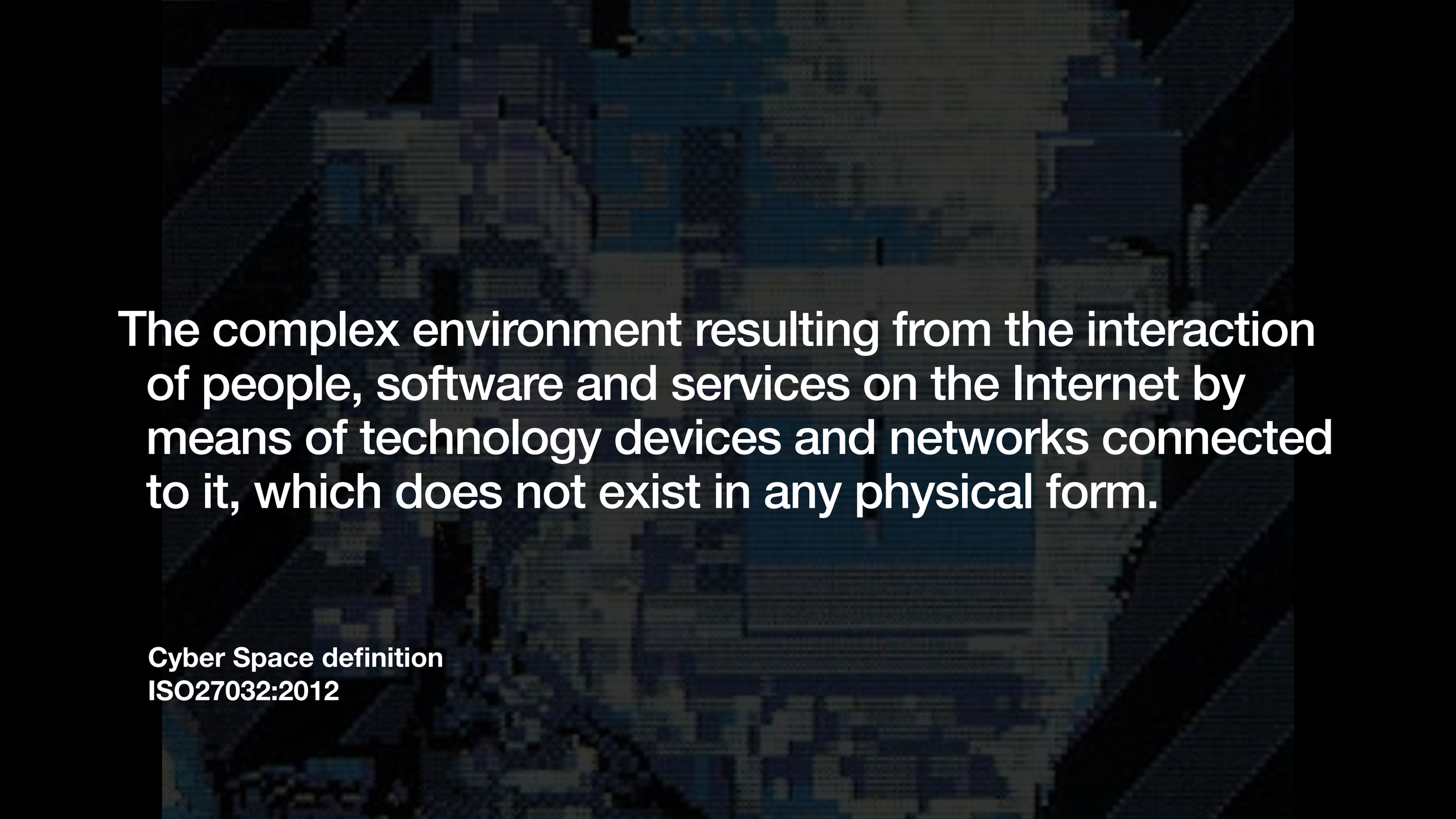
Cyber space and systems

Cyber space


The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.
Cyber Space definition
ISO27032:2012

Cyber space

- The Internet is a prominent example of a cyber space, but the two terms are not interchangeable.
- An alternative and more general definition of cyber space may lack the idea of being connected to the Internet.
- Realistically, many systems are connected to the Internet.
- NSFNET and APRANET are examples of cyber spaces predating the Internet.

Cyber space

- The European Union (EU), as well as the UK, effectively uses the term interchangeable with the Internet.
- The International Telecommunications Union (ITU) prefers the term ‘cyber environment’.
- The National Institute of Standards and Technology (NIST) emphasises cyber space within the context of critical infrastructures.

Cyber system

cyber system

- In simple terms a cyber systems are dependent or make use of a cyber space.
- It is important to understand that this dependency is potentially a vulnerability.
- Cyber-systems have become increasingly ubiquitous within societies and critical to modern economies.
- Such systems are so important to modern life, that they are often referred to as **critical infrastructure**.

Cyber-physical System

Cyber-physical System (CPS)

- Industry, increasingly academia as well, often focus and discuss cyber-physical systems.
- Cyber-physical systems are specific cyber systems that control and react to the physical environment.
- Such systems are common within industry (e.g. distributions of clothes, dispatching of goods etc).
- Networked actuators and sensors are becoming increasingly relevant beyond industry (e.g. smart grids, autonomous vehicles).

Cyber security

cyber security

- cyber security is the defence of cyber systems from **cyber threats**.
- cyber threats can be thought of any threat that makes use of a cyber space.
- threats to systems can be considered malicious or non-malicious.
- cyber security is not so much defined by the **kind of asset**, but rather the **threat to that asset**.

information security

- concerned with the protection of information assets.
- maintaining the **confidentiality**, **integrity** and **availability** of data.
- information is vulnerable from physical threats as well as cyber threats.

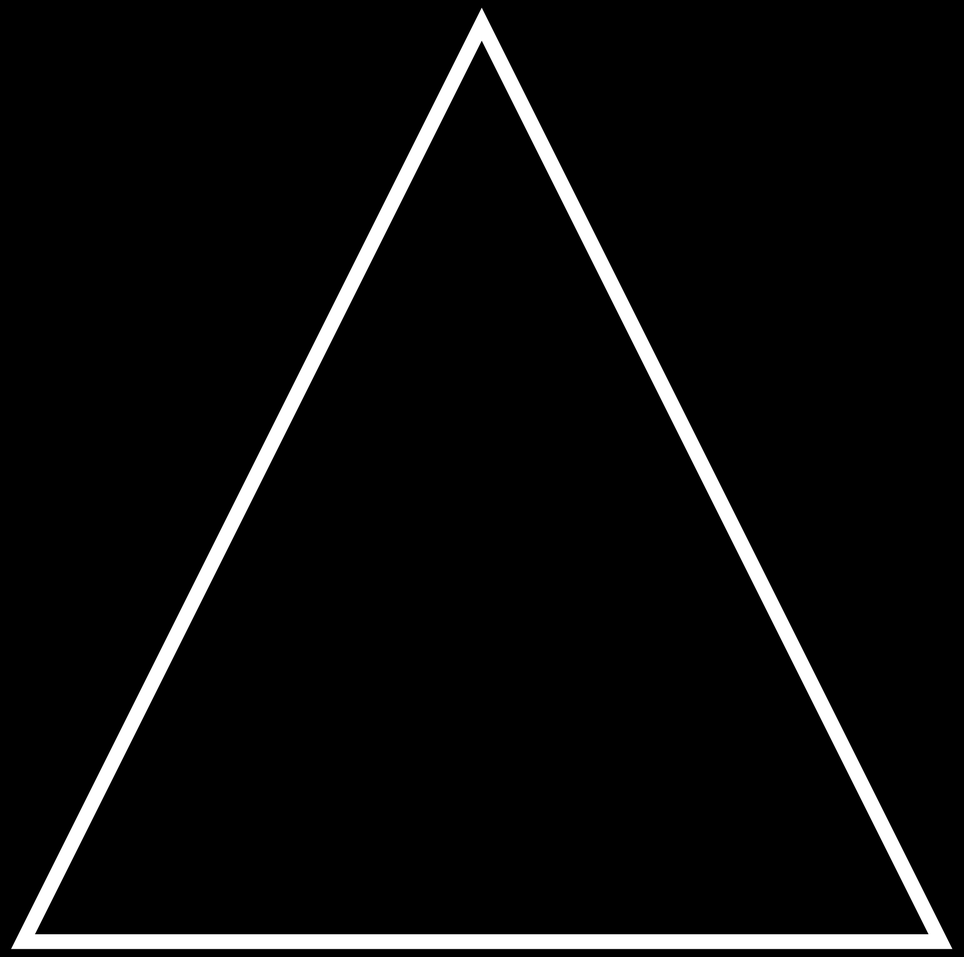
Cyber security and information security

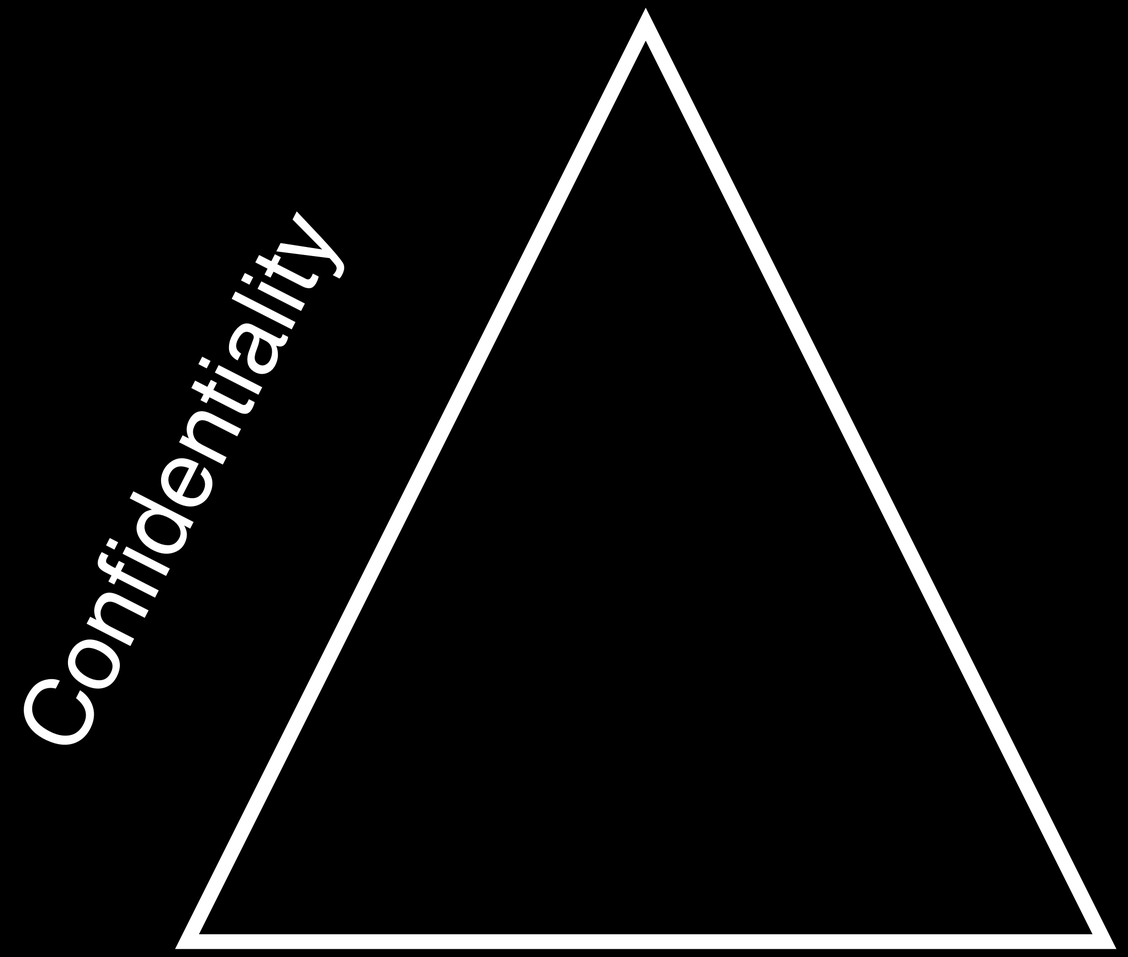
- standards and guidelines often conflate cyber security and information security.
- cyber security as a topic goes **beyond** the defence of information from cyber threats.
- nevertheless, Information Security goes **beyond** cyber security as it concerned about more than threats emerging from cyber space.

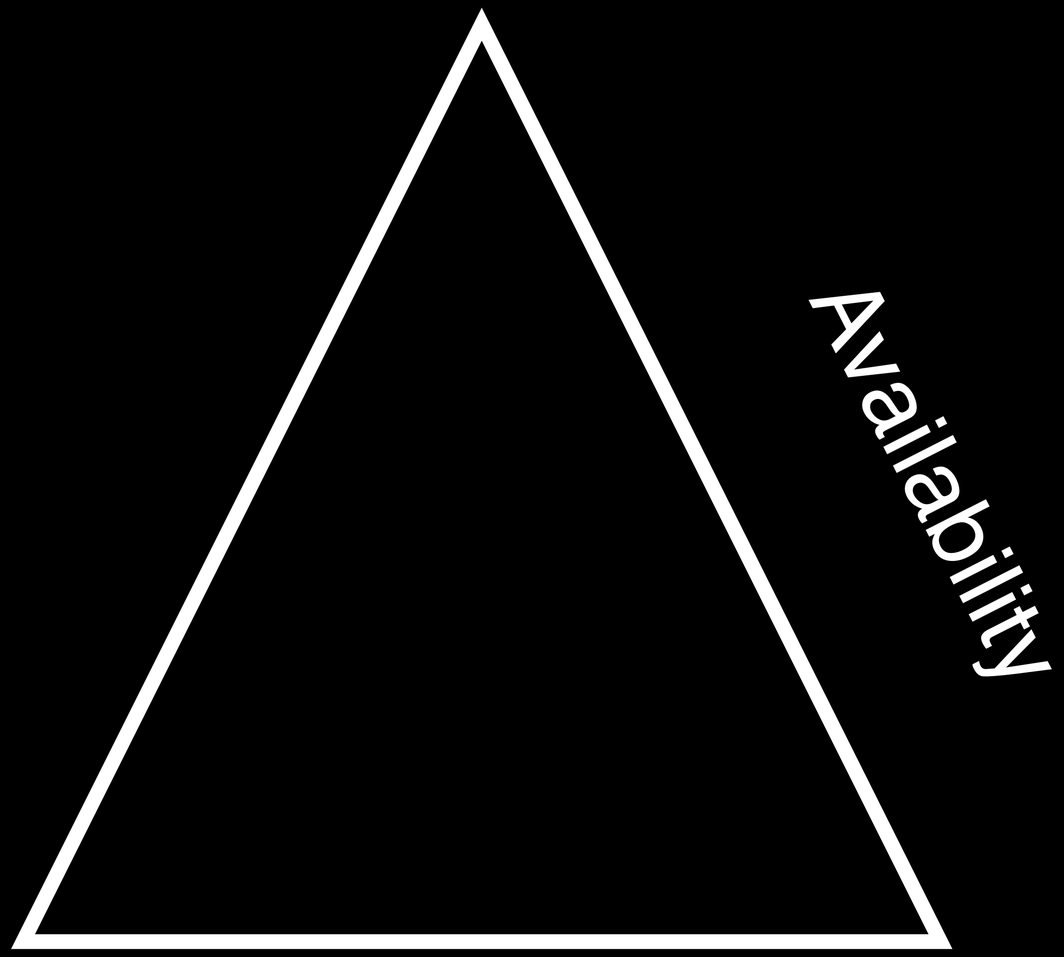
Preservation of confidentiality, integrity and availability of information.

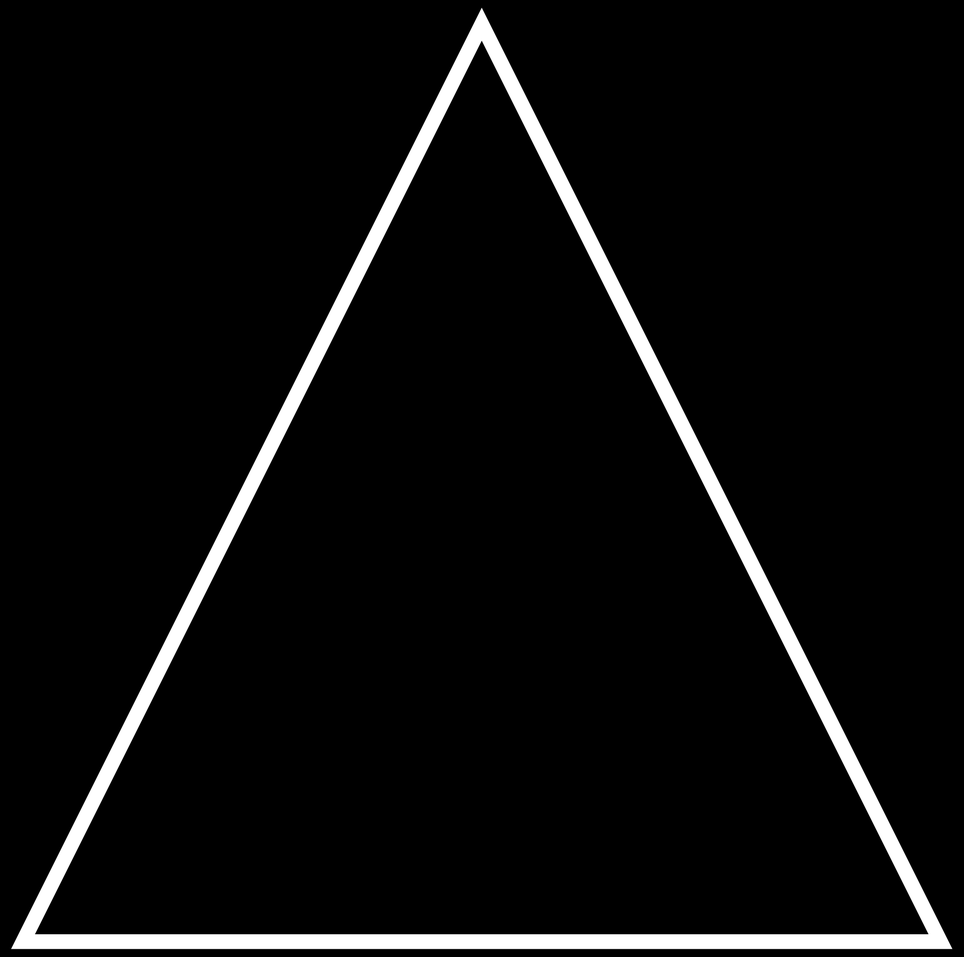
Information Security Definition
ISO27000:2016

CIA Triad

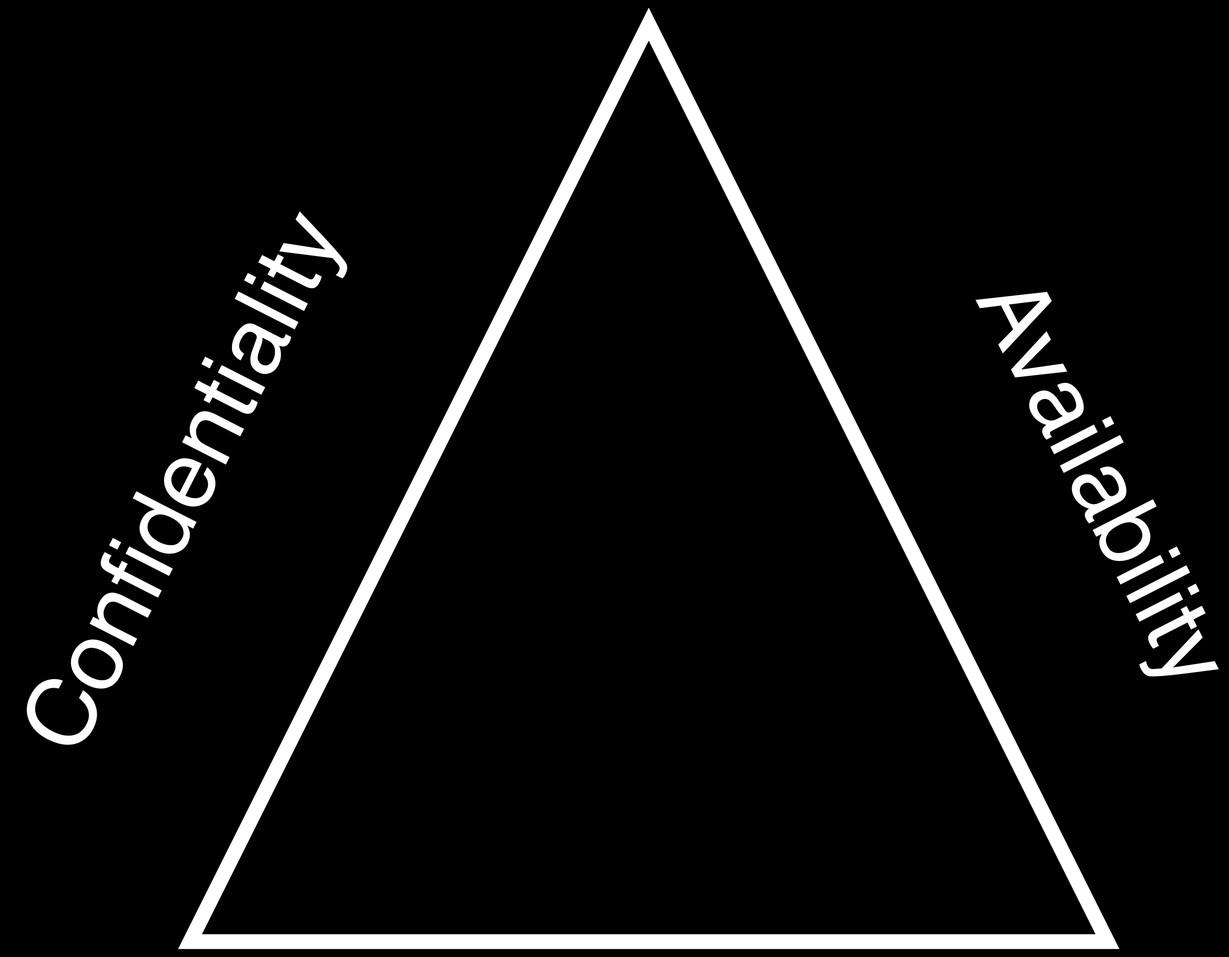



Confidentiality


Availability



Integrity


Confidentiality
Availability
Integrity

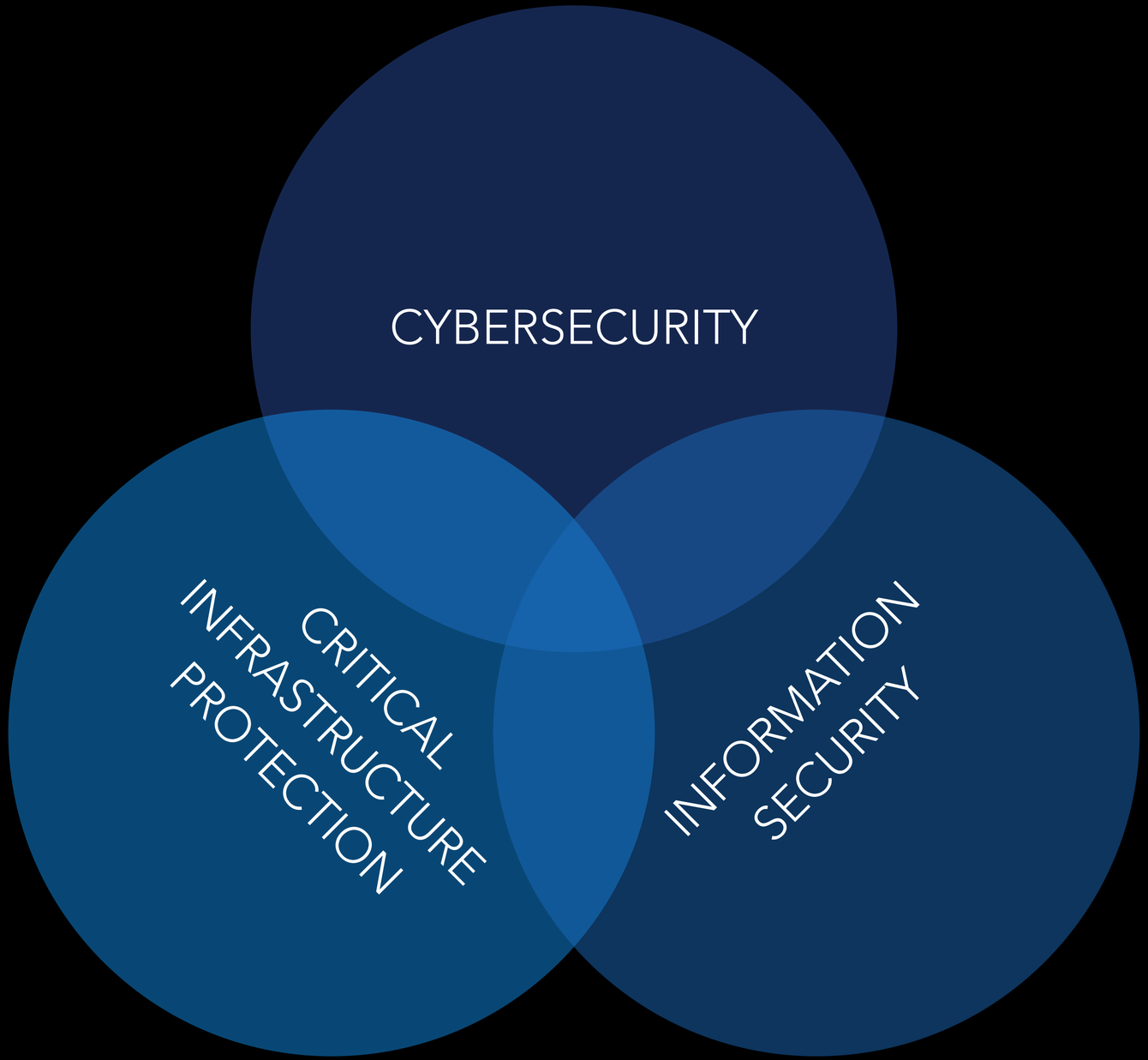
CIA Triad (ISO/IEC27000)

- **Confidentiality** is the property that information is not made available or disclosed to unauthorised individuals, entities or processes.
- **Integrity** is the property of accuracy and completeness.
- **Availability** is the property of being accessible and usable upon demand by an authorised entity.

Critical Infrastructure Protection

Critical Infrastructure Protection (CIP)

- Safeguarding infrastructure crucial to modern society from interruption and destruction.
- Critical infrastructure includes telecommunication networks, supplies of energy and water as well as emergency services.
- Critical infrastructure typical make use of a cyber space and needs protection from cyber threats.
- Critical infrastructure protection goes beyond cyber security as it also refers to systems that do not make use of a cyber space.


CYBERSECURITY
CRITICAL INFRASTRUCTURE PROTECTION
INFORMATION SECURITY

Safety

Safety

- Safety can be defined as being free from unacceptable risk to human life, injury or damage (IEC 61508).
- Safety is typically concerned with assets that are associated with human life and/or environment.
- Nevertheless, while they can be differentiated this does not mean that safety can not impact on cyber security.
- Similarly, cyber security incidents could have an impact on safety.

Cyber space and systems