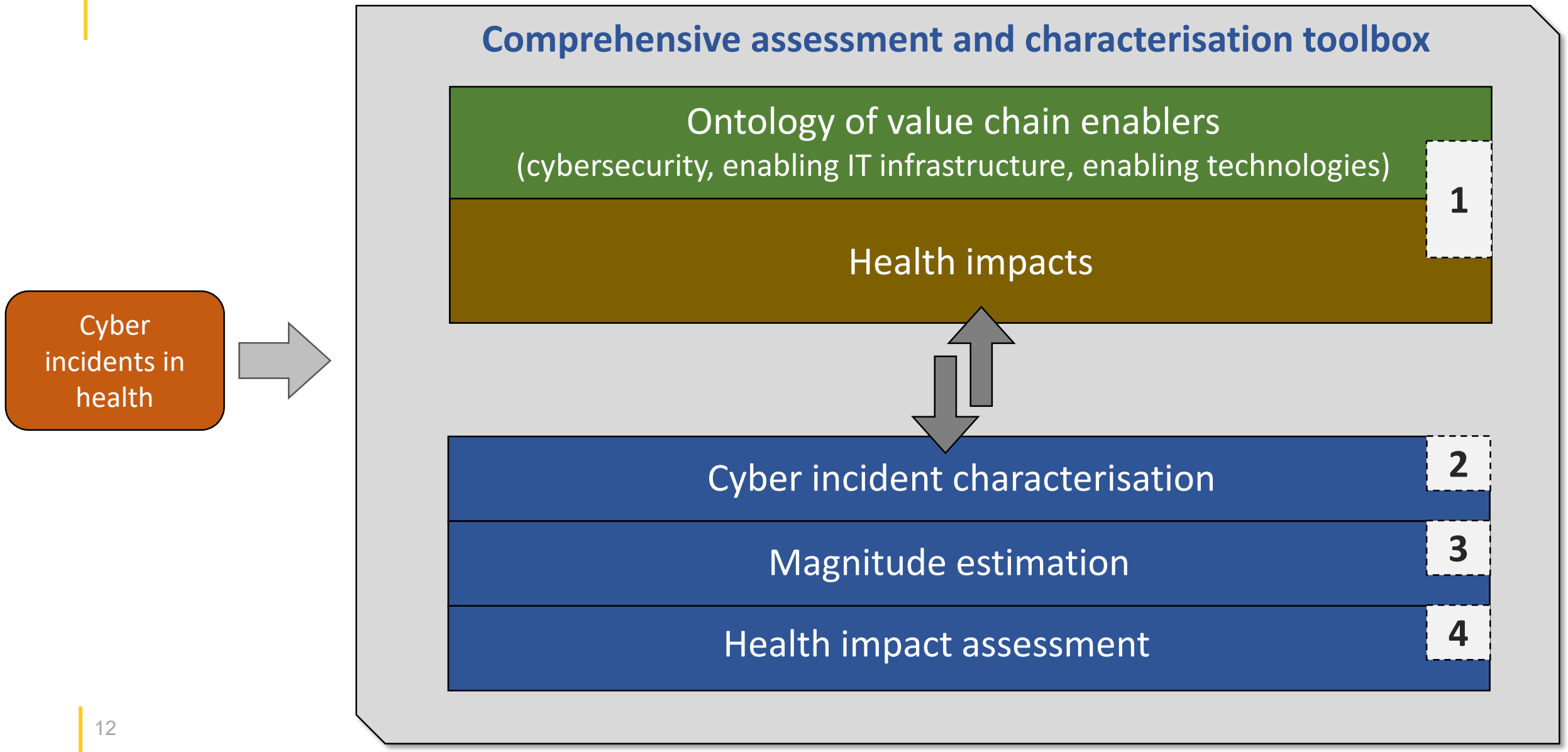
Comprehensive assessment and characterisation toolbox



Comprehensive assessment and characterisation toolbox



Comprehensive assessment and characterisation toolbox



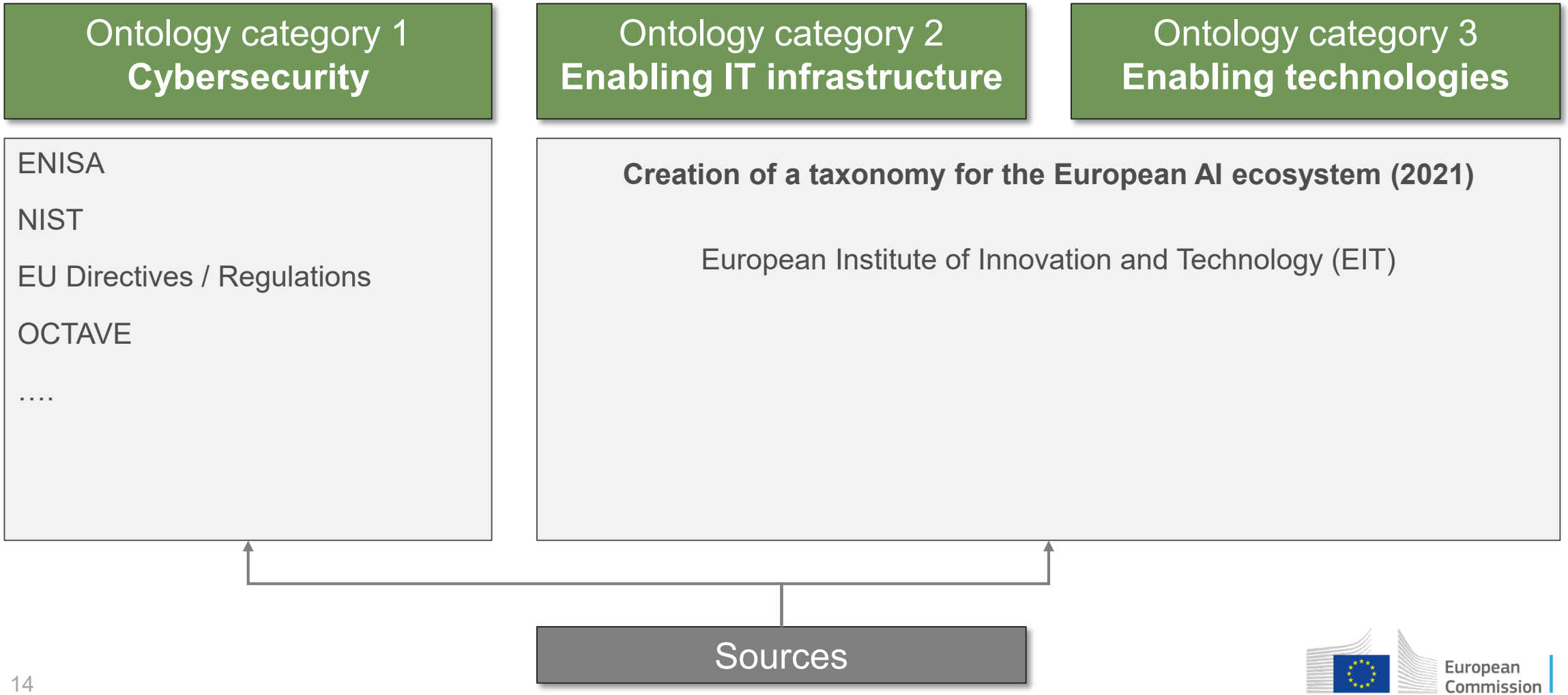
Comprehensive assessment and characterisation toolbox

Element 1 – Ontology: value chain enablers

Ontology category 1 **Cybersecurity**	Ontology category 2 **Enabling IT infrastructure**	Ontology category 3 **Enabling technologies**
Key terms and concepts of cybersecurity (e.g. threats, vulnerabilities, risks, attacks, incidents, scale, scope, seriousness).	Components necessary to operate and manage IT environments of organisations (e.g. IT hardware, cloud computing, computer software, network and storage infrastructure).	Platforms, frameworks and applications employed for the development, implementation and operation of AI systems (e.g. containerization solutions, data pipelining, code repositories or software products).

Comprehensive assessment and characterisation toolbox

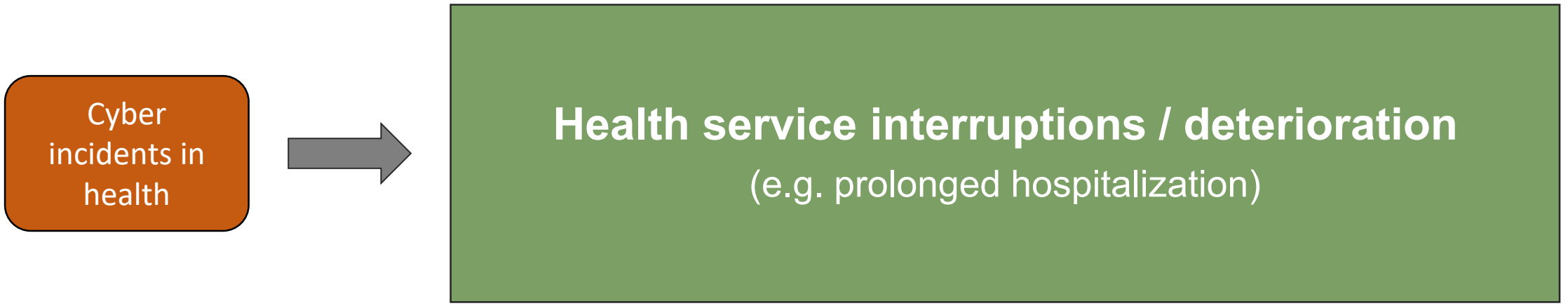
Element 1 – Ontology: value chain enablers



European Commission

Comprehensive assessment and characterisation toolbox

Element 1 – Ontology: health impacts

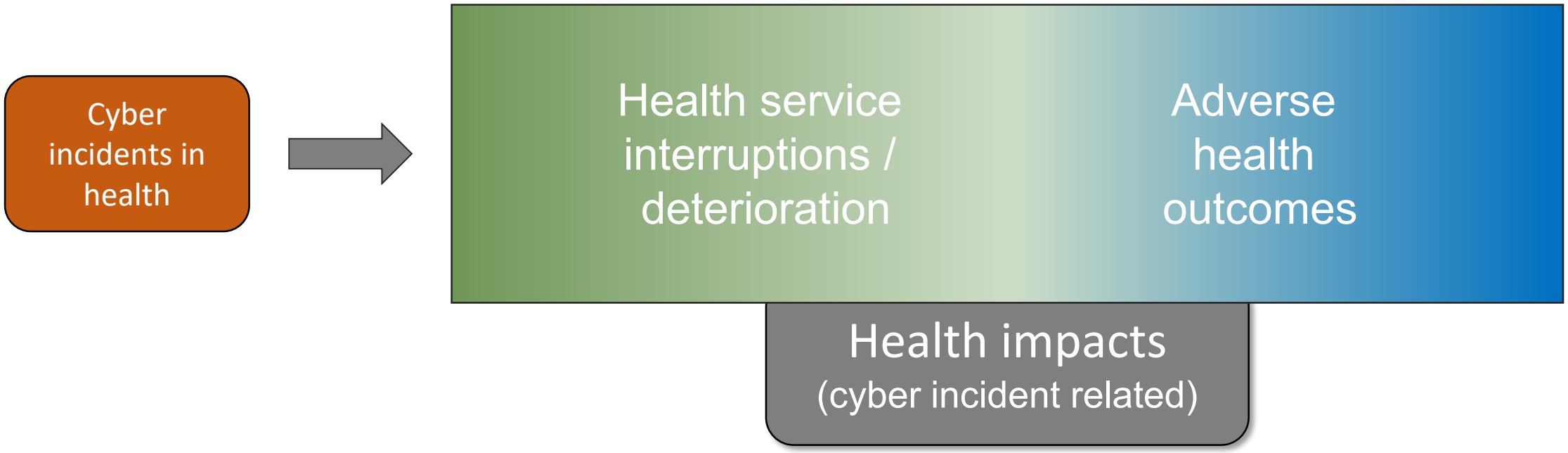


Comprehensive assessment and characterisation toolbox

Element 1 – Ontology: health impacts

Comprehensive assessment and characterisation toolbox

Element 1 – Ontology: health impacts



Comprehensive assessment and characterisation toolbox

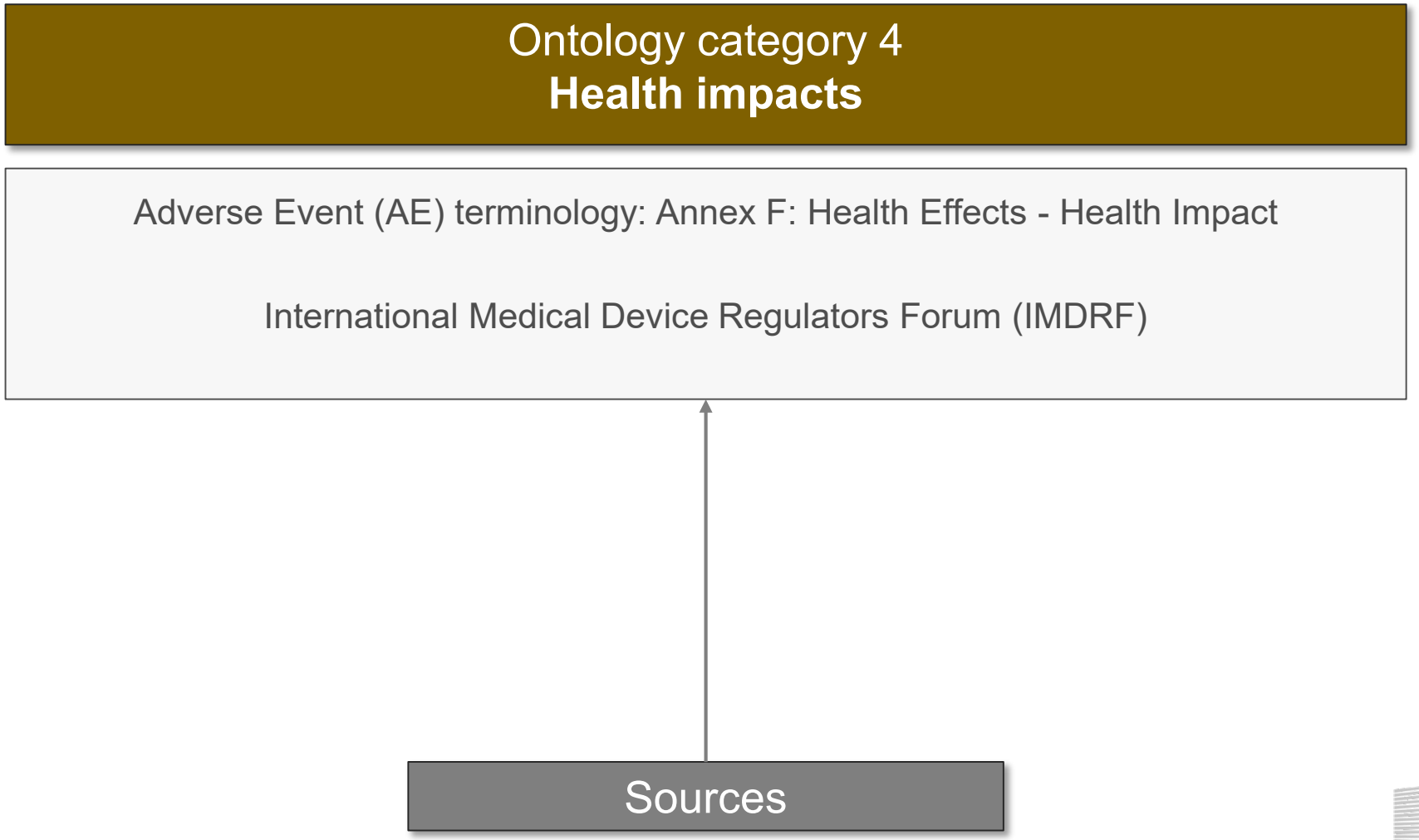
Element 1 – Ontology: health impacts

Ontology category 4
Health impacts

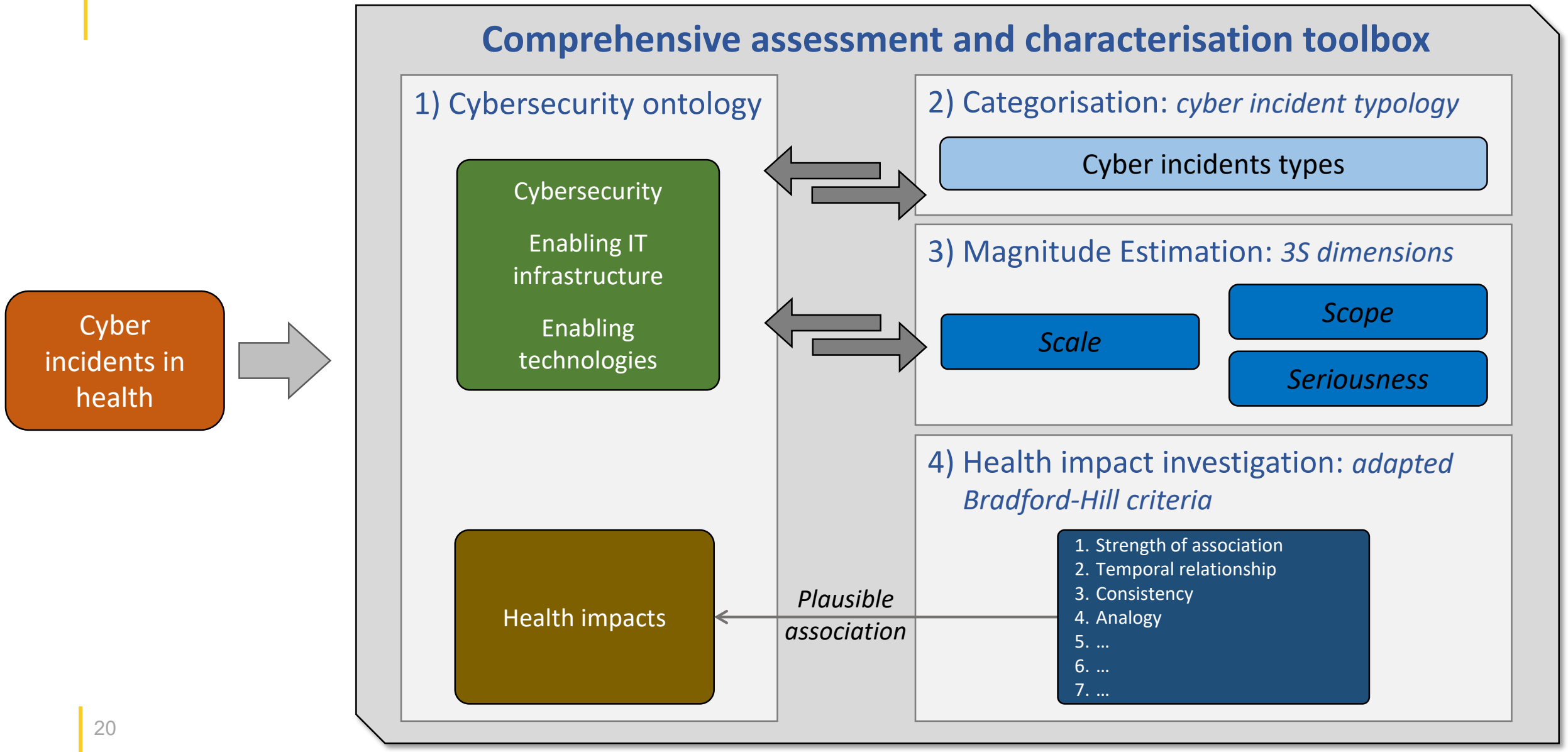
Additional Surgery	More Complex Surgery
Death	No Health Consequences or Impact
Delay to Diagnosis	No Patient Involvement
Delay to Treatment / Therapy	Prolonged Episode of Care
Disruption of Subsequent Medical Procedure	Prolonged surgery
Hospitalization or prolonged hospitalization	Serious Injury / Illness / Impairment
Inadequate/Inappropriate treatment or diagnostic exposure	Serious Public Health Threat
Insufficient Information	Surgical Procedure Delayed
Minor Injury /Illness / Impairment	Unexpected Deterioration
Misdiagnosis/Misclassification	Unexpected Diagnostic Intervention
Modified Surgical Procedure	Unexpected Medical Intervention

Comprehensive assessment and characterisation toolbox

Element 1 – Ontology: health impacts



Comprehensive assessment and characterisation toolbox



Comprehensive assessment and characterisation toolbox

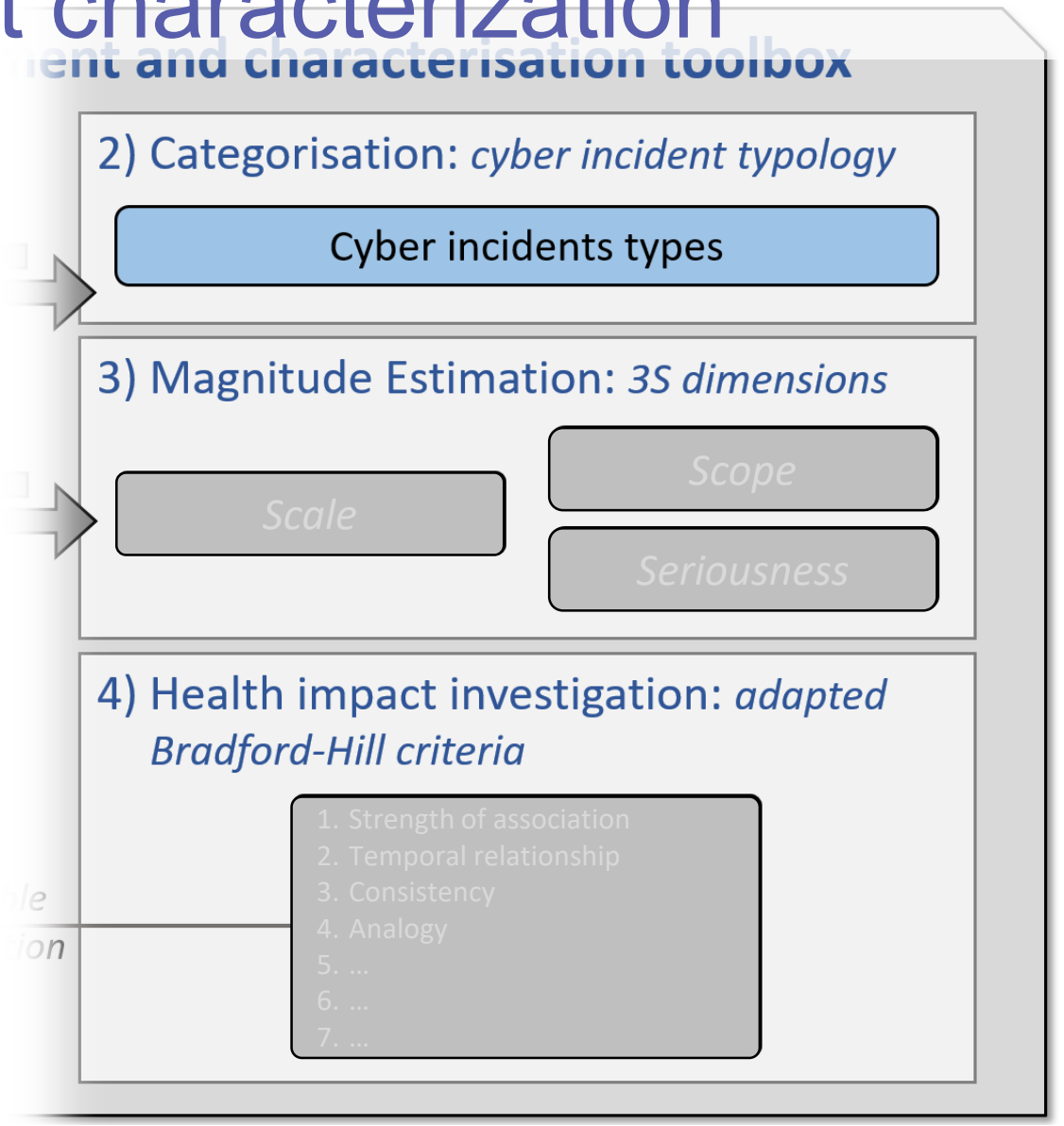
Element 2 – Cyber incident characterization

The function of this element is to **associate each cyber incident with a specific type**, enabling healthcare organizations to rapidly identify and categorize the nature of the incident.

The characterization process facilitates the implementation of targeted response strategies, ensuring that the organization's response is proportionate to the type of incident.

Examples of cyber incident types are:

- Incident compromising **availability and/or integrity of services**
- Incident involving critical **supply chains and availability of health products**
- …



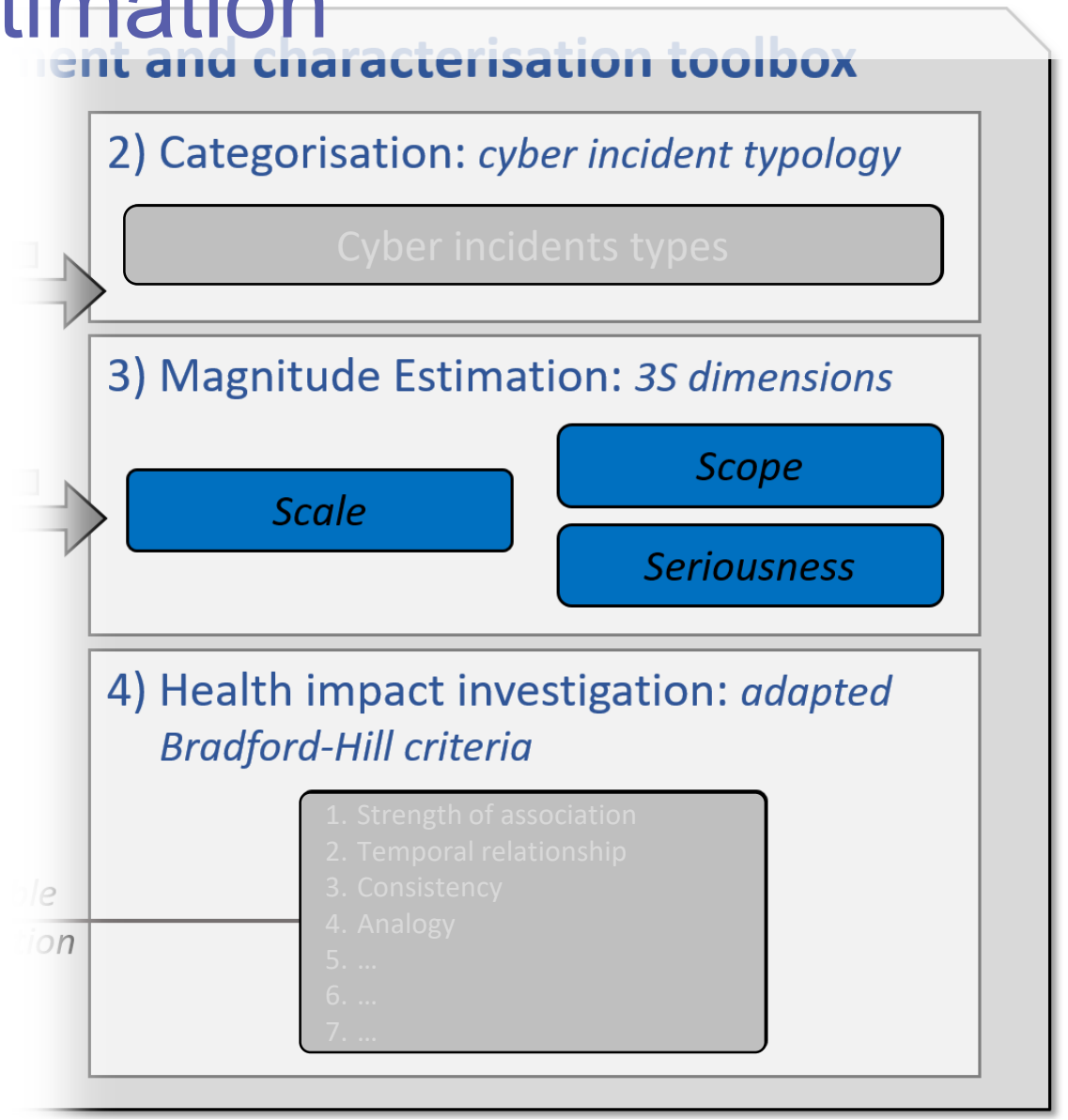
Comprehensive assessment and characterisation toolbox

Element 3 – Magnitude estimation

The function of this element is to estimate the magnitude of the incident based on a model comprising three dimensions:

- **Scale**: the extent and severity of the impacts at the entity targeted by the attack (e.g. a provider of cloud storage solutions, a company developing AI systems, a hospital)
- **Scope**: the "breadth" or "latitude" of the incident impact (e.g. geographical spread of stakeholders)
- **Seriousness**: the gravity of adverse impacts/damages experienced by the stakeholders (including individuals such as patients)

This multi-dimensional approach provides a comprehensive understanding of the incident, allowing healthcare organizations to allocate resources effectively and prioritize response efforts.



Comprehensive assessment and characterisation toolbox

Element 4 – Health impacts investigation

The function of this element is to establish a plausible correlation between cyber incidents and patient health impacts included in the 4th category of our ontology.

Adapted version of the *Bradford Hill criteria:* nine principles ideated in 1965 to establish epidemiologic evidence of a causal relationship between a presumed cause and an observed effect

Not checklist but means to evaluate the evidence and to highlight areas where further study is necessary.

Strength of Association

Consistency

Specificity

Temporal precedence

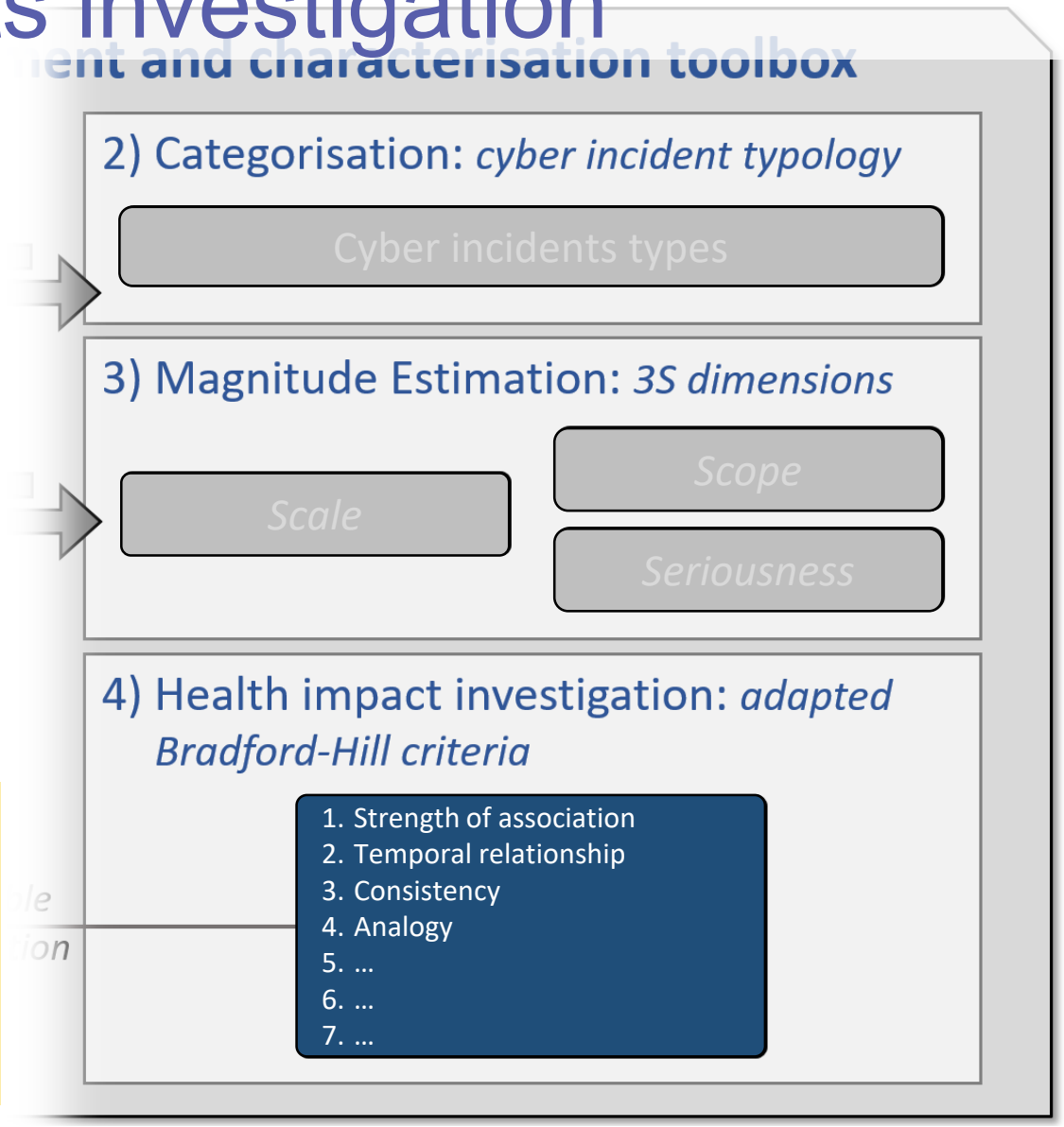
Dose-Response Relationship

Plausibility

Coherence

Experimentation

Analogy



Comprehensive assessment and characterisation toolbox

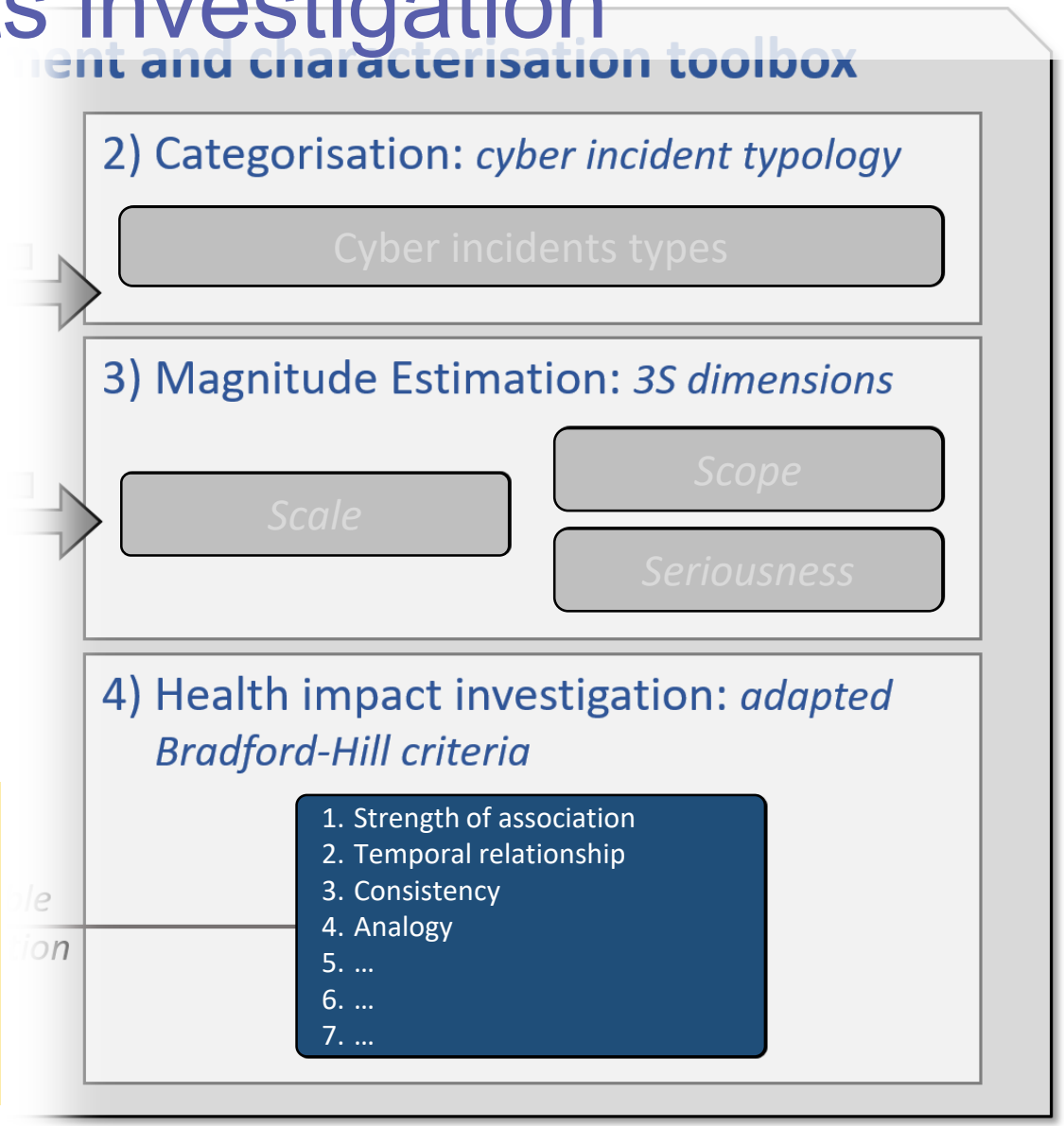
Element 4 – Health impacts investigation

The function of this element is to establish a plausible correlation between cyber incidents and patient health impacts included in the 4th category of our ontology.

Adapted version of the *Bradford Hill criteria:* nine principles ideated in 1965 to establish epidemiologic evidence of a causal relationship between a presumed cause and an observed effect

Not checklist but means to evaluate the evidence and to highlight areas where further study is necessary.

Analogy -> e.g. health care provider staff on strike, IT outage, power cut, lack of care delivery due to pandemic situations



Conclusions

- Without adequate tools, the human cost of cyber attacks in health may remain a blind spot of public health management and public health policies
- Our toolbox:
  - Provides a clear and consistent **set of terms and concepts** that are required for the comprehensive characterisation of cyber incidents in health (element 1 – the ontology)
  - Facilitates the implementation of targeted response strategies, ensuring that the organization's response is proportionate to the **type of incident** (element 2 - cyber incident characterization)
  - Provides a **comprehensive understanding of the incident**, allowing healthcare organizations to allocate resources effectively and prioritize response efforts (element 3 - magnitude estimation)
  - Enhance the analysis of **potential consequences of a cyber incident on patient care and health outcomes**, healthcare organizations can take proactive measures to mitigate harm and ensure the continued delivery of high-quality care efforts (element 4 - health impact assessment)

Thank you

Vittorio REINA, vittorio.reina@ec.europa.eu
Claudius GRIESINGER, claudius.griesinger@ec.europa.eu

EU Science Hub
joint-research-centre.ec.europa.eu

European Commission