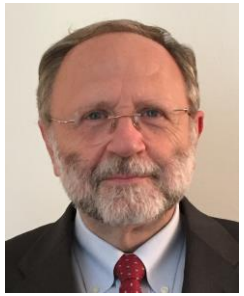
Panacea

People-centric cybersecurity in healthcare

Public and Private Healthcare Organisations: a Socio-Technical Model for Identifying Cybersecurity Aspects



Speaker:
Pasquale Mari
Gemelli Policlinic Foundation-Italy
Panacea Project Deputy Coordinator

ICEGOV-Paper Session 3: Security, Privacy and Ethics in Digital Governance
23 September 2020

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

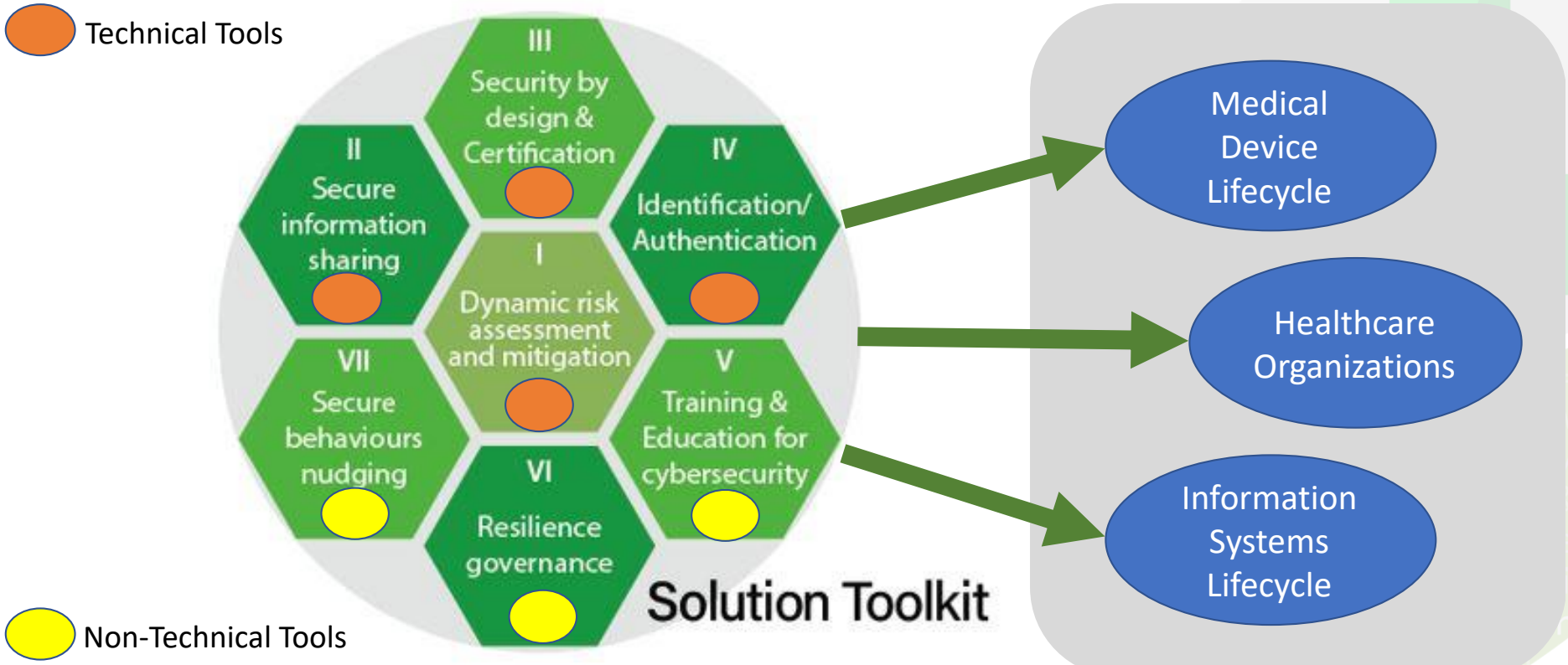
Topics

1. Introduction: why a model?
2. Approach: how the model was built?
3. Entities and taxonomies: what the model is?
4. Examples of application: how the model can be used?
5. Contribution to security regulation: how the model can help?

Appendix

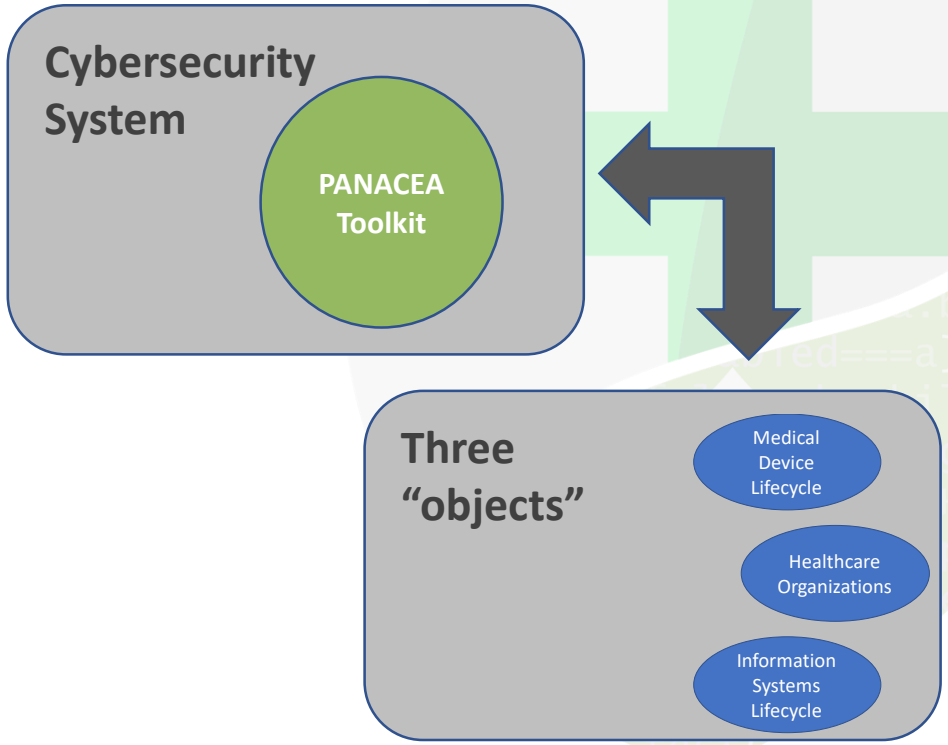
1. Introduction: why a model? (1/2)

- The Socio-Technical Model described in the article and in this presentation has been set-up by the **PANACEA Project**, a Horizon 2020 funded project running from January 2019 to December 2021, aiming to deliver **people-centric cybersecurity solutions in healthcare**
- PANACEA will deliver a **Solution Toolkit** to ensure cybersecurity in **three types of "objects"**



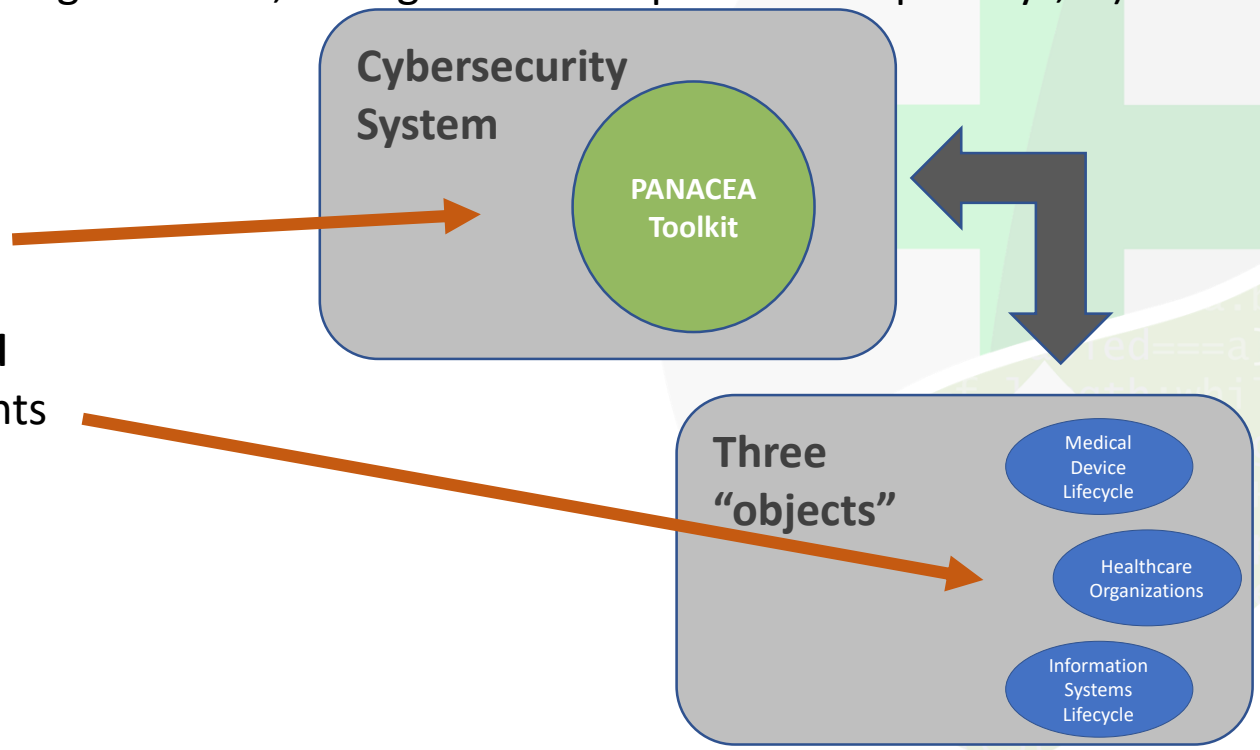
1. Introduction: why a model? (2/2)

- In PANACEA we needed a **descriptive model** to
  - **customize** the PANACEA Toolkit **to the Healthcare context**
  - **harmonize project operations and output** with a common language across the 7 Tools, the 9 Work Packages and 44 Tasks, the 15 Partners
  - **facilitate the adoption** of the PANACEA Toolkit **in existing hospital's cybersecurity systems**
- In particular the model was needed to describe
  - the **three "objects"** in a manner relevant from the cybersecurity perspective and for the project
  - a **cybersecurity system** and the position of the PANACEA toolkit inside it
  - the **relationship** between the cybersecurity system and the three objects



2. Approach: how the model was built? (1/3)

- **Healthcare providers** attracts cybercrime because not only they are a rich source of valuable data, but they also have **weak defences against cybercrime, due to**
  - **Dynamic Complexity** (IT + Networked Medical Devices + thousands of access points and users; frequent deployment of new devices and sw applications)
  - **Barriers to the adoption** of security solutions (skill shortage, budget constraints,…) .
  - **Human error (**due to overwhelming workload, strong culture of "patient care priority", …)
- As a consequence, Cybersecurity solutions :
  - **must include organizational measures**
  - **must consider also humans and business activities** as components of the reality to be protected



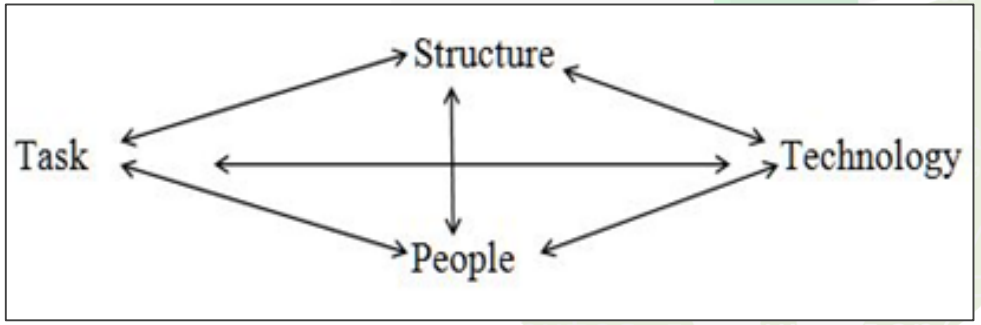
2. Approach: how the model was built? (2/3)

- The literature provides **two approaches** for building models of systems including both technological and organizational components.

- ***Enterprise Architecture (EA).*** There are many versions of EAs Most represent an enterprise using five interconnected descriptive layers

Business
Process
Software
Data
Infrastructure

- ***Socio-Technical-Systems (STS).*** The EA approach misses a critical aspect: *people and their formal relationship (structure)*. We adopted the STS approach because it fills this gap.

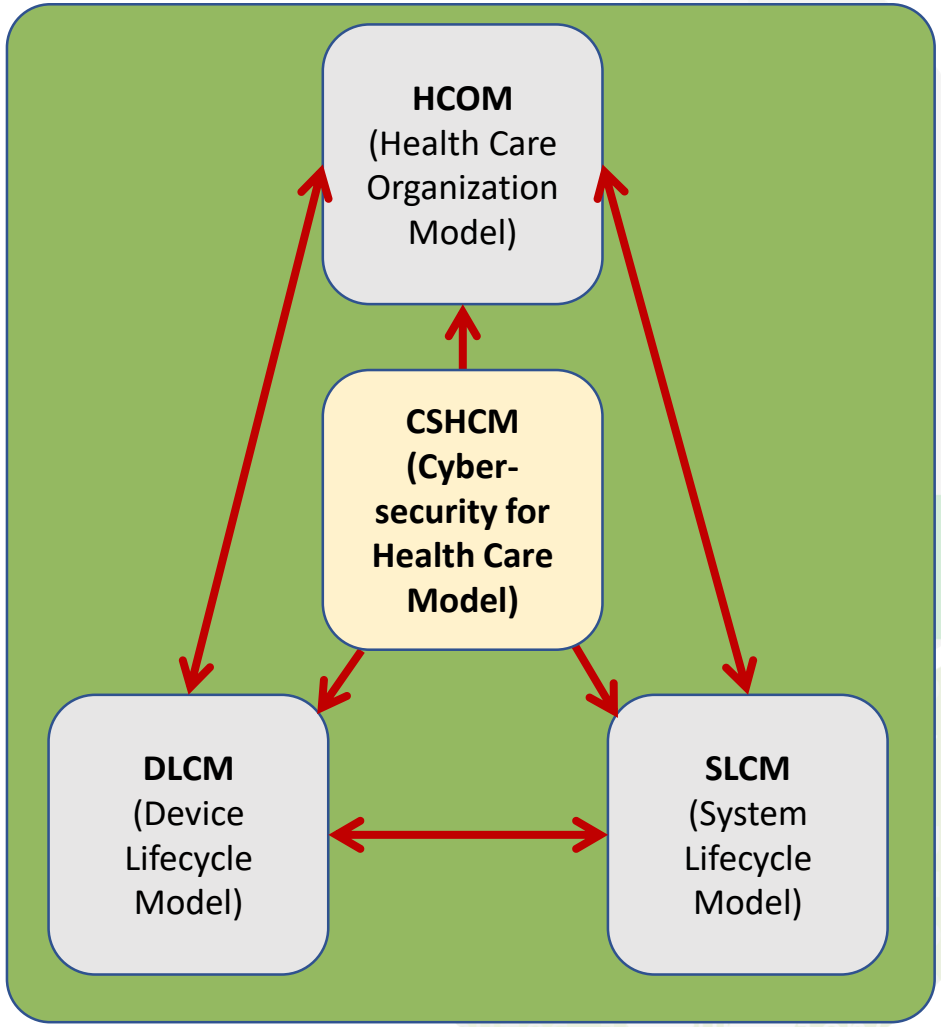


2. Approach: how the model was built? (3/3)

- **Modelling** was performed in **five main steps**:
  - **Scope**: state models' purpose and requirements (context, content, use, key variables);
  - **Literature review**: search for applicable modelling approaches, models or parts of models in literature;
  - **1st version**: define tentative models and instantiation schemes, adopting when possible, descriptive components already available in the literature;
  - **Validation**: validate the models in real settings, using the instantiation schemes;
  - **Final version**: fine-tune and finalise the model.
- The **validation** has been performed by instantiating the models to describe **real systems**
  - the **healthcare organisation** and **cybersecurity system** of
    - Gemelli Hospital, Rome, Italy, private
    - 7th Health Region of Crete, Greece, public
    - South-South-West Hospital Group, Ireland, public
  - the **lifecycle of a medical device** (QTrobot, an assistive robot)
  - the **lifecycle of a software application** (Gemelli clinical trial).

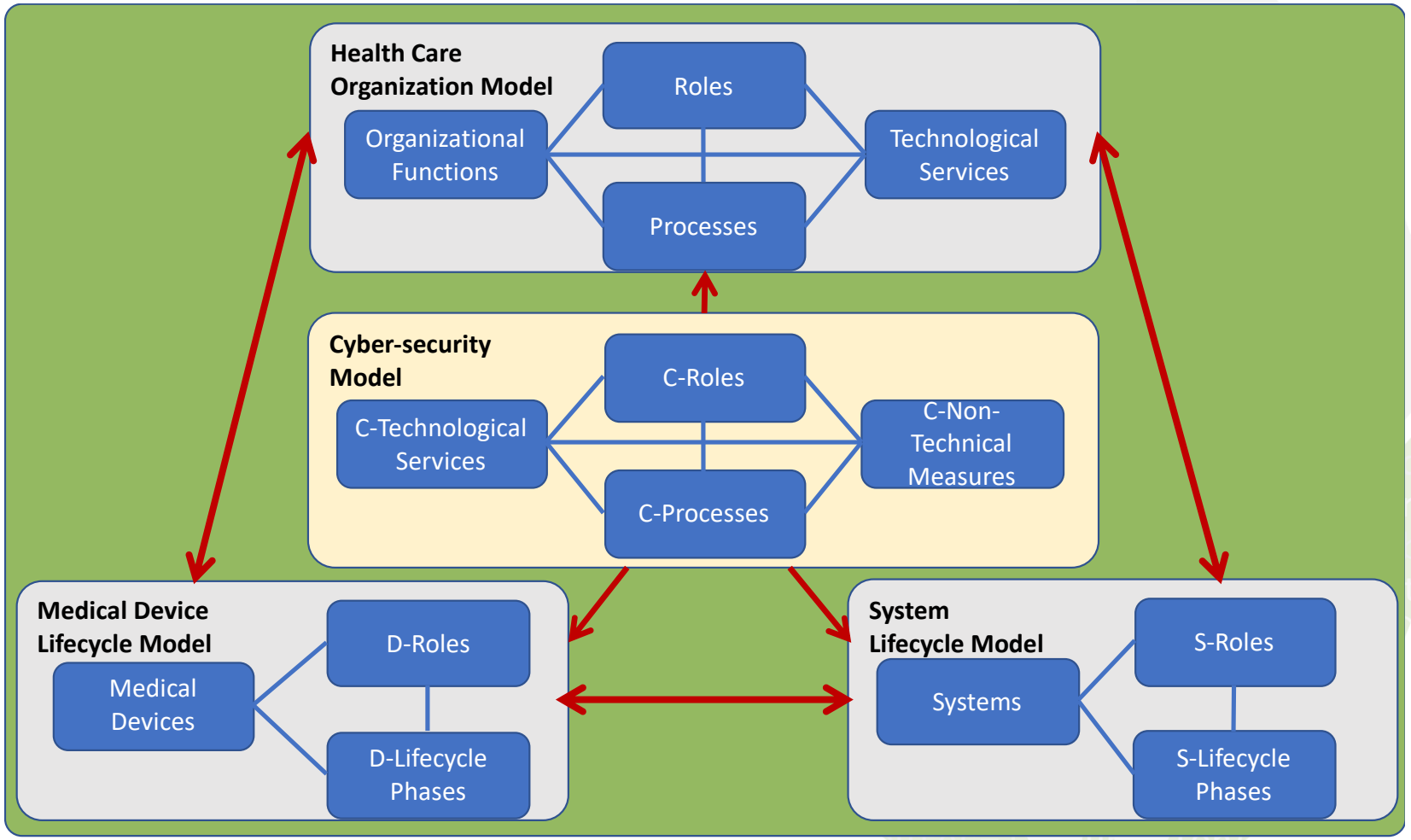
3. Entities and taxonomies: what the model is? (1/4)

- We identified
  - four inter-related models:
    - A Healthcare Organization
    - A Medical Device Lifecycle
    - An Information System Lifecycle
    - A Cybersecurity system (encompassing Technical and non-Technical measures)
  - the relationships among them



3. Entities and taxonomies: what the model is? (2/4)

- Models are **sociotechnical in nature** and are described in terms of **Entities**, and **Relationships**.
- For each Entity there is a **Taxonomy**.
- Some taxonomies are taken from **already existing sources** (e.g. ENISA, NIST, ILO)
- Some have been **built by the project** (e.g. HCOM organizational functions and technological services; the catalogue of cybersecurity technologies).



3. Entities and taxonomies: what the model is? (3/4)

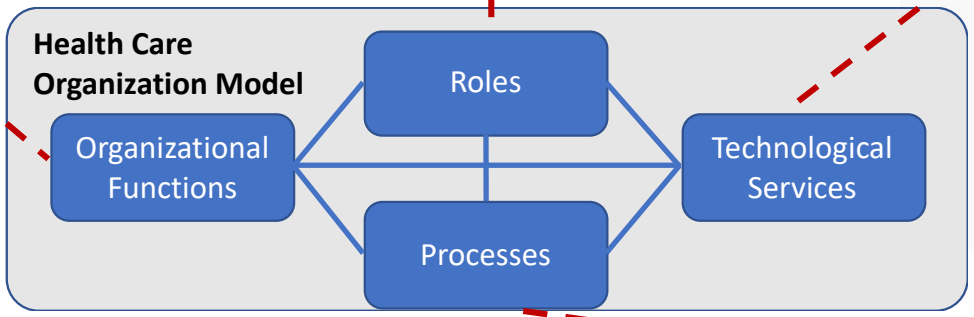
HCOM
1st and 2nd level taxonomies

1. Territorial health functions
1.1. Prevention
1.2. Diagnosis
1.3. Assistance
1.4. Emergency
1.5. Legal and tax medicine
1.6. Drug pharmaceutics
1.10. Other territorial functions
3. Support functions
3.1.Operation Support functions
3.2. Administrative support functions
3.3.Technical support functions
3.4. Communication functions
3.5. Education and lifelong Learning
3.6. Quality assurance
3.7. Other support functions

2. Hospital health functions
2.1. Emergency
2.2. Anaesthesia
2.3. Intensive therapy
2.4. Surgery
2.5. Medicine
2.6. Rehabilitation
2.7. Diagnostic services
2.8. Histopathology
2.9. Outpatient Clinics
2.10 Drug pharmaceutics
2.11.Blood banks
2.12.Ethical Committee
2.13.Other hospital functions

Managers
Health services Managers
Health Roles
Generalist Medical Practitioners
Specialist Medical Practitioners
Nurses
Paramedical practitioners
Medical and Pharmaceutical Technicians
Ambulance Workers
Personal care workers in Health Services
Other Heath roles
Non-health Roles
Technical roles
Administrative back-office roles
Administrative front-office roles
Medical Secretaries
Information and Communications Technology roles
Other non-health roles
External roles
Patients
Suppliers

Type	Area
Applications	Clinical services
	Internet accessible services
	Corporate services
	Facility management services
	Data services
	Infrastructure services
Devices	Networked medical devices
	Identification devices
	Access devices
	Infrastructure

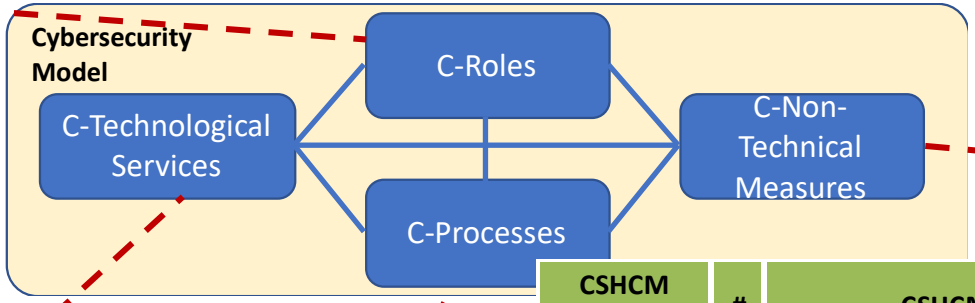


Health Processes
Hospital workflows
Inter-hospital medical consultations
Territorial workflows
Cross-border exchange of patient related data
Emergency pre-hospital workflows
Administrative/Technical processes
Patient billing
Centralized processes
In-Hospital processes

3. Entities and taxonomies: what the model is? (4/4)

CSHCM
1st level taxonomies

Role Category
Security Provision
Operate and Maintain
Oversee and Govern
Protect and Defend
Analyze
Collect and Operate
Investigate



#	Cyber-Technology Service	#	Cyber-Technology Service (continued)
1	Anti-Virus System (AV)	22	Image recovery System
2	Application tampering detection System	23	Incident management System
3	Audit trail System	24	Interactive Application Security Testing System (IAST)
4	Authentication services	25	Intrusion Detection System (IDS)
5	Configuration and systems management	26	Intrusion Prevention System (IPS)
6	Data encryption System	27	Netflow System
7	Data loss prevention System (DLP)	28	Physical Access behavioural analytics System
8	Data monitoring System	29	Physical access control system
9	Data recovery System (backup/restore)	30	Risk Assessment System (RAS)
10	Device authentication System	31	Runtime Application Self-Protection Service (RASP)
11	Device blacklisting System	32	Secure Remote Access System (SRA)
12	Device identification System	33	Security By Design Assessment System (SDAS)
13	Dynamic Application Security Testing System (DAST)	34	Static Application Security Testing System (SAST)
14	Endpoint control System	35	Structural vulnerability assessment System
15	Factory reset System	36	Threat analysis System
16	Firewall System (FW)	37	Threat detection System
17	Firmware reset System	38	User behavioural analytics System
18	Full Packet Capture System (PCAP)	39	User identification system
19	Host Intrusion Prevention System (HISP)	40	Video surveillance System
20	Identification and authentication System	41	Web application firewall System (WAF)
21	Identity and access management System (IAM)	42	Web fraud detection System

CSHCM Functions	#	CSHCM Processes
IDENTIFY	1	Asset Management
	2	Business Environment Assessment
	3	Governance
	4	Risk Assessment
	5	Risk Management Strategy
PROTECT	6	Access Control
	7	Awareness and Training
	8	Data Security
	9	Information Protection Processes and
	10	Maintenance
	11	Protective Technology
DETECT	12	Anomalies and Events
	13	Security Continuous Monitoring
	14	Detection Processes
RESPOND	15	Response Planning
	16	Communications
	17	Analysis
	18	Mitigation
	19	Improvements
RECOVER	20	Recovery Planning
	21	Improvements
	22	Communications

Security measure class
Governance
"Nudging" guidelines
Communication plans
Insurance schemes
Security Risk Management Plan
Standard Operating Procedures
Technical processes and/or procedures
Training and/or education packages

Panacea
People-centric cybersecurity in healthcare

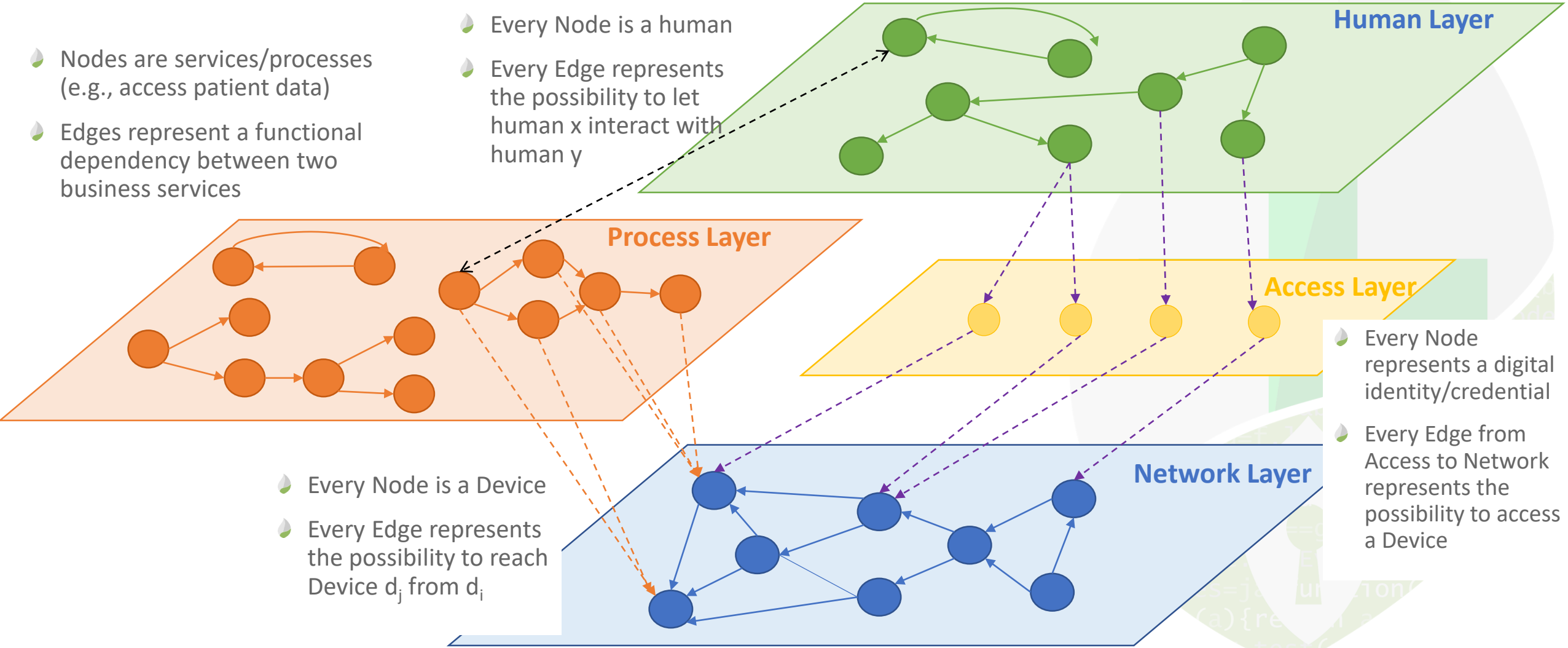
4. Examples of application: how the model can be used? → *Example 1: A framework for an automated holistic risk assessment (1/2)*

- **PANACEA will deliver a "Dynamic Risk Assessment & Mitigation tool"**, a software helping to perform risk assessment evaluation and to identify and prioritize mitigation measures, both technical and non-technical
- **The tool includes a representation of the reality to be assessed.** It is based on the socio-technical model and is **structured in four interconnected layers**
  - Network layer
  - Human layer
  - Access layer
  - Process layer
- Each layer is a network of nodes and edges, with attributes qualifying them, e.g., in terms of risk profile.
- The representation allows to simulate attack paths to identify vulnerable nodes and recommend mitigation measures

Panacea
People-centric cybersecurity in healthcare

4. Examples of application: how the model can be used?
→ *Example 1: A framework for an automated holistic risk assessment (2/2)*

- Nodes are services/processes (e.g., access patient data)
- Edges represent a functional dependency between two business services



- Every Node is a human
- Every Edge represents the possibility to let human x interact with human y

- Every Node is a Device
- Every Edge represents the possibility to reach Device d_j from d_i

- Every Node represents a digital identity/credential
- Every Edge from Access to Network represents the possibility to access a Device

4. Examples of application: how the model can be used?
→ *Example 2: Localization of criticality*

- The table below describes the **Cybersecurity criticality** in one of the three end-user organizations,
  - for the **Emergency workflow process**
  - which involves **five Roles** and **three Technology Services**.

- Criticality is estimated using **two scales**:
  - **Access score** (**1=very low. 5=very high**): how much the role can do (Read, Read + Write, Read + Authorize, Read + Write + Authorize)
  - **Impact score** (**A=very low impact, E=very high impact**): negative effect on the process in case of malicious intent

Technology services used in the **Emergency workflow**	**Roles**				
	Nursing Professionals	**Specialist Medical Practitioner**	**Paramedical Practitioner**	**Business and Administration Professional**	**Medical Imaging Technician**
Admission Transfer Discharge	**5E**	**1E**	**1E**	**5E**	
Radiology Picture Archiving Communication System	**2E**	**5E**			**5E**
Emergency Medical Record	**2D**	**4E**	**4E**	**1B**	

4. Examples of application: how the model can be used?
→ *Example 3: Cyber Defence Matrix*

The Matrix shows the **portfolio of Cybersecurity technological services** and its **coverage in a given organization** (e.g. a Hospital).

The concept of Cyber Defence Matrix has been created by the **OWASP** (Open Web Application Security) Project.

PANACEA project has contextualized the Assets to the Healthcare sector **and produced a catalogue of 42 Cybersecurity technological services**

Assets		Cybersecurity Processes (according to NIST framework)								
		Structural awareness and defence					Situational awareness and defence			
		Identify			Protect		Detect	Respond	Recover	
Asset categories	ENISA asset types									
Devices	Networked medical devices (e.g. IOMT)	30. Risk Assessment System (RAS)	5. Configuration and systems management System	12. Device identification System	21 Identity and access management System (IAM) 32 Secure Remote Access System (SRA)		14 Endpoint control System 37 Threat detection System	11 Device blacklisting System	17 Firmware reset System	
	Identification systems					19. Host Intrusion Prevention System (HISP)				
	Desktop and mobile devices					1. Anti Virus System (AV)			22 Image recovery System	
	Mobile Client devices (BYOD)								15 Factory reset Sytem	
	Remote care system assets					36 Threat analysis System 35 Structural vulnerability assessment System 10 Device authentication System			17 Firmware reset System	
Applications	Interconnected information systems			33. Security By Design Assessment System (SDAS)		34 Static Application Security Testing System(SAST) 13 Dynamic Application Security Testing System (DAST) 24 Interactive Application Security Testing System (IAST) 31 Runtime Application Self-Protection Service(RASP) 41 Web application firewall System (WAF)	2 Application tampering detection System 42 Web fraud detection System	23 Incident management System		
Networks	Networking equipment			27. Netflow System		16 Firewall (FW) 26 Intrusion Prevention System (IPS)	25 Intrusion Detection System (IDS)	18 Full Pack Capture System (PCAP)		
Data	Data					6 Data encryption System 7 Data loss prevention System (DLP)	8 Data monitoring System		9 Data recovery System (backup/restore)	
Users	Identification systems		20. Identification and authentication System			3 Audit trail System	38 User behavioral analytics System			
infrastructure	Building and facilities		39. User identication system		29. Physical access control system		28 Phyisical Access behaviorial analytics System 40 Video surveilance System			
Vendors (product suppliers) Service suppliers	Interconnected information systems		4. Authentication services							

Fully covered

Partially covered

Not coverd

Panacea
People-centric cybersecurity in healthcare

5. Contribution to security regulation: how the model can help?

In agreement with the aim of this Session 3 of ICEGOV Conference, I now answer following question: ***How this Socio-technical model can enhance*** *the ability of governments to ensure privacy, safety and* ***security of its citizens, through*** *traditional* ***regulatory frameworks****, such as GDPR or ISO 27000 and the sort,* ***or self-regulating approaches, so that e-health is an advantage and not a threat****?*

Regulatory frameworks

PANACEA model provides a taxonomy to standardize e-Health and Cybersecurity in domains such as

- **Healthcare-specific Controls for essential services** of cybersecurity frameworks (e.g. ISO 27001 and NIST framework), to apply EU Directive 2016/1148
- **IPS standards**, e.g. *prEN 17269 Health informatics - The Patient Summary for Unscheduled, Cross-border Care; FprCEN/TS 17288 Health informatics - The International Patient Summary: Guidance for European Implementation Technical Specification*
- **ISO/TC 215 Privacy and Security Standards**, e.g. *ISO/IS 27799 Information security management in health using ISO/IEC 27002*

Self-Regulatory approaches

PANACEA model provides a standard "map" to

- **Compare cybersecurity coverage** of technical and non-technical solutions offered to Healthcare (HC) organizations
- **Describe targets of cyberattacks** also in terms of social network in the HC context
- **Transfer lesson learned** in the cybersecurity domain for HC organizations
- **Speak non-technical language** with non-IT top managers and staff in HC organizations

Panacea
People-centric cybersecurity in healthcare

Appendix

- **Panacea Project:** www.panacearesearch.eu
- **Article:**
  - **Title: Public and private healthcare organisations: a socio-technical model for identifying cybersecurity aspects**
  - **Authors**
    - Kalliopi Anastasopoulou, 7th Healthcare Region of Crete Ministry of Health, Greece, kanastasopoulou@hc-crete.gr
    - Pasquale Mari, Fondazione Policlinico Universitario Agostino Gemelli, Italy, pasqualemari3@gmail.com
    - Aimilia Magkanaraki, 7th Healthcare Region of Crete Ministry of Health, Greece, amagkanaraki@hc-crete.gr
    - Emmanouil G. Spanakis, Foundation for Research and Technology – Hellas, Greece, spanakis@ics.forth.gr
    - Matteo Merialdo. RHEA GROUP, Belgium, m.merialdo@rheagroup.com
    - Vangelis Sakkalis, Foundation for Research and Technology – Hellas, Greece, sakkalis@ics.forth.gr
    - Sabina Magalini, Fondazione Policlinico Universitario Agostino Gemelli, Italy. sabina.magalini@unicatt.it
- **A detailed description of the models is provided in a document delivered by the Panacea Project:**
  - **Title:** D1.1 Models of health services and of medical device lifecycle for cybersecurity
  - **Link:** https://www.panacearesearch.eu/sites/default/files/PANACEA_D1.1_Models%20of%20health%20services%20and%20of%20medical%20device%20lifecycle%20for%20cybersecurity%20v1.0_0.pdf
- **Funding:** PANACEA Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 826293.

Panacea

People-centric cybersecurity in healthcare

Thank you!

Questions?!

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293