Connectivity, Internet Complexity, and Data Security in Public Health

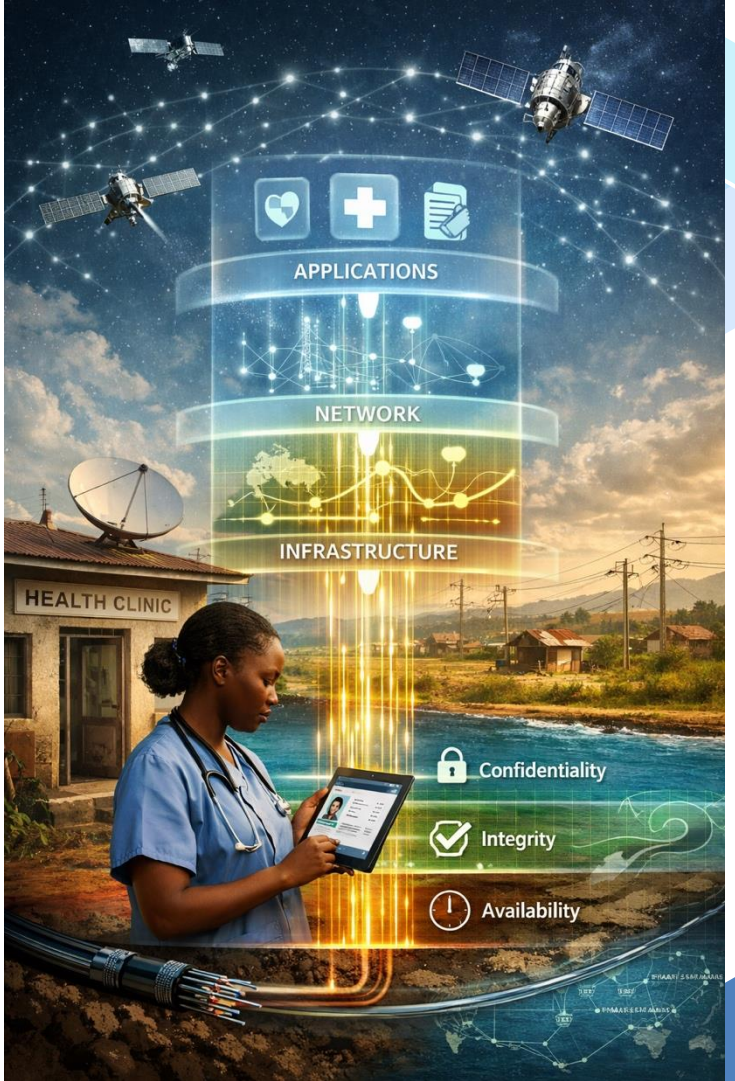
Prof. Gabriele Oliva

Complex Systems and Security, Director
University Campus Bio-Medico of Rome, Italy

g.oliva@unicampus.it
https://linktr.ee/gabrieleoliva

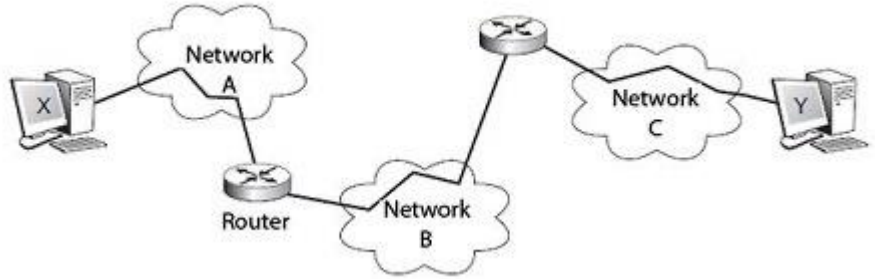
Why it matters?

- The Internet is a layered infrastructure enabling modern health, agricultural, and social services
- Network disruptions, attacks, or failures can directly affect public health and access to care
- Connectivity and security are essential to protect **availability**, **integrity**, and **confidentiality** of health data



A (very brief!) introduction to the Internet

What is the internet?



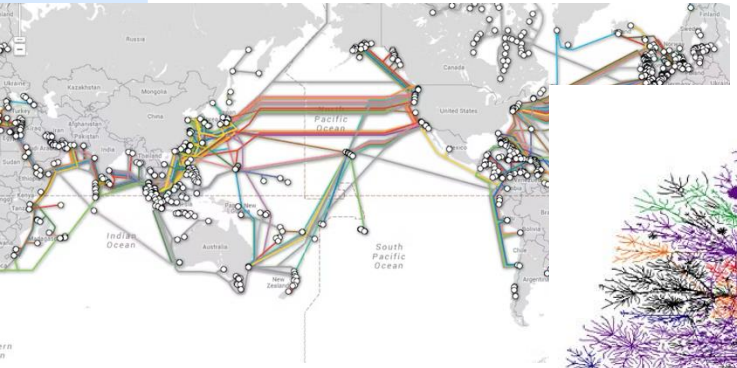
Computer network that interconnects computing devices

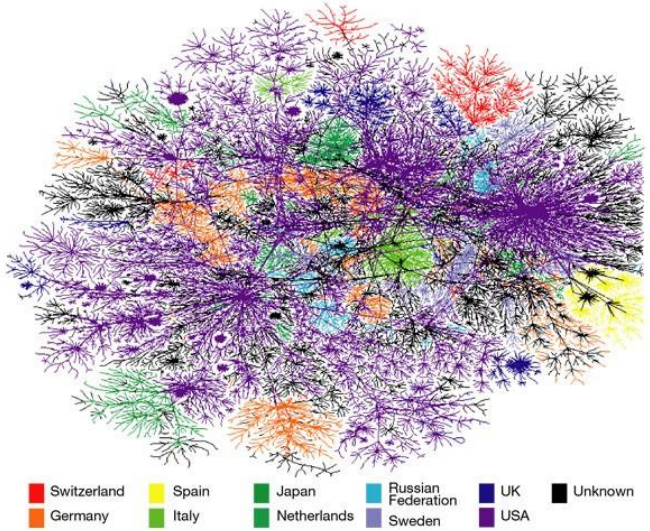
- Host or end systems (ES)
- Network links and intermediate systems (IS): switch and router

Infrastructure that provides services to the distributed applications

- Examples of applications: www, electronic email, social networks, VoIP …

Internet is a Complex Network

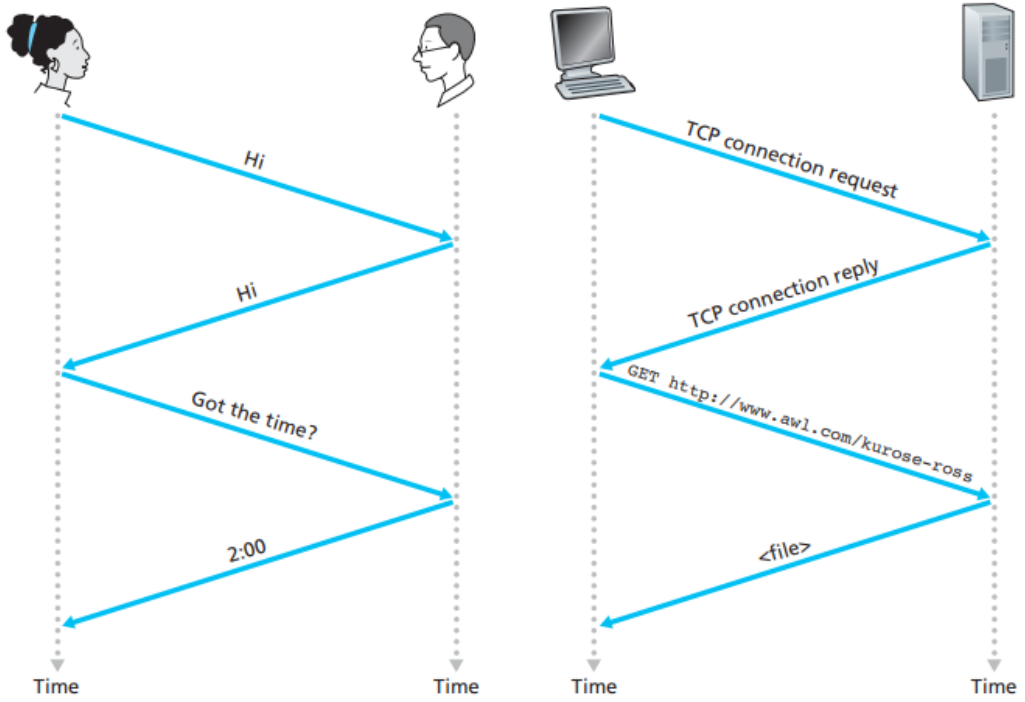




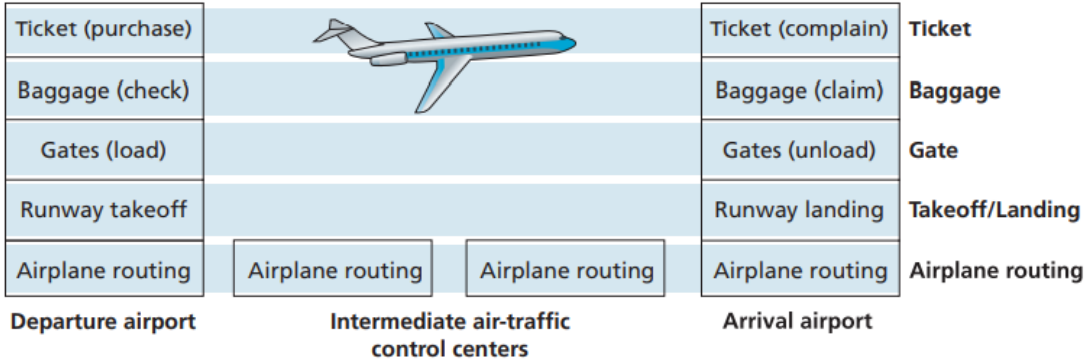
- Large number of entities
- High degree of mutual interaction
- It is more than the sum of its parts

Network Protocols

- Internet provides connectivity to end systems which send messages to each other in order to run applications.
- Such connections have to respect *specific rules* which are defined in the so-called **network protocols.**

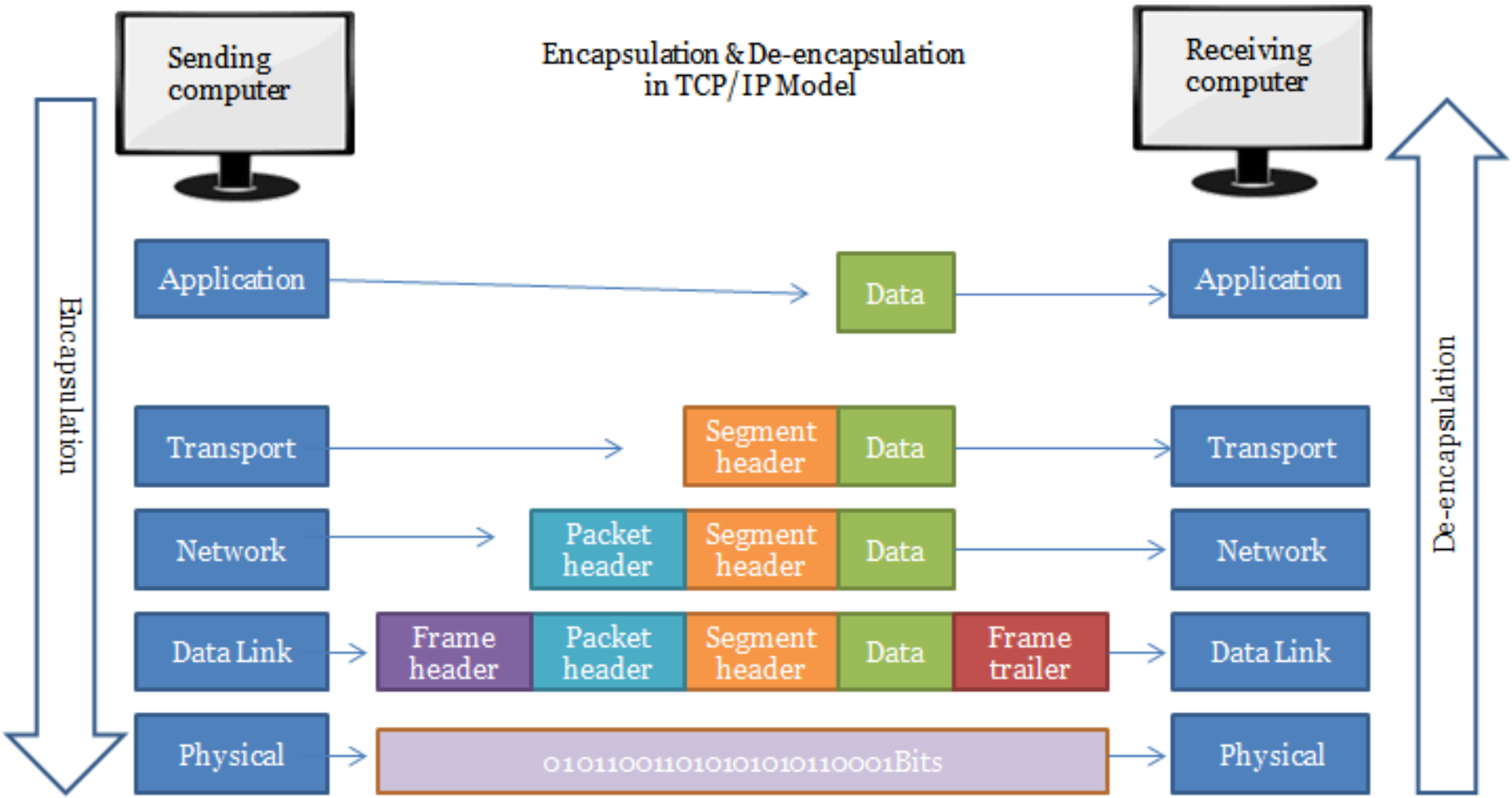


Internet is like taking a plane!

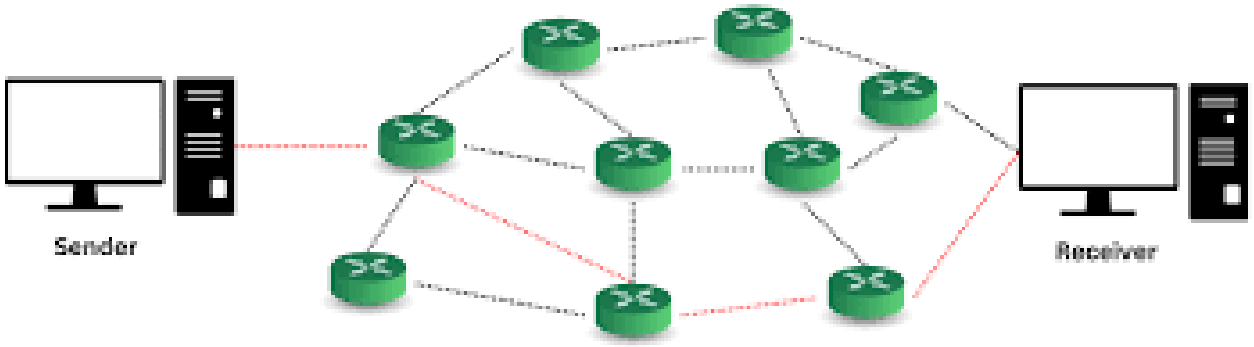


Horizontal structure in which each layer provides a specific service to the layer above using services offered by the layer directly below:

- Ticket layer: airline-counter-to-airline-counter transfer of a person
- Baggage layer: baggage-check-to-baggage-claim transfer of a person and bags is accomplished
- Gate layer: departure-gate-to-arrival-gate transfer of a person and bags is accomplished
- Takeoff/landing layer: runway-to-runway transfer of people and their bags is accomplished.


Sending computer
Encapsulation & De-encapsulation in TCP/IP Model
Receiving computer
Encapsulation
De-encapsulation
Application
Data
Application
Transport
Segment header
Data
Transport
Network
Packet header
Segment header
Data
Network
Data Link
Frame header
Packet header
Segment header
Data
Frame trailer
Data Link
Physical
0101100110101010101100001Bits
Physical

Routing

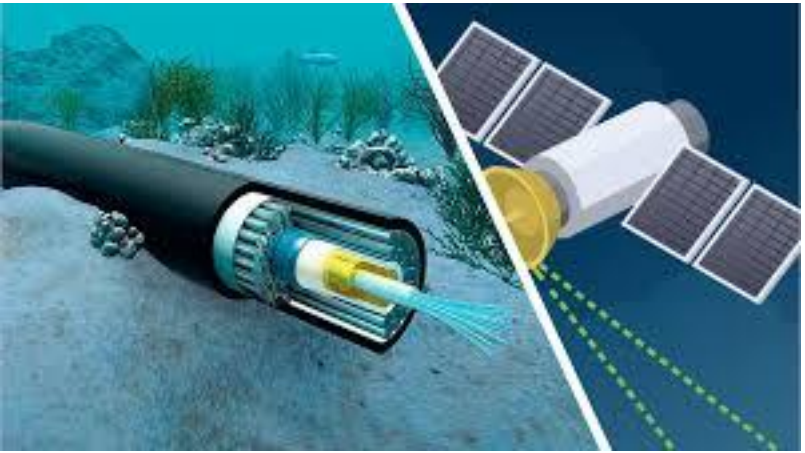


- The Internet is a network of interconnected networks, where data travels through multiple intermediate nodes
- Routing is the process of selecting a path that data packets follow from the source to the destination
- Routes can change dynamically in response to congestion, failures, or attacks, ensuring continued connectivity

TCP vs UDP: Two Ways to Deliver Data

- **TCP (reliable delivery):** data is delivered carefully, in order, and checked for errors
- **UDP (fast delivery):** data is sent quickly without guarantees of delivery or order
- **Trade-off:** TCP prioritizes reliability, UDP prioritizes speed and low delay

Where Does Internet Data Actually Travel?



- ~95% of global Internet traffic is carried by undersea fiber-optic cables
- Terrestrial fiber networks connect cities and regions within continents
- Satellites carry only a small fraction of traffic, but are **crucial for remote and underserved areas**

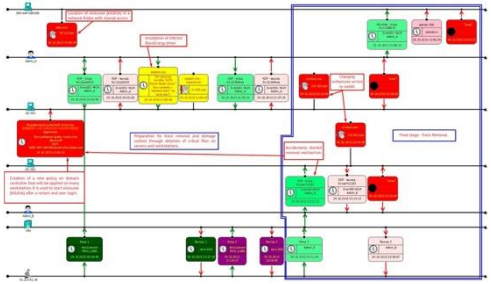
Data Security in Public Health

What Is Cybersecurity?

- Security of information systems and networks
- Protection against attacks, accidents, and failures
- Preservation of operations and assets

A few worrying examples

RANSMOMWARE
Universal Health Services (2020)
400+ facilities affected
~$42 mln loss
3 weeks to recover

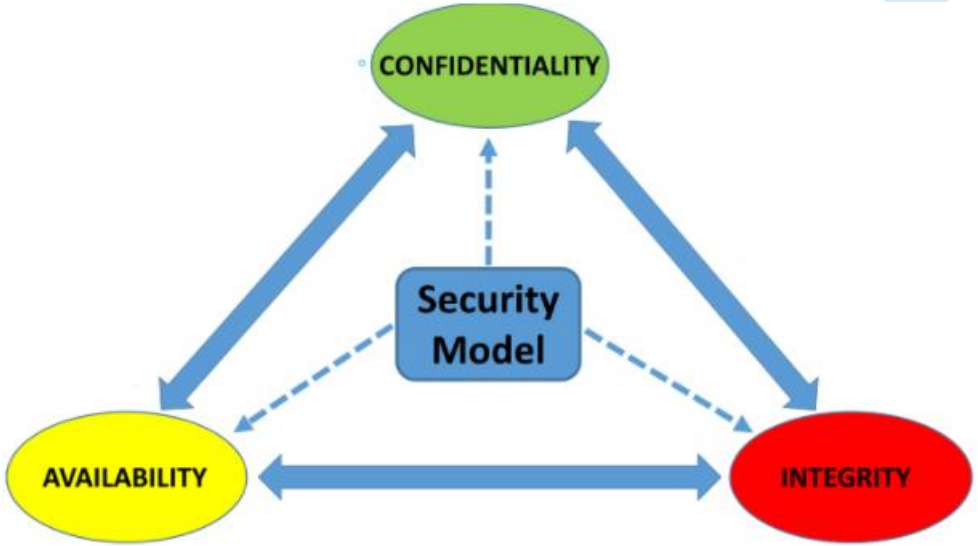


CYBER-PHYSICAL
Blackenergy 3 malware (2015)
Blackout for 230k consumers in Ukraine
Entry point: cyber
Damage to phisycal process!

DATA BREACH
Vastaamo Psychotherapy Center (2020)
Sensitive mental health records stolen
Company AND clients blackmailed
680k€ fine from Finnish GDPR Authority

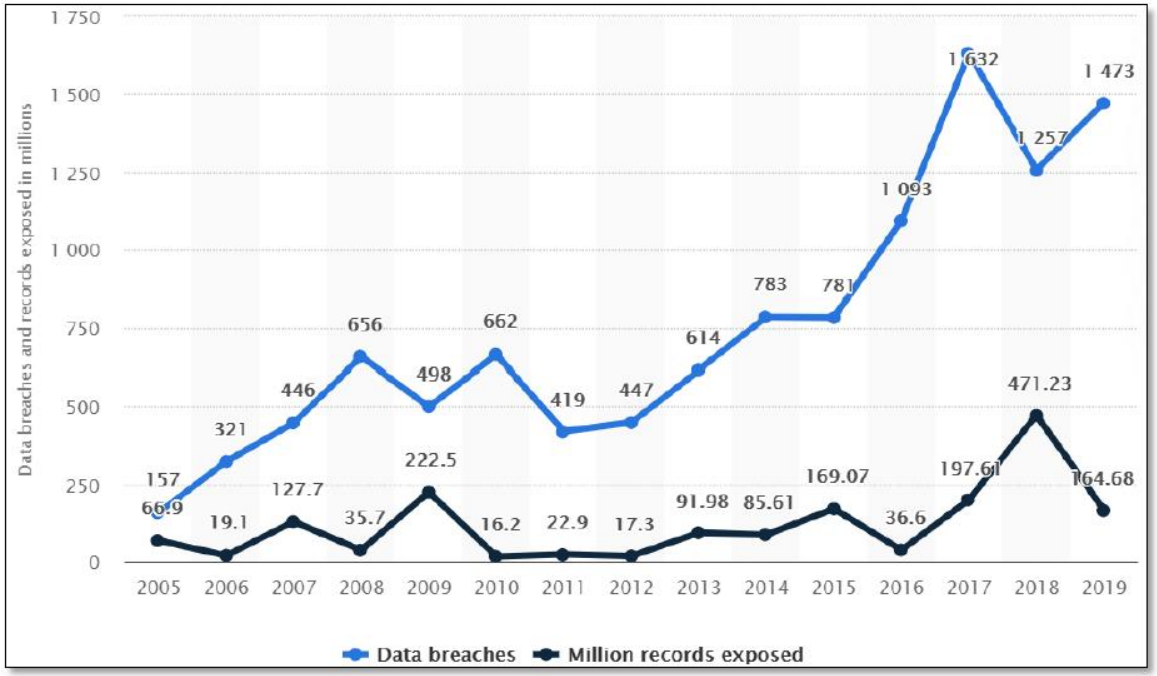
The Three Pillars of Cybersecurity

- **Confidentiality:** unauthorized access is prevented
- **Integrity:** data cannot be modified
- **Availability:** data must be available



"There are two types of companies: those that have been hacked, and those who don't know they have been hacked"

- John Chambers, ex CEO, Cisco



Cybersecurity and Healthcare

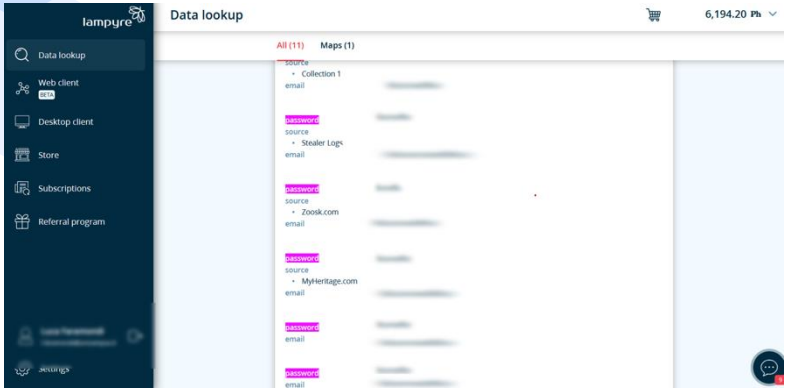
Two main factors

HUMAN FACTOR
Leveraging on human behavior with the aim to induce individuals to do specific actions (e.g., click on a link)

TECHNICAL FACTOR
Leveraging on intrinsic vulnerabilities and lack of protection


Utente di Accesso al pc
user: vaccinazioni.Iseo
PW: Vaccino2021
tg3
tg3

Passwords are easy to guess!



Leak	Number of Credentials	Estimated %
LinkedIn	105+	~25%
Zoosk	22+	~5%
Facebook	15+	~4%
Badoo	8+	~2%

- **27% of passwords consist only of letters**: vulnerable to brute-force attacks
- **Only 18% include special characters**
- **About 30% are common or easily guessable** (e.g., *Pizza,123456, birth date*)
- **Many passwords are reused**
- **Numerous passwords follow simple patterns**, such as *name + year* or *word + number* (e.g., *Francesca71, Andrea1054*)

Why Healthcare is a target?

High pressure

Precious data

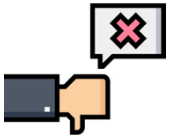
Legacy infrastructures

Digitalization

Growth of Telemedicine

In Italy, spending on digital healthcare, including telemedicine, grew by 12% in 2024, reaching €2.47 billion compared to 2023.
52% of general practitioners conducted teleconsultations, and 46% used telemonitoring services.

Remote access
Continuous monitoring
Sustainability



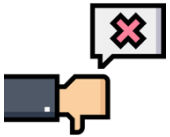
Enlarged attack surface
Healthcare data can be exposed

https://www.osservatori.net/comunicato/sanita-digitale/sanita-digitale-italia-investimenti/

Cloud Adoption

In 2024, the global healthcare cloud computing market reached a value of approximately USD 54.28 billion, with projections to grow to USD 197.45 billion by 2032.

Scalable monitoring
Better access to data
More efficiency



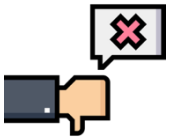
Increased unauthorized access risks
Healthcare data can be exposed

https://www.healthcareittoday.com/2024/01/09/healthcare-interoperability-data-and-cloud-2024-health-it-predictions/

Rise of AI

The global healthcare AI market is expected to reach USD 20.9 billion by 2025, with projected growth to nearly USD 150 billion by 2029.
Applications such as predictive analytics and robotic surgery are becoming increasingly widespread, improving clinical outcomes and operational efficiency.

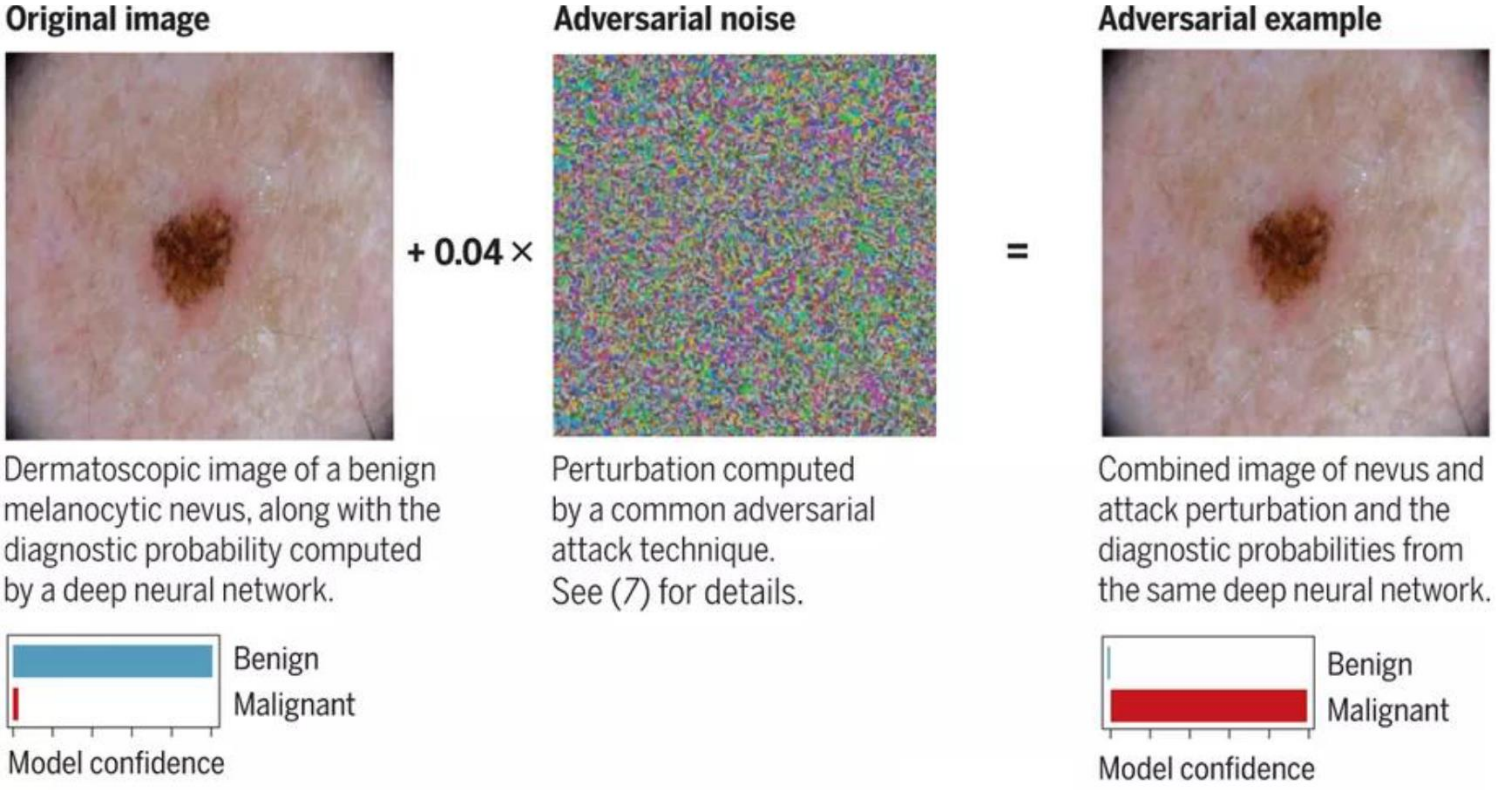
Better diagnosis
Personalized treatmenet
Activity optimization



Adversarial machine learning
Ethical issues (privacy/bias/explainability/access)

https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-healthcare-market-54679303.html

Adversarial Machine Learning



Source: [10.48550/arXiv.2012.06332](https://doi.org/10.48550/arXiv.2012.06332)

Attacker Categories

Cybercrime:
Cybercrime is an offense in which the conduct or the target of the crime is related to an information or telecommunications system, either by using such a system or by attacking it.

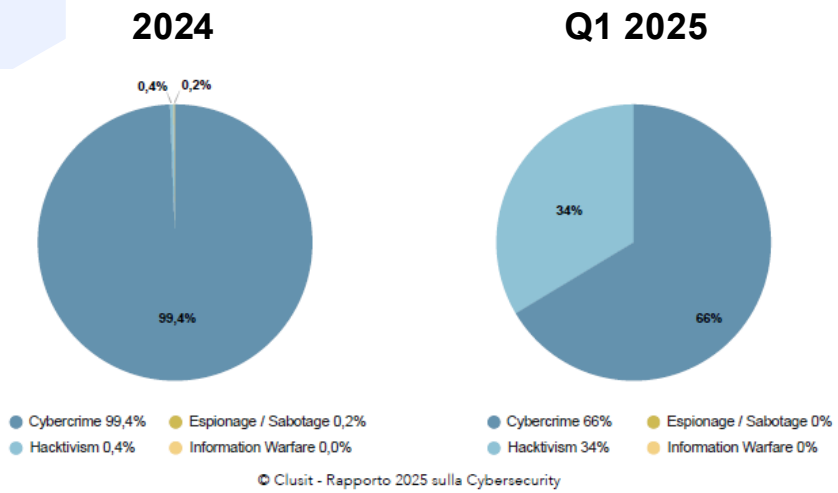
Cyber Warfare:
Cyber warfare refers to the set of activities involved in the preparation and execution of defensive and offensive operations in cyberspace.
.

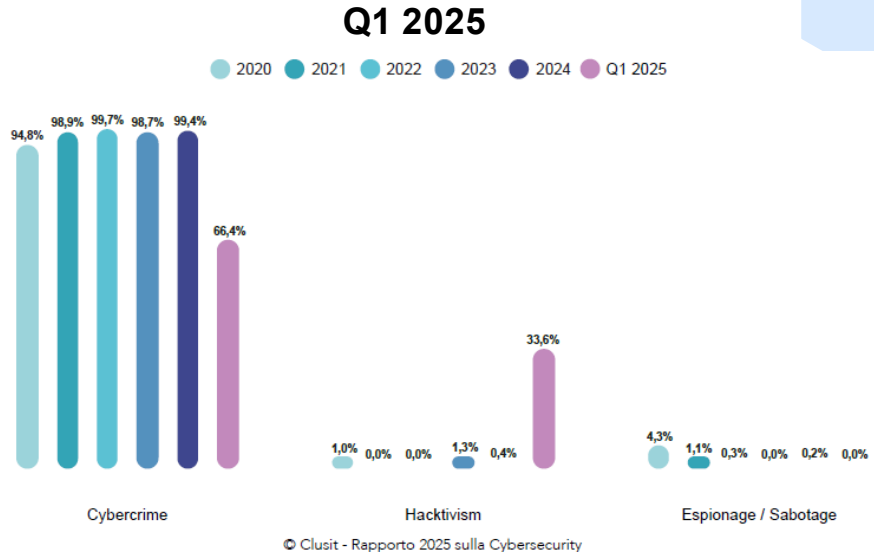
Hacktivism:
The term was coined to describe early forms of online civil disobedience. It refers to digital actions carried out worldwide to protest against civil rights abuses, corrupt governments, or practices such as the death penalty.

Cyber Espionage:
Cyber espionage is a rapidly growing practice used to steal know-how and confidential information from public and private organizations.

.

Helthcare and Attacker Categories





2025 has seen a rise of Hacktivism!

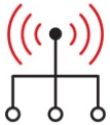
Threat Categories

Phishing / social engineering: deceives staff into revealing credentials or installing malware

Third-party risks: breaches occurring through contractors or service providers

Insider threats: employees or contractors acting maliciously or making costly mistakes

DoS / DDoS attacks: overload systems or networks with abnormal traffic, making critical services unavailable and disrupting operations



IoMT attacks: exploit vulnerabilities in Internet-connected medical devices

Malwares Categories

Worms: designed to replicate themselves by spreading to other computers via the Internet or removable storage; this leads to disk space consumption and system slowdowns

Trojans: create a backdoor that allows malicious programs or users to access the system and steal sensitive data

Spyware: often bundled with freeware, these programs monitor browsing activity and other personal data and transmit them to a remote user

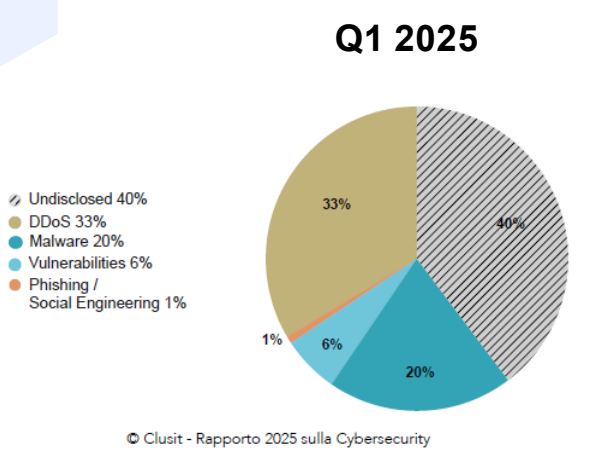
Malwares Categories

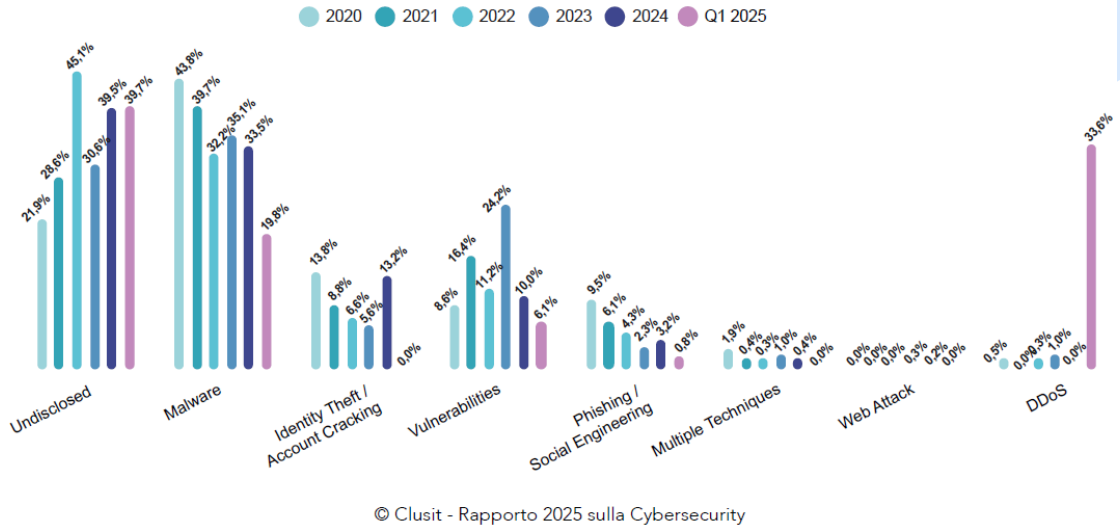
Ransomware: a type of malware that encrypts data on infected systems, making it inaccessible, and demands a ransom in exchange for the decryption key

Impact on healthcare: blocks access to electronic health records and diagnostic systems

Additional risk: stolen patient health data may be leaked or published online

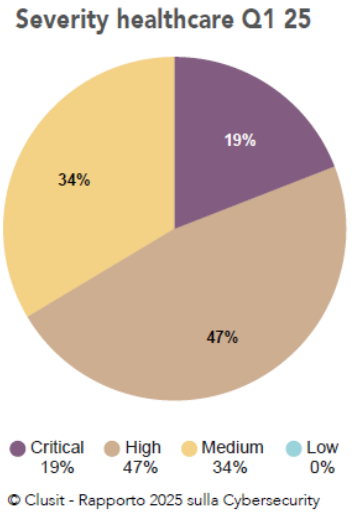
Healthcare: Threat Categories

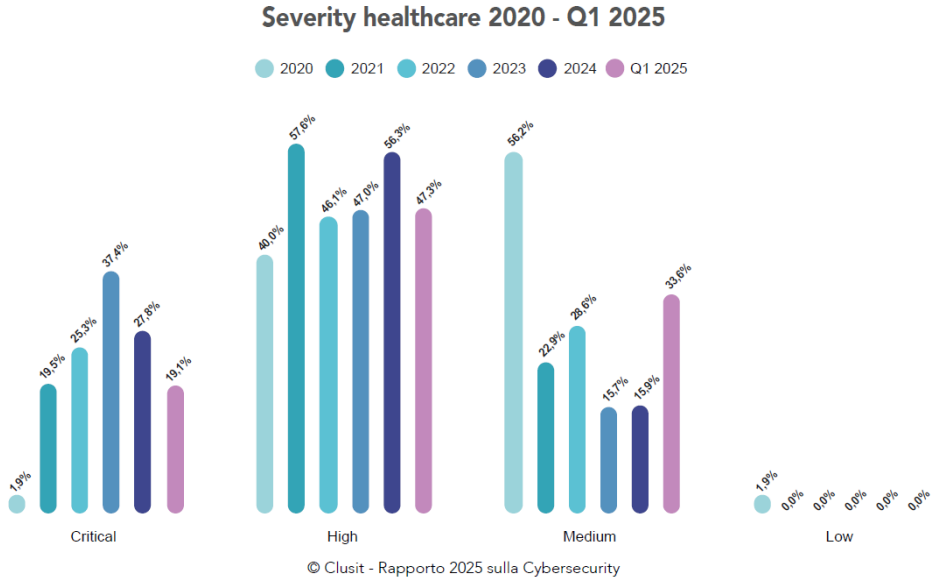




In the first half of 2025, there was a significant increase in the number of DDoS attacks, mainly driven by hacktivist activities.

Healthcare: Threat Severity





In 2025, the overall severity of cyber attacks decreased, consistent with a shift toward DDoS incidents, which typically have a lower impact than cybercrime attacks.

How to react?

Intrusion Detection System (IDS)
Device or software application that monitors network traffic for malicious activity or policy violations and sends alert or detection.

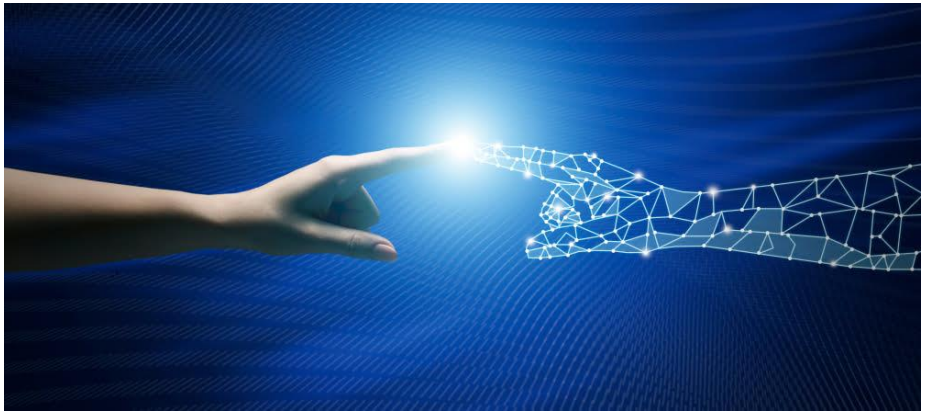
Intrusion Prevention System (IPS)
Device that inspects traffic, detects it, classifies and then proactively stops malicious traffic.

Firewall
Network security device that filters incoming and outcoming network traffic based on predefined rules

Is it enough?!?

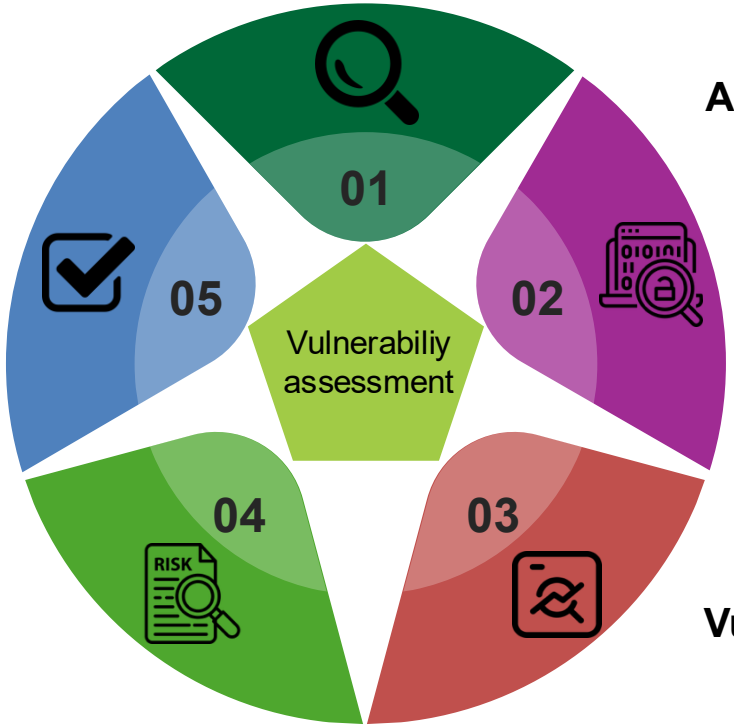
We need to go beyond a mere technological approach!

Organizational Level



Human Level

Organizational Level



Asset discovery

Vulnerability identification

Vulnerability analysis

Risk assessment

Vulnerability remediation

Human Level

- A system is only as strong as its weakest link
- People are often the weakest link, especially under pressure or lack of awareness
- Security culture and training are essential to strengthen the entire system

What can be done?

- Regular awareness training (phishing, passwords, safe behavior)
- Clear procedures for reporting suspicious emails or incidents
- Simple rules, reinforced over time (updates, reminders, drills)
- Shared responsibility, not blame, when mistakes happen

g.oliva@unicampus.it