POLITECNICO DI TORINO

Fundamentals of Information Systems Security

Student:

Gianmarco Michelini

Academic Year 2024/2025

Indice

Elenco delle figure

Elenco delle tabelle

The more complex a system is, the more difficult its correctness verification will be.[1]

[1] All notes are derived from oral presentations and written papers.

Capitolo 1

Introduction to Cybersecurity

1.1 Risk Estimation and Management

[1] Complexity is an enemy of security, in fact, consequence of a succsseful attack are as follows:

- Financial loss
- Recovery cost
- Productivity loss
- Business disruption
- Reputation damage

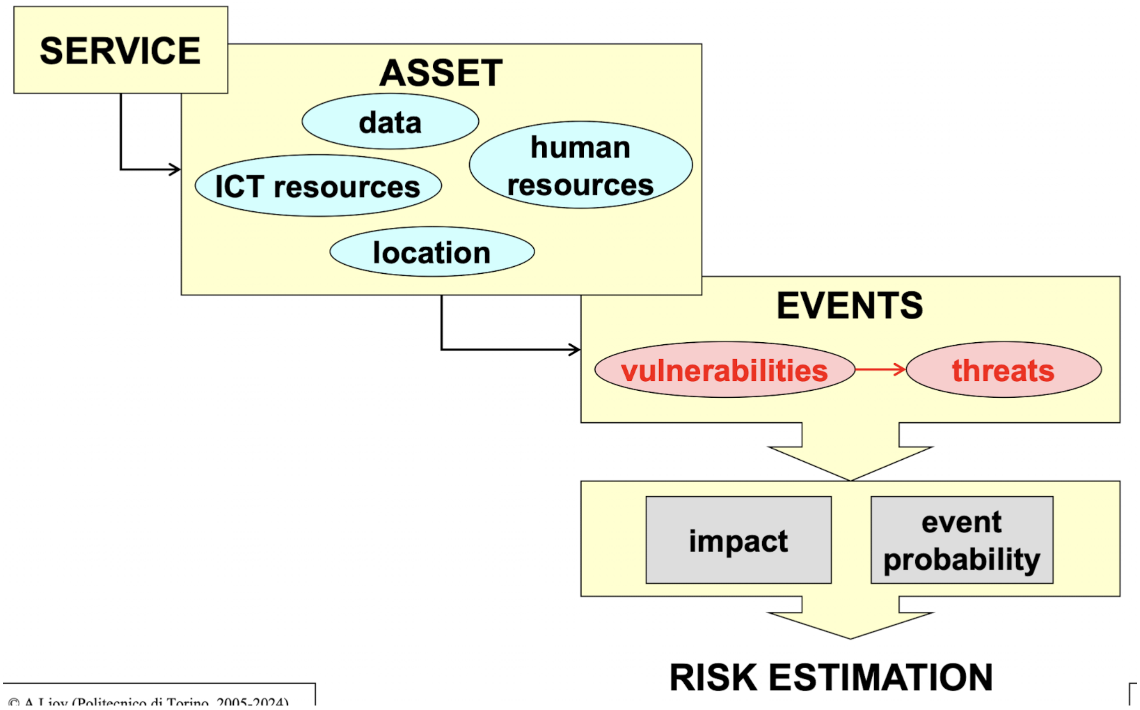

Figura 1.1: The risk estimation process

Terminolgy:

- Asset: the set of goods, data and people needed for an IT service.
- Vulnerability: intrinsic weakness of an asset.
- Threat: possible deliberate action/accidental event that can produce the loss of a security property by exploiting a vulnerability.
- Attack: threat occurrence (deliberate action)
- (Negative) event: threat occurrence (accidental event)

Managing threats requires us to **prioritize risks**, considering not only the impact but also the available **time and budget**[1].

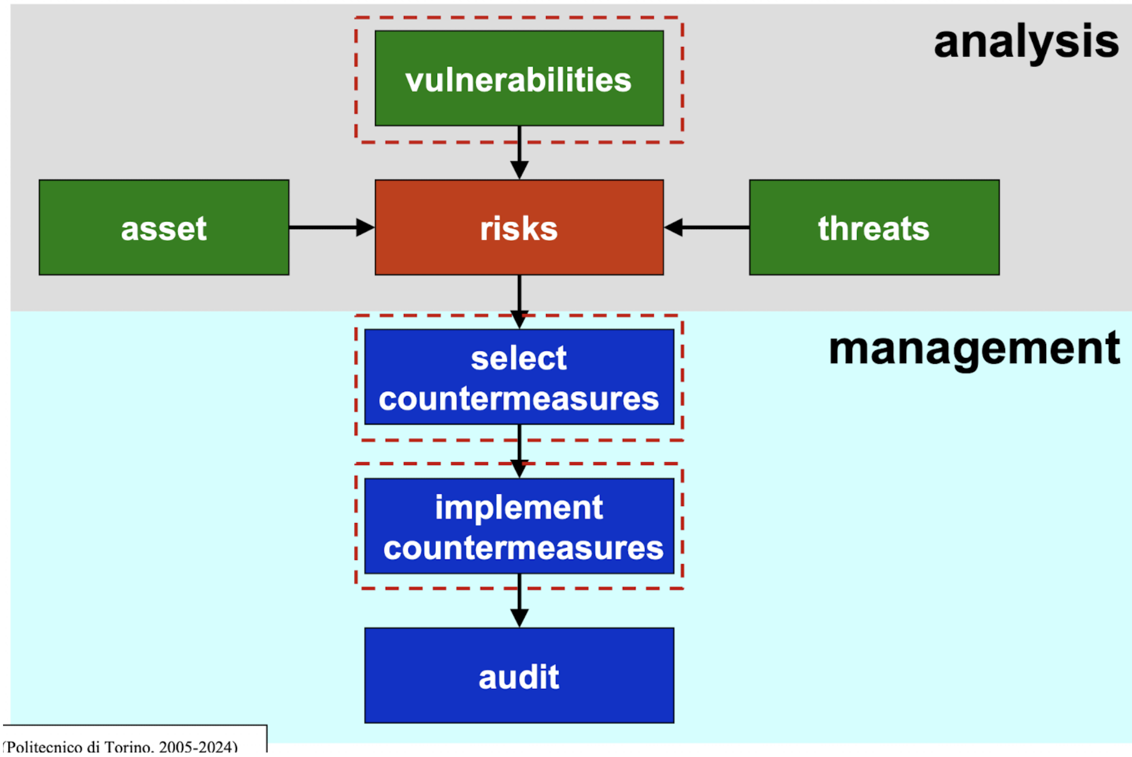

Figura 1.2: Analysis and management of security

[1] A risk assessment matrix (or risk heat map) can be useful in this process

Capitolo 2

Cryptography

The information is provided in the slides [2].

Capitolo 3

Cybersecurity and Society

[3] - 20hrs module
Objectives of this module:

- Gain an introduction to sociology, its terminology, relevant theories, and risk sociology applicable to Cybersecurity.
- Understand the fundamental concepts of cybercrime and cybersecurity from a sociotechnical perspective.
- Explore the social, cultural, and organizational dimensions of cybercrime.
- Develop skills in identifying, analyzing, and mitagating cyber threats with a focus on social impacts.

It is relevant to learn more about cybersecurity in the societal sphere because "Humans are authors within Society".

3.1 Sociology, Really?

3.1.1 What is Sociology?

Some definitions to sociology.

> The science of social phenomena subject to natural and invariable laws, with goal of discovering these laws.
>
> – Auguste Comte

This assertion is overly positivist, as it overlooks potential negative impacts and seems somewhat naive. There are no general laws that describe social phenomena. In the modern view, in fact, no laws exist a priori. Some key parameters in Sociology: historical context and humankind.

> Sociology is the study of human social life, groups and societies.

– Sir Anthony Giddens

A post-positivist claim, states that there are no strong natural laws. This perspective is much more dynamic and mechanistic.

> Sociology is the scientific study of society, including the intricate patterns of **social behavior, relationships and human interactions**. It is a systematic examination of social institutions, **cultural norm** and social change, **using empirical research and critical analysis**. This discipline aims to understand the underlying mechanisms that govern <u>social order</u>, dynamics and transformation, ranging from **individual interactions at the micro level** to **social structures at the macro level**. Those in sociology investigate various aspects of human life, including social stratification, movement and change, with an emphasis on **how collective and individual behavior shapes and is shaped** by the broader social context.

– ChatGpt

3.1.2 Ethics and Epistemic

The main skill to develop is *evaluative reasoning*, also referred to as *avalutativity*. This involves the ability to **assess, critique, and reflect on knowledge claims, methodologies, and ethical implications** in various contexts. In both ethical theory and epistemology[1], individuals must be able to differentiate between valid and invalid arguments, recognize biases, and consider the consequences of knowledge application. The epistemic status of data is uncertain information (probabilistic way). Other skills concern:

- Extensivity: generalizing (macro), stimulus invariance, quantification
- Intensivity: understanding (micro), meaning to actions, qualification

– Max Weber [2]

3.1.3 Sociological Imagination

Sociology offers explanations of social phenomena that are less biased than common sens and empirically grounded. Is a creative gift of the intellect that must be trained. In order to do that, Mills uses the idea of adopting a “Martian” perspective to encourage readers or philosophers to take an objective or detached view of societal norms. Observe micro- and macro-social phenomena without awe and wonder even if they are distant from us and seemingly disconnected. Not taking everyday life and what is *normal* (i.e. institutionalized) and (apparently) related to us for granted.

– Charles W. Mills [3]

[1] Epistemology is the branch of philosophy that studies the nature, scope, and limits of knowledge.

[2] European sociologist. 1864-1920.

[3] American sociologist. 1916-1962.

> You must train yourself to acquire new skills (a new normality) and avoid focusing on what feels strange. Instead, try to learn more from the other perspective.

3.1.4 Basic Sociological Vocabulary

Keywords that unlock access to the cybercrime field from a sociological perspective.

- Norms, i.e. rules and expectations that guide the behavior of members within a society. Cultures and languages also evolve according to certain norms. We can distinguish between two different types of norms:
  - Silent norms: we adhere to them without the need to read them or be exposed to any formal institution. Most of these are acquired through imitation from families, social groups, etc.
  - Codified norms: rules that are formally written down and established by an authoritative body, such as laws, regulations, or official guidelines.
- Values: collective ideas about what is good, desirable, and proper.

  > A lighthouse in the darkness.

- Role: set of norms, behaviors and expectations that are associated with a particular social status or position within a society. Roles guide how individuals are supposed to act and interact with others in specific contexts.
- Social structure: the organized pattern of social relationships and social institutions that together constitute society.
- Culture: shared beliefs, values and practices.

Insight on Role:
It is possible to draw a dependency chain between:

$$\boxed{\textit{Network}} \rightarrow \boxed{\textit{Position}} \rightarrow \boxed{\textit{Role}}$$

In this chain, the Network represents the broader system of connections or relationships, which influences an individual's Position within the structure. This position, in turn, determines the Role that the individual is expected to perform within the network. The interaction between these three elements highlights how individual behaviors and responsibilities are shaped by both social connections and hierarchical placement.

> You can do it without an actor, but it is the role that carries all the expectations.

3.1.5 Cybersecurity and Society

The figure 3.1 depicts the “Iceberg Model” of Sociology, which illustrates the visible and invisible elements that influence social dynamics. Similarly, in cybersecurity, there are layers of visible actions and hidden processes that determine the behavior and vulnerabilities of systems. There are relationships between perceptions (what I see) and behaviors (how you act). Social interactions are also crucial, in fact, as they form the vast ocean of sociological imagination. Sociological imagination pertains to primary and secondary socialization. Primary socialization refers to the process by which individuals, typically in early childhood, learn and internalize the norms, values, beliefs, and behaviors of their culture or society, while secondary socialization develops when individuals step outside their comfort zone, though begins even before we are born.

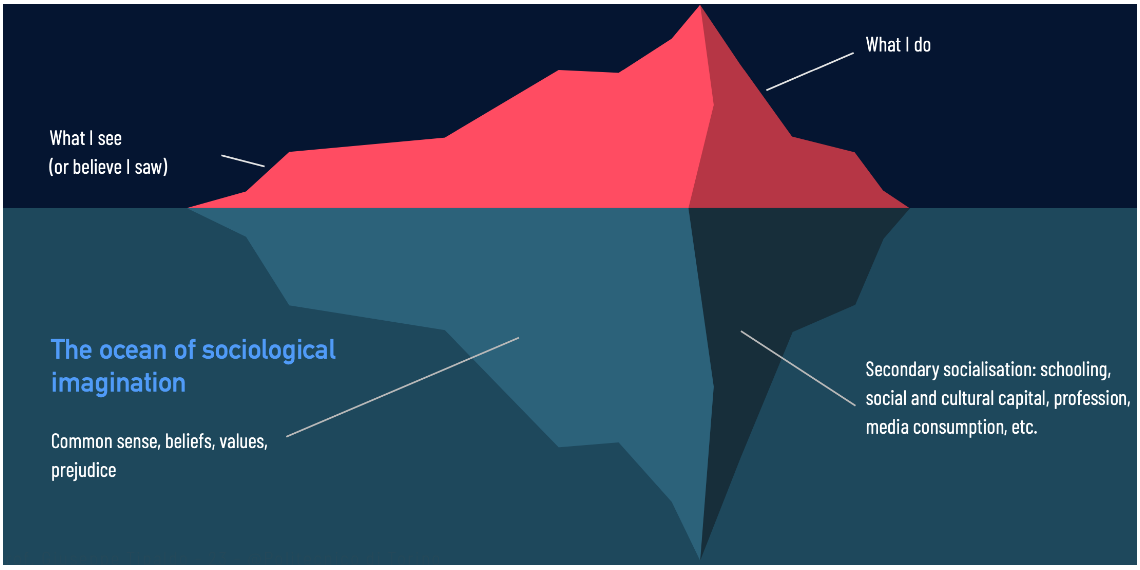

Figura 3.1: The Iceberg Relation

3.2 Nomina Nuda Tenemus

“Nomina Nuda Tenemus” [4] translates to “we hold only bare names.” It suggests that without deeper understanding or context, words are merely empty labels. Without a clear name or definition—in this case, within the realm of cybersecurity—it becomes impossible to identify what needs protection. Moreover, this lack of clarity prevents the formulation of an effective legal framework.

3.2.1 Overview of Cybersecurity

The diagram 3.2 provides an overview of cybersecurity from a sociological perspective, broken down into two main sections: Definitions and Terminologies and Concepts. Here’s an explanation of each component:

- Definitions: This section focuses on defining key concepts like cybercrime and cybersecurity. It includes an analysis of the historical development of these fields and discusses current trends in cyber threats and protection strategies.

- Terminologies and Concepts: This section introduces foundational terms necessary for understanding cybersecurity, such as malware, phishing, and ransomware. It highlights the necessity of a shared vocabulary for precisely identifying and describing cyber threats, offering structured classifications and comprehensive definitions of cybercrime.

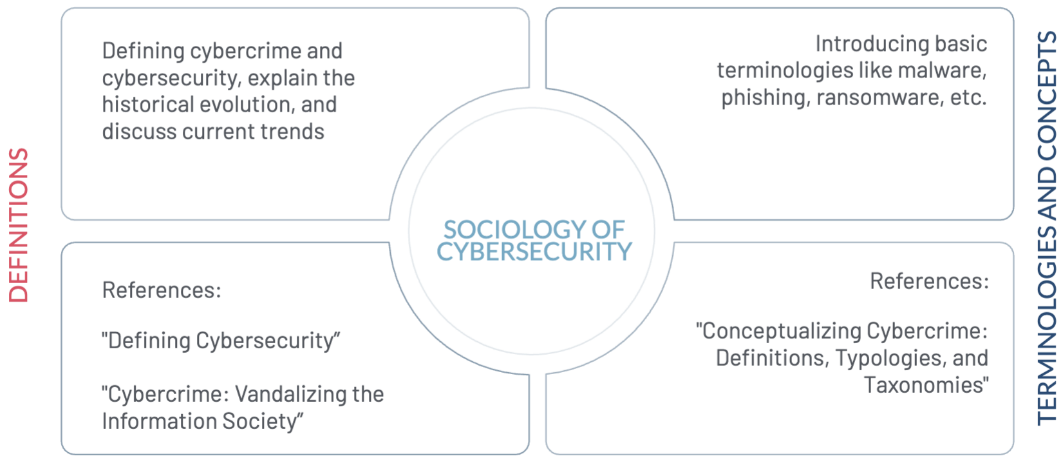

Figura 3.2: Overview of Cybersecurity from a sociological perspective

[4]This phrase is notably referenced in Umberto Eco’s The Name of the Rose, where it highlights the importance of meaning beyond mere names.

3.2.2 Definitions of Cybercrime

Vocabulary

Figure 3.3 illustrates how the vocabulary used to describe similar phenomena has changed over time. Nowadays, cybercrime attacks are a top priority on the agenda of many countries.

	Number of Occurrences	
Terminology	**1995–2000**	**2001–2018**
Cybercrime	1476	28,100
Cyber crime		17,900
Computer crime	2760	19,000
E crime	585	15,800
Internet crime	236	7500
Digital crime	50	3830
Online crime	49	3120
Virtual crime	43	1100
Techno-crime	19	55
Netcrime	17	216

Note. Copyright 2020 by Routledge, from McGuire, M. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In *The Human Factor of Cybercrime*; Leukfeldt, R., Holt, T.J., Eds.; Routledge: New York, NY, USA, 2020; p. 8 (Table 1.1 and 1.2). Reproduced by permission of Taylor and Francis Group, LLC, a division of Informa plc.

Figura 3.3: Cybercrime terminology in the periods 1995-2000 and 2001-2018

Official Definitions

Figure 3.4 illustrates a shift from material to immaterial concerns regarding cybercrime attacks. In 1994, the United Nations issued the first official document, although cybercrimes already existed at that time, even if they were not yet formally named. Initially, cybercrimes were strictly related to the computer sphere. Over time, however, the definition of cybercrime expanded to encompass a broader range of activities, incorporating various new aspects. The main points of the new definitions are: data processed by computer systems or networks and information systems, either as a primary tool or as a primary target.

Year	Organization	Definition of Cybercrime
1994	The United Nations	"The United Nations manual [23] on the prevention and control of computer-related crime (1994) uses the terms, computer crime and computer-related crime interchangeably. This manual did not provide any definition" [18] (p. 116)
2000	The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders	1. "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them." 2. "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" [24] (p. 5)
2001	The Council of Europe Cybercrime Convention (also known as The Budapest Convention)	"action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" [25] (p. 2)
2007	The Commission of European Communities	"criminal acts committed using electronic communications networks and information systems or against such networks and systems" [26] (p. 2)
2013	Shanghai Cooperation Organization (SCO) Agreement	"the use of information resources and (or) the impact on them in the informational sphere for illegal purposes" (cited in Malby et al. [27] (p. 15))
2013	Cybersecurity Strategy of the European Union	"a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" [28] (p. 3)
2016	Commonwealth of Independent States Agreement	"a criminal act of which the target is computer information" (cited in Akhgar et al. [29] (p. 298))

Figura 3.4: Organization definitions of cybercrime

Dichotomous Definitions

In research and policymaking, a distinct dichotomy was established. A discrete categorical approach was applied to define cybercrimes, classifying them as either cyber-enabled or cyber-dependent. Cyber-enabled crimes are traditional offenses that predate the advent of technology but are now facilitated or made easier (i.e., enabled) by digital technology. Cyber-dependent crimes are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside the digital world.

Figura 3.5: Categorical approach to cybercrime

Many people also agree with another, non-discrete dichotomy from a continuum approach perspective. The continuum approach to cybercrimes views cybercrime not as a discrete category but as a spectrum, where offenses range from traditional crimes that are cyber-enabled to those that are fully cyber-dependent. Crimes of Type 1 are more technical in nature, while crimes of Type 2 involve more human interaction.

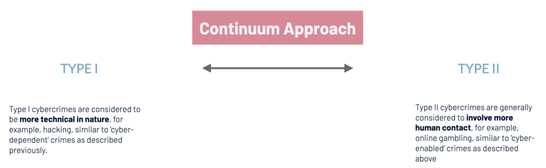

Figura 3.6: Continuum approach to cybercrime

Trichotomous Definitions

Industries have also attempted to classify clusters of crimes using trichotomous definitions within a categorical approach. First, we analyze the one made by David S. Wall in 2007. Wall introduced three sections:

- Crimes against the machine: Computer integrity crimes (e.g., hacking).
- Crimes in the machine: known as computer content crimes (e.g., online hate).
- Crimes using the machine: Computer-assisted crimes (e.g. piracy).

The EU Commission also released labels in 2013 addressing cybercrimes, which share many similarities with the ones presented above. In fact, cybercrimes were divided in three stages: offenses unique to computers and information systems, content-related offenses and traditional offenses.

3.2.3 Cybersecurity is

As stated by Fredrick Chang, former Director of Research at the National Security Agency in the United States:

> A science of cybersecurity offers many opportunities for advances based on a **multidisciplinary approach**[5], because, after all, cybersecurity is fundamentally about an **adversarial engagement**. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed.

Analyzing literature[6] "Cyber" is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality. The term "cyberspace" describes a vision of a three-dimensional space of pure information, moving between computer and computer clusters where people are generators and users of the information. Public Safety Canada[7] defines cyberspace as:

> the electronic world created by interconnected networks of information technology and the information on those networks. It is a global common where people are linked together to exchange ideas, services, and friendships.

Cyberspace is a dynamic mixed-reality[8] environment where hardware is significant, as it hosts real interactions.

[5] Crimes concern many fields of phenomena.
[6] Craigen et al.2014
[7] 2010
[8] The *phygital* reality. A funsion of physical and digital realities

In addition, cybersecurity must necessarily include and seek to understand:

- Who securitizes, identifying the actors and entities responsible for enforcing security.
- What issues, specifying the particular assets, systems, or information at risk.
- for Whom, clarifying the stakeholders, such as individuals, organizations, or governments, who benefit from the security measures
- Why, analyzing the motivations behind security implementations, whether they are economic, political, or social
- with What results, evaluating the effectiveness and outcomes of the security strategies applied
- under What conditions (structure), defining the structural or environmental factors influencing the security landscape

3.2.4 Cybersecurity Definitions

Defensive perspective

1. Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders. (Kemmerer, 2003)
2. Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption. (Lewis, 2006)
3. Cybersecurity is the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. (ITU, 2009)
4. The ability to protect or defend the use of cyberspace from cyber-attacks. (CNSS, 2010)
5. The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. (Oxford University Press, 2014)
6. The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (DHS, 2014)

Continuous perspective (ability to survive and adapt over time)
Ecosystem perspective

8. The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access to ensure confidentiality, integrity and availability. (Public Safety Canada, 2014)

Risk perspective

9. Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on. (Amoroso, 2006)

Sociepistemic definition [9] - the 10th defintion

10. Cybersecurity is the organization and collection of **resources, processes, and structures** used to **protect** cyberspace and cyberspace-enabled systems from **occurrences** that **misalign** de jure from de facto **property rights**.

The last definition comprehend four key dimensions:

"the organization and collection of **resources, processes, and structures**"	**Complexity** Complex interactions among humans, between systems and between humans and systems.
"used to **protect** cyberspace and cyberspace-enabled systems"	**Extensiveness** Protection from all threats, including intentional, accidental, and natural hazards.
"from **occurrences**"	**Unpredictability** Threats can also be unpredictable, often arising unexpectedly and in forms that are difficult to anticipate or prepare for.
"**misalign** de jure from de facto **property rights**"	**Ownership** Any event or activity that causes a misalignment between actual (de facto) property rights and perceived (de jure) property rights, whether intentional or accidental. i.e. "The system does not work properly".

[9]Examines how knowledge is created, validated, and shared within social contexts.

3.2.5 Terminologies and Concepts

There is a need to scrutinize the evolving landscape of technology that brings with it new cybercriminal behaviors.

Society is the domain we aim to study.

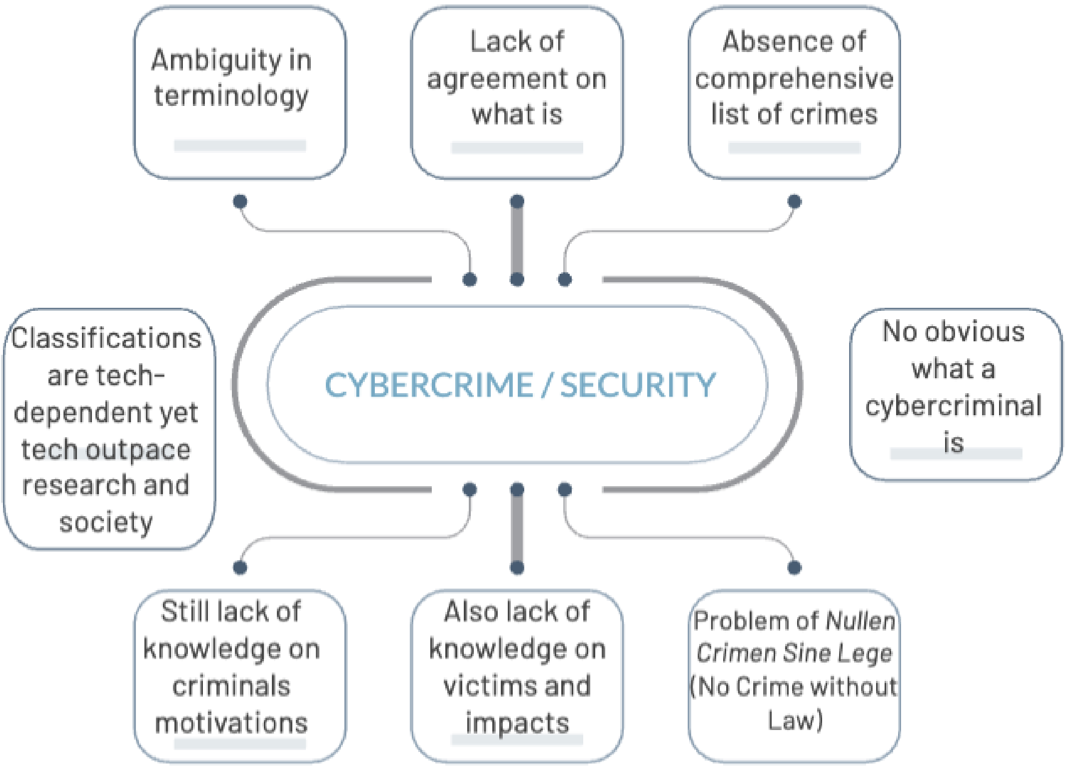

Figura 3.7: Limits and key challenges of cybercrime and cybersecurity

Be aware: today, the spread of knowledge is also influenced by public opinion and various sociological and political factors.

Capitolo 4

LABoratories

4.1 First LAB

[4]

4.1.1 Software Tools

Tool	Description
nmap	It is designed to perform quick scanning of large networks.
Ettercap	Allows performing man-in-the-middle (MITM) attacks and sniffing attacks in a Local Area Network (LAN).
Wireshark	Allows to capture network traffic.
GVM	Performs vulnerability scanning.

Tabella 4.1: Main Software Tools

Command	Description
Apache2	Web server.
VSFTP	FTP server.
SSH2	SSH server
Exim	Mail server

Tabella 4.2: Additional Software Tools

Commands for Softwares

Command	Description	Options
sudo systemctl [options] apache2	Configuration of server ports are at: /etc/apache2/ports.confs	start; stop; restart
systemctl [options] vsftpd	Configuration of server ports are at: /etc/vsftpd.conf	start; stop; restart
sudo systemctl [options] ssh **Before starting the server the first time you must generate the keys of the host with the command:** `ssh-keygen -A`	Configuration of server ports are at: /etc/ssh/sshd_config	start; stop; restart
sudo systemctl [options] exim4	Configuration of server ports are at: /etc/default/exim4.	start; stop; restart
sudo wireshark	Network analyzer	

Tabella 4.3: Softwares Commands

Commands for Networking

Command	Description	Options
arp	Manipulets the system ARP cache.	-d(elete) <ipAddr>; Show: -e (fixed); -a
ip	Analyse and manipulate the routing of IP packets	neigh flush all (delete); -s -s neigh flush all (all-verbose)
netstat	Displays detailed information about a network.	-l(istening) -t(cp); -u(dp)
nmap <ipAddrVictim>	Obtain information of a victim in the network	-O(S); -sT(CP); -Pn (ping) -p <port>; -v(erbose); -sV (service/Version) -T<num> (timer 0-6) -A(ggressive)
ettercap configuration files: `man etter.conf` `/etc/ettercap/etter.conf`.	Executes man-in-the-middle attacks in a LAN.	-T(ext UI); -q(uiet) -M(ITM) [arp;icmp;dhcp;port] -e "<regExpr>" -L <logFile>; -P(lugin)
s-nail	Mail Client. Send and receive Internet mail	-s(ubject); -S(et var)

Tabella 4.4: Network Commands

Insights

- Network Fingerprinting allows obtaining information on the remote host's operating system. Possible using the tool nmap. This technique is based on the fact that different types of operating systems implement differently the TCP/IP stack →nmap.
- The technique known as Port Scanning is used to obtain information about which ports of a particular host are open →nmap.
- A special expression can be used with the port parameter as `-p <initial>-<ending>`
- Identification of services →nmap or a vulnerabilities scanner like GVM (Uses an in-depth scanning).
- MITM attacks (like ARP poisoning) →ettercap.

Commands from the Text

```
#FINGERPRINTING
#Bob(attacker) tries to establish a TCP connection (-sT)
   on the port 80 (-p 80) of the target host Alice, in
   order to obtain information about the operating system
   (-O) running on the victim's machine
nmap -sT -p 80 -O -v <ipAddrVictim>

#PORT SCANNING
#the attacker wants to scan ports of the victim that use
   tcp connections. Scan the first 1024 ports
nmap -sT -p 1-1024 -v <ipAddrVictim>
#version with ping interaction
nmap -Pn -p 1-1024 -v <ipAddrVictim>

#IDENTIFICATION of SERVICES
#the attacker wants to dentify the (application) services
   running on the open ports on victims's machine
nmap -sV -Pn -p 1-1024 -v <ipAddrVictim>
#or a more aggressive version:
nmap -sV -A -Pn -p 1-1024 -v <ipAddrVictim>
#-A: Enable OS detection, version detection, script
   scanning, and traceroute
#more information are provided on the target machine!!

#ARP poisoning
ettercap -Tq -M arp /<ipAddrVictim1>// /<ipAddrVictim2>//
#in addition with regular expression
ettercap -Tq -M arp /<ipAddrVictim1>// /<ipAddrVictim2>//
   -e "<regExpr>"
```

How to use Mail Server - exim

```
#mail server configuration
dpkg-reconfigure exim4-config

#start the mail server
sudo systemctl start exim4

#another user sends an e-mail to the mail server
    #follow the configuration details reported below
#all on the same line
s-nail -S mta=smtp://10.0.24 -S 'from=<userMittent> \\
    @kali' -s "<subjectText>" <userReceiver>@kali
#press enter when finished and then ctrl-D
```

1. Alice configures the `exim` mail server with the command:

   ```
   dpkg-reconfigure exim4-config
   ```

   and by selecting the parameters in the following manner:

   (a) General type of mail configuration: Internet site; mail is sent and received directly using SMTP.
   (b) System mail name: kali
   (c) IP-addresses to listen on for incoming SMTP connections: *// leave blank (delete data if present)*
   (d) Other destinations for which mail is accepted: kali
   (e) Domains to relay mail for: *// leave blank (delete data if present)*
   (f) Machines to relay mail for: *// leave blank (delete data if present)*
   (g) Keep number of DNS-queries minimal (Dial-on-Demand) ?: No
   (h) Delivery method for local mail: mbox format in /var/mail
   (i) Split configuration into small files ? : No
   (j) Root and postmaster mail recipient: *// leave blank (delete data if present)*

Figura 4.1: Configuration parameters for exim mail server in the LAB

4.2 Second LAB

[5]

4.2.1 OpenSSL Commands

Command	Description	Options
man openssl <command>		
openssl enc	Allows the encryption and decryption of data with several symmetric cipher routines.	-help; -ciphers; -p -<algorithm>; -nopadK; -K <hexKey>; -iv <hexVector> -in <inputFile>; -out <outputFile> -iter <n>; -pbkdf2; -nosalt -e (default); -d;
openssl rand <numBytes>	Generates nBytes pseudo-random data.	-hex -out <outputFile>
openssl genrsa <numBits>	Performs simple asymmetric (key pair) operations with the RSA algorithm.	-out <outputFile>
openssl rsa	To manage and use the RSA keys in cryptographic operations.	-in <inputFile>; -out <outputFile> -text; -noout -pubin; -pubout
openssl ecparam	To manage and manipulate the EC algorithm parameters.	-list_curves -name <curveName>; -genkey -out <outputFile>
openssl ec	To manage and manipulate the EC algorithm keys.	-in <inputFile>; -out <outputFile> -pubin; -pubout -text
openssl pkeyutl **Supported algorithms:** RSA, DSA, Diffie-Hellmann and Elliptic Curve. **The order in which the parameters are passed is important.**	Performs asymmetric encryption/decryption, signature/verification, and key exchange, by using various asymmetric algorithms.	-encrypt; -decrypt; -sign; -verify; -verifyrecover -in <inputFile>; -out <outputFile> -pubin; -inkey <keyFile> -sigfile <signatureFile> (verify)
openssl dgst <inputFile>	Allows to calculate the digest of data using different algorithms.	-list -<algorithm>; -out <outputFile>
openssl speed	Measures the performance of the various algorithms implemented by OpenSSL	-evp (ctr)

Tabella 4.5: openssl commands

Insights

- 1 Byte = 2 HEX characters.
- In order to decrypt a file you need to know: iv, K and cipher algorithm.
- In practice, if you have an N-Bytes RSA key, you can perform successfully encryption/decryption operations with OpenSSL only if the (plaintext) data is at most N-11 bytes long.
- RSA-encrypt →public key.
- RSA-decrypt →private key.
- RSA-sign →private key.
- RSA-verify →public key.
- The pubin parameter is used to specify that the input key it has to be a public key.

4.2.2 Utility Commands

Command	Description	Options
systemctl [options] ssh	Must be enabled on the Receiver **Remember to stop it at the end**.	start ; stop ; restart enable ; status
scp <user>@<ipReceiver> :<dirFullName>	Transfers a file to the specified user's directory	start ; stop ; restart enable ; status
openssl rand -out <outputFile> <numBytes>	Creates a file numBytes long.	
time <openssl_command>	Measures the elapsed time of a command.	
expr <arg1> <basicOperation> <arg2>	Performs basic operations. Such as: * / + -	
wget <URL>	For non-interactive download of files from the Web.	
atril <fileName> &	A simple multi-page document viewer.	
sha1sum	Easy computation of the hash of one or more files.	
hashdeep <file/dirName>	Easy computation of the hash of one or more files. Processes recursively the files contained in a directory with a chosen algorithm.	-r; -c <dgstAlgorithm> -m (match) -x (negative match) -k <fileName> (for m or x)

Tabella 4.6: Utility Commands

Insights

- File-transfer protocol: enable ssh server on the receiver (remember to stop it at the end), send the file from the mittent with scp tool.
- Command: `scp <fileName> <user>@<ipReciever>:/home/<user>/Desktop`
- `scp`: in my case user=Alice or Bob, with their ip provided from `ifconfig`, password=0000

Operations with Digests

```
#generate hashes for the files within the "tree" directory
   and save them to hash_list
hashdeep -c sha256 -r tree > hash_list
#check for differences on the same files
hashdeep -c sha256 -r -x -k hash_list tree
```

Operations on Key Pair

```
#create a key pair and save them to a file
openssl genrsa -out rsa.key.Alice 2048
#read the key file
openssl rsa -in rsa.key.Alice -text
#extract only the public key and save it to a file
openssl rsa -in rsa.key.Alice -out rsa.pubkey.Alice -pubout

#encrypt a plain text with a public key
openssl pkeyutl -encrypt -in plain -out encRSA -pubin -inkey
    rsa.key.Alice
#decrypt a cipher text encrypted with RSA, knowing the
   private key
penssl pkeyutl -decrypt -in plain.enc.RSA.for.Alice -inkey
   rsa.key.Alice

#sign a file ("plain") using the private key of Alice
openssl pkeyutl -sign -in plain -inkey rsa.key.Alice -out
   sig.Alice
#verify the signature (on the file "plain") using the public
    key of Alice
openssl pkeyutl -verify -in plain -pubin -inkey rsa.key.
   Alice -sigfile sig.Alice

#generate a SECG curve over a 192 bit prime field and save
   it to a file
openssl ecparam -name secp192k1 -genkey -out ec.key.Alice
#extract the ec public key from a file and save to another
   file
openssl ec -in ec.key.Alice -pubout -out ec.pubkey.Alice

#sign a file ("plain") with  ECDSA and save the signature to
    a file
openssl pkeyutl -sign -in plain -inkey ec.key.Alice -out
   ecsig
#verify the signature of the file signed with ECDSA
openssl pkeyutl -verify -in plain -pubin -inkey ec.pubkey.
   Alice -sigfile ecsig
```

Symmetric Algorithms Performances

Be aware: The real time reported by the time command in the table 4.7 refers to the elapsed wall clock time — the total time from when the command starts executing to when it finishes.

Creating files: `openssl rand -out <outputFile> <numBytes>`.
Measuring elapsed time: `time <opensslEncryptionCommand>`.

	100 B	10 kB	1 MB	100 MB
des-ede3	0.01 s	0.01 s	0.11 s	9.91 s
aes-128-cbc	0.01 s	0.01 s	0.11 s	10.21 s
aes-192-cbc	0.01 s	0.01 s	0.11 s	10.48 s
aes-256-cbc	0.01 s	0.01 s	0.11 s	10.37 s
aes-128-ctr	0.01 s	0.01 s	0.14 s	10.39 s
chacha20	0.01 s	0.01 s	0.12 s	9.18 s

Tabella 4.7: Performance of some symmetric encryption algorithms.

Digest Algorithms Performances

	100 B	10 kB	1 MB	100 MB
sha256	0.01 s	0.01 s	0.01 s	0.12 s
sha512	0.01 s	0.01 s	0.02 s	0.15 s

Tabella 4.8: Costs associated with some digest algorithms

Bibliografia

[1] Antonio Lioy. Introduction to cybersecurity, 2024.

[2] Antonio Lioy. Cryptographic techniques for cybersecurity, 2024.

[3] Giuseppe Tipaldo. Cybersecurity and society, 2024.

[4] Antonio Lioy. Network security – basic attacks, 2024.

[5] Antonio Lioy. Cryptography with openssl– basic operations, 2024.