D4 Data and Ethics

Autumn 2022 | Lecture 2 - Part I

Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Asprion | FHNW

KW	Date	Date	#	Topics	LernSetting WI	Lecturer
38 39	Self Study	First 2 weeks	0	Awareness - Entry Test with Moodle Test (20% counted to course grade)	Virtual	Selfstudy
38		KW38	0 + 7	Coaching Session (according to the information of the respective school)	on site	JRN= Juchler Norman Rerabek Martin Nyfeler Matthias
38	Fr, afternoon	23.09.2022	1	Personal Security	Virtual	Pascal Moriggl
39		KW39	1	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
39	Fr, afternoon	30.09.2022	2	Information Security & Cybersecurity I	Virtual	Petra M. Asprion
40		KW40	2	Coaching Session	on site	FHNW: Petra M. Asprion ZHAW: JRN
40	Fr, afternoon	07.10.2022	3	Information Security & Cybersecurity II	Virtual	Petra M. Asprion
41		KW41	3	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
41	Fr, afternoon	14.10.2022	4	Data Stewardship I	Virtual	Pascal Moriggl
42		KW42	4	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
42	Fr, afternoon	21.10.2022	5	Data Stewardship II	Virtual	Pascal Moriggl
43		KW43	5	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
43	Fr, afternoon	28.10.2022	6	Data Ethics	Virtual	Pascal Moriggl
44		KW44	6	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
44	Fr, afternoon	04.11.2022	7	Data Privacy	Virtual (Flipped Classroom)	Pascal Moriggl

Moodle Link: https://mslscommunitycentre.ch/course/view.php?id=113

MS Teams Link: https://teams.microsoft.com/l/meetup-join/19%3ameeting_YTdhMmU5ODQtZGMxYy00MmY2LWFjNzItMTA3NGU5OThlY2Rh%40thread.v2/0?context=%7b%22Tid%22%3a%229d1a5fc8-321e-4101-ae63-530730711ac2%22%2c%22Oid%22%3a%223fab2c24-f87a-4c23-91d5-b0e1bc7b5892%22%7d

Part I -- Intro: data & more	→ SD1
Part II -- From yesterday until today	→ SD2
Part III -- Organization Layer: Be informed!	→ SD3
Part IV -- Organization Layer: Be prepared -- GRCM	→ SD4
Coaching Session #2	→ SD5

→ SD = Slide Deck

Our topic --
Information Security and Cybersecurity (I&CS)

Now more than ever, every company is a data company

Our topic –
Information Security and Cybersecurity (I&CS)

By 2025, individuals and companies around the world will produce an estimated **463 exabytes of data** each day[1], compared with less than **3 exabytes** a decade ago[2].

[1] Jeff Desjardins, “How much data is generated each day?” World Economic Forum, April 17, 2019.
[2] IBM Research Blog, “Dimitri Kanevsky translating big data,” blog entry by IBM Research Editorial Staff, March 5, 2013

Our topic --
Information Security and Cybersecurity (I&CS)

McKinsey*: We define …

"data ethics as data-related practices that seek to preserve the trust of users, patients, consumers, clients, employees, and partners"

[1] 2022 McKinsey Data ethics: What it means and what it takes. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes?stcr=6D675D11F79B4EC8A9E9B7FAA420040F&cid=other-eml-alt-mip-mck&hlkid=b27c433530d34acd86f305e3fe95a250&hctky=10425183&hdpid=831f8eca-0c57-48a4-9757-061b1dfeb2222022

*McKinsey is a influential global management consulting firm founded in 1926 by University of Chicago professor James O. McKinsey, that offers professional services to corporations, governments, and other organizations.

Data and data related practices …

and here comes into account:

Information Security and **Cybersecurity** (I&CS)[1] --

because they refer to the same thing:

to protect data
from unauthorized access
and to preserve trust.

[1] In context of this course, we use I&CS interchangeably where it makes sense and otherwise we explicitly point out the differences.

Our topic --
Information Security and Cybersecurity (I&CS)

Data

?

Our topic --
Information Security and Cybersecurity (I&CS)

Information ?

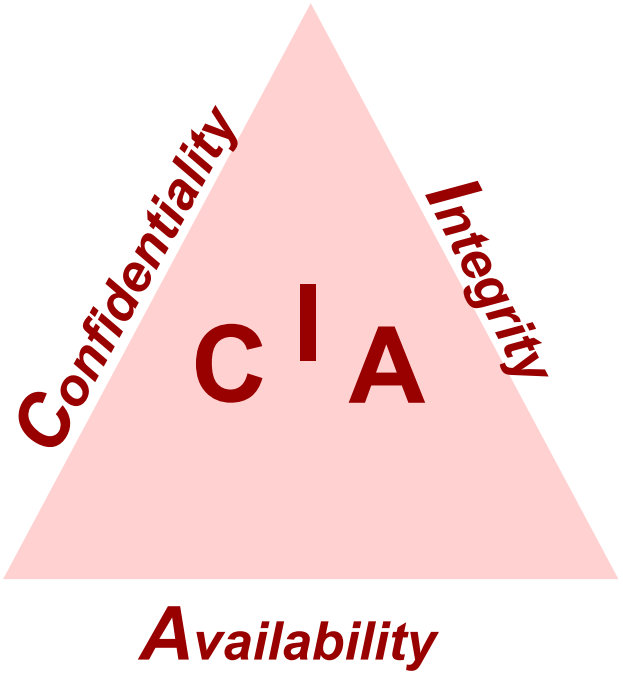
Who has the sovereignty of interpretation?

Information Security and **Cybersecurity** (I&CS)[1] -- what do these terms mean?

In their most basic forms, they refer to the same thing: the **confidentiality**, **integrity** and **availability** of information

The concept of the CIA triad

a well-known model for security policy development, used to identify problem areas and necessary solutions for information security.



Confidentiality -- restrict access to authorized individuals

Integrity -- data has not been altered in an unauthorized manner

Availability -- information can be accessed and modified by authorized individuals in an appropriate timeframe

Source: 2012, Perrin, Chad. "The CIA Triad"

Have a look: https://www.youtube.com/watch?v=bhLbnOa4wno

Our topic --
Information Security and Cybersecurity (I&CS)

Information Security

versus

Cybersecurity

Information Security …

ensures that, within the enterprise, information is protected against disclosure to unauthorized users (**confidentiality**), improper modification (**integrity**) and nonaccess when required (**availability**). Information security deals with all formats of information — paper documents, digital assets, intellectual property in people's minds, and verbal and visual communications.

ISACA glossary - https://www.isaca.org/resources/glossary

Note: ISACA glossary is a recognized and highly up-to-date reference work for almost all terms related to (IT) Governance, Risk and Compliance. Highly recommended when adequate explanations of terms are required (e.g., in the master thesis).

Information Security enhancements …

Information security governance

The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly.

Information security program

The overall combination of technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis.

Information security testing tools

Tools used to test the accuracy and completeness of an enterprise's cybersecurity practices and controls.

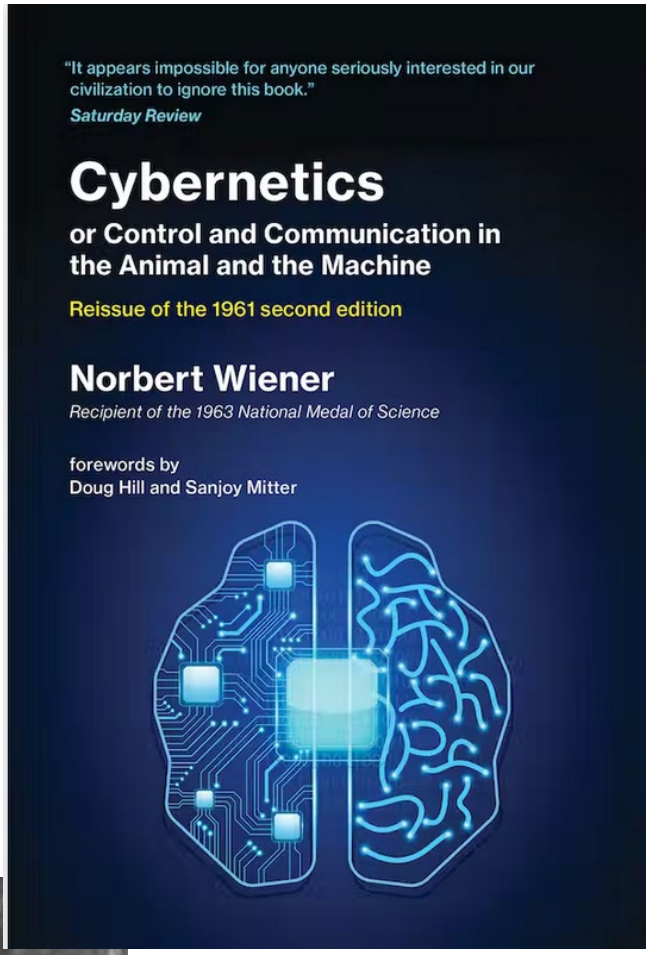
ISACA glossary - https://www.isaca.org/resources/glossary

Cybersecurity … Cybernetics

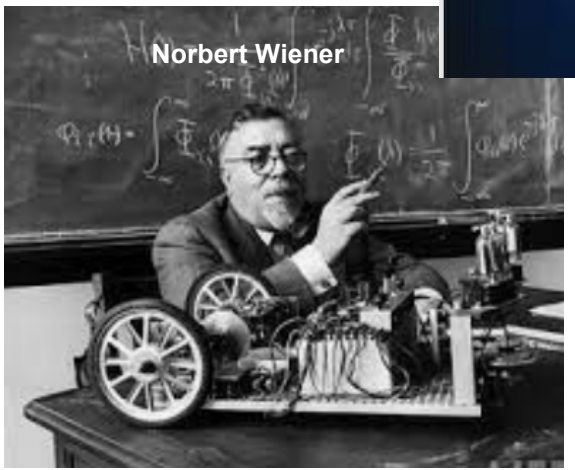
The term **cybernetics** was developed and first used by Norbert Wiener in his book "Cybernetics or Control and Communication in the Animal and the Machine" (MIT Press, 1948).

He used the term in reference to the **control of complex systems**.

→ The term "cyber" has a long cultural background through which the term has become commonplace, and inevitably multi-nuanced.



https://mitpress.mit.edu/9780262537841/cybernetics-or-control-and-communication-in-the-animal-and-the-machine/



Source: ENISA (2015) Definition of Cybersecurity – Gaps and overlaps in standardisation. www.enisa.europa.eu/publications/definition-of-cybersecurity

Cybersecurity is … (1/3)

1. the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems

2. the protection and restoration of products, services, solutions, and supply chain; including technology, computers, telecommunications systems and services, and information; to ensure their availability, integrity, authentication, transport, confidentiality, and resilience. Cybersecurity is a part of information security (CMMI)

ISACA glossary - https://www.isaca.org/resources/glossary

Note: There are different spellings of cybersecurity; to get a sound overview the 2015´ ENISA paper “Definition of Cybersecurity – Gaps and overlaps in standardisation” is recommended (see also on Moodle).
In this course we use the spelling 'cybersecurity'.

Cybersecurity is … (2/3)

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

Source(s):

CNSSI 4009-2015 from NSPD-54/HSPD-23

NIST SP 1800-10B under Cybersecurity from CNSSI 4009-2015, NSPD-54/HSPD-23

NIST SP 1800-25B under Cybersecurity from CNSSI 4009-2015, NSPD-54/HSPD-23

NIST SP 1800-26B under Cybersecurity from CNSSI 4009-2015, NSPD-54/HSPD-23

NIST SP 800-160 Vol. 2 Rev. 1 from CNSSI 4009-2015

NIST SP 800-37 Rev. 2

NIST SP 800-53 Rev. 5 from OMB Circular A-130 (2016)

NISTIR 7621 Rev. 1 under Cybersecurity from CNSSI 4009-2015

NIST glossary https://csrc.nist.gov/glossary/term/cybersecurity

Cybersecurity is … (3/3)

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

the process of protecting information by preventing, detecting, and responding to attacks

Source(s):

NIST SP 800-160 Vol. 2 Rev. 1 from NIST Cybersecurity Framework Version 1.1

NIST Cybersecurity Framework Version 1.1 under Cybersecurity

NISTIR 8183 under Cybersecurity from NIST Cybersecurity Framework Version 1.1, NIST Cybersecurity Framework Version 1.0

NISTIR 8183 Rev. 1 under Cybersecurity from NIST Cybersecurity Framework Version 1.1

NISTIR 8183A Vol. 1 under Cybersecurity from NIST Cybersecurity Framework Version 1.1

NISTIR 8183A Vol. 2 under Cybersecurity from NIST Cybersecurity Framework Version 1.1

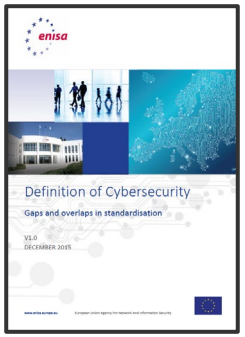
NISTIR 8183A Vol. 3 under Cybersecurity from NIST Cybersecurity Framework Version 1.1

NIST glossary https://csrc.nist.gov/glossary/term/cybersecurity

Cybersecurity Domains

Figure 1: Different domains of Cybersecurity

ENISA (2015) Definition of Cybersecurity - Gaps and overlaps in standardisation. https://www.enisa.europa.eu/publications/definition-of-cybersecurity



See on Moodle

Communications Security: Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users.

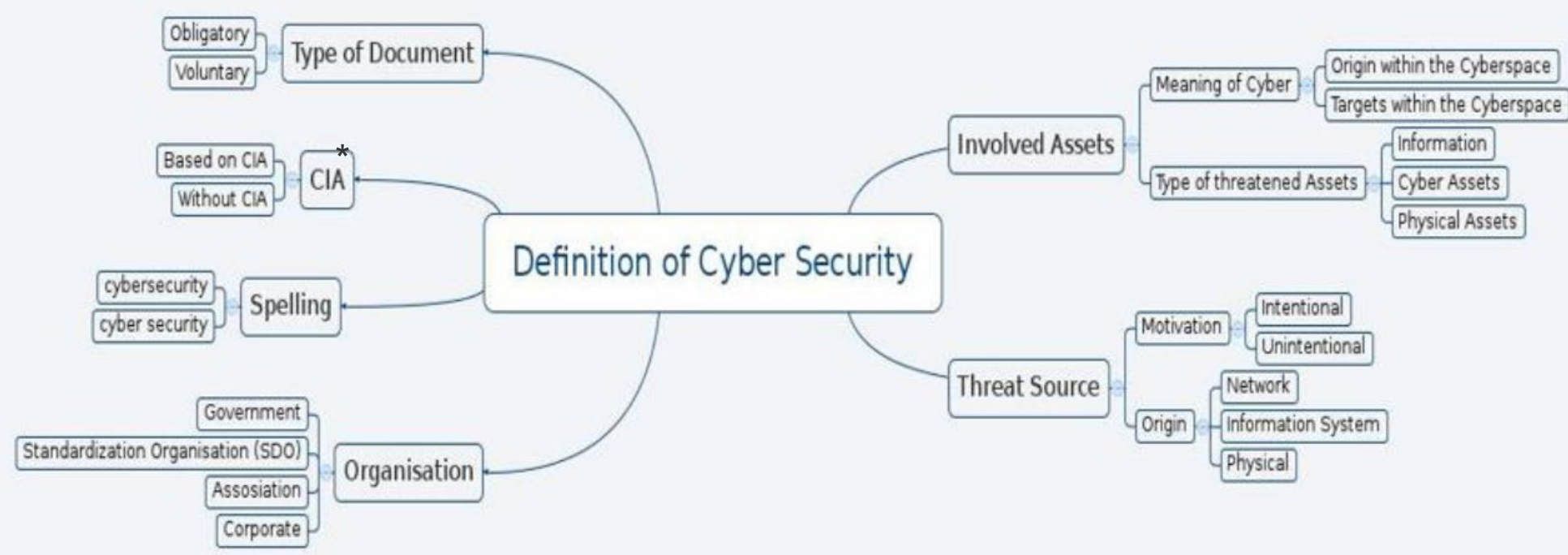
Operations Security: Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users.

Information Security: Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system.

Physical Security: Protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families.

Public/National Security: Protection against a threat whose origin is from within cyberspace, but may threaten either physical or cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications financial system or other critical public or industrial infrastructures.

Composition of the Term (1/2)

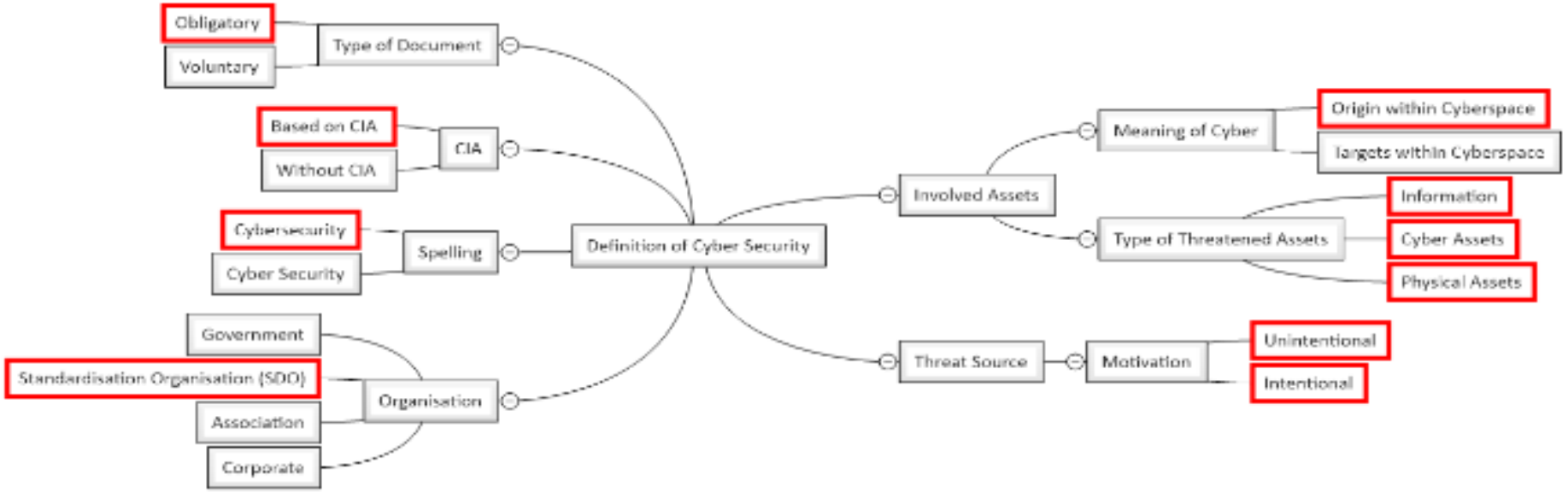


* Based on CIA: The definition of 'Cybersecurity' uses and addresses the terms 'Confidentiality', 'Integrity' and 'Availability'

A deconstruction of the components that make up the definition of the 'Cybersecurity' domain is illustrated above. This diagram looks at the various aspects of the definition which are referred to and implied when the definition is used by stakeholders. This wide range of components adds to the wide variations in meaning of the term and has a potential to obscure the true scope of a particular cybersecurity action or intention.

Source: ENISA, 2015. https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Composition of the Term (2/2)
Inclusion of components by NIST*



*NIST is the National Institute of Standards and Technology, a unit of the U.S. Commerce Department. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.

Source: ENISA, 2015. https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Cybersecurity – Terminology as defined by dictionaries

Oxford

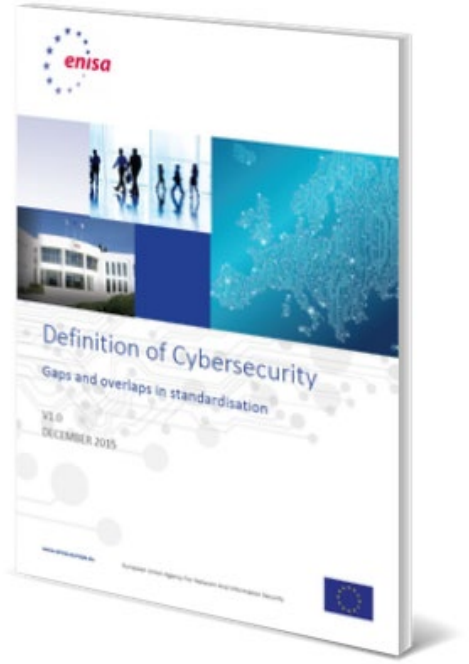
The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

http://www.oxforddictionaries.com/definition/english/cybersecurity?q=cyber+security

Merriam Webster

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

http://www.merriam-webster.com/dictionary/cybersecurity



Download
PDF document, 1.57 MB

https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Some Glossaries of Security Terms …

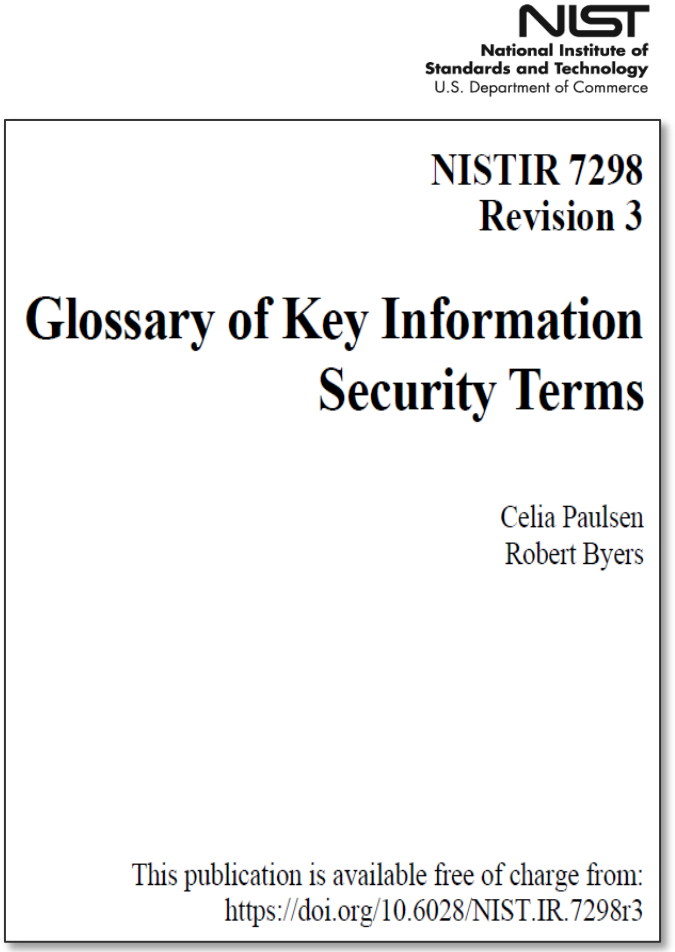
BSI
https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

ISACA (online)
https://www.isaca.org/resources/glossary

NIST (online)
https://csrc.nist.gov/glossary

NICCS
https://niccs.us-cert.gov/about-niccs/glossary#I

SANS https://www.sans.org/security-resources/glossary-of-terms/



Related online glossary from NIST: https://csrc.nist.gov/glossary

Standardisation work in Cybersecurity

Organisation	Type of organisation	Summary
3GPP – 3rd Generation Partnership Project	SDO partnership	3GPP unites six telecommunications standard development organizations (TTA, TTC), and provides thei
CableLabs	Indu	
CEN – Comité Européen de Normalisation	Euro	
GlobalPlatform	Industry forum	G a p a o It t e h
GSMA – GSM Association	Industry forum	G r t G g d c o e C h
IEEE – Institute for Electrical and Electronic Engineers	Industry forum	T e a a C la S escalating its ongoing involvement in the field of cybersecurity. Its standards activities are principally in the area of SmartGrid and other critical infrastructure security. http://www.ieee.org/
ISO – International Organization for Standardization	Global SDO	The ISO is a Swiss based private interna standards development and publishing composed of representatives from vari standards organizations with multiple c – several of which have significant Cybe related activity. http://www.iso.org
ITU – International Telecommunication Union	Global SDO	The ITU is a Swiss based intergovernme with three sectors dealing with the dev and publication of Recommendations fo systems (ITU-R), telecommunications (I development assistance (ITU-D). https://www.itu.int
OASIS – Organization for the Advancement of Structured Information Standards	Independent industry forum	OASIS is a major global industry body fo developing and publishing worldwide st security, Internet of Things, cloud comp energy, content technologies, emergen management, and other areas requiring information exchange. Although it bega on XML language schema, it has subseq expanded to JSON. Its currently hosts t Cybersecurity technical committees list https://www.oasis-open.org/org
OMG – Object Management Group	Industry forum	OMG is a computer industry consortium enterprise integration standards. The G principal current Cybersecurity work de threat modelling where its System Assu Force Security Fabric Working Group is a Unified Modeling Language Threat & I http://sysa.omg.org/

Source: ENISA, 2015. https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Our topic --
Information Security and Cybersecurity (I&CS)

Influential Organisations

(you should know)

ABOUT ENISA -- The European Union Agency for Cybersecurity. Towards a Trusted and Cyber Secure Europe

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

Watch the video (2.02)

Source: ENISA, 2022, https://www.enisa.europa.eu/about-enisa

ABOUT NIST -- The National Institute of Standards and Technology.

The NIST was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time - a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.

Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations - from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.

Watch the video (2.16)

Source: NIST, 2022, https://www.nist.gov/about-nist

ABOUT ISO -- International Organization for Standardization

ISO is an independent, non-governmental international organization with a membership of 167 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

You'll find the Central Secretariat in Geneva, Switzerland.

Watch the video (0.46)

https://www.youtube.com/watch?v=hCAa7OWdjfo

Source: ISO, 2022, https://www.iso.org/about-us.html

ABOUT ISACA --

Today, ISACA's constituency of more than 165,000 strong worldwide is characterized by its diversity. These professionals live and work in more than 180 countries and cover a variety of professional IT-related positions in the disciplines of IS/IT audit, risk, security and governance as well as educators, consultants and regulators. … They work in nearly all industry categories, including financial and banking, public accounting, government and the public sector, utilities and manufacturing.

You'll find the Swiss Chapter in Zurich (https://www.isaca.ch/en/).

https://www.isaca.org/why-isaca/about-us/history

The Pursuit of Digital Trust Starts Today …

"*The modern world relies on the digital space to get business done.*
But with the increase in cyberattacks, scams and security breaches, a secure digital world is more important than ever.
ISACA is leading the way in the pursuit of digital trust — creating a digital ecosystem where value is created and confidence is the norm."

What have we discussed so far?

Relevance of **data** in 2022

Definitions and Differentiations of data & information

Definitions and Differentiations of I&CS

Concept of CIA

Influential organisations *(you should know)*

And nearby ...

Evidence from sources

Some of the most (not all) important organizations that provide a certain instance of definition and interpretation.

Some topic related frameworks – at least their citation