Politecnico di Torino

Information Systems Security 02TYMWQ

Social Engeneering Module

Accademic Year 2025/2026

Adrian Boniolo S356966

Contents

1 Introduction

1.1 Exam Informations

This part of the course is weighted about the 25% the entire exam. The exam of this module includes contributions from two type of questions.

- **Theoretical Knowledge:** you have to evaluate what you learned about sociological theory relevant to cybersec. In particular you have to interpret / comment a definition, classification scheme or sociological concept ("iceberg", "Cialdini's principle", "3 common traits"). Avoid common sense and demonstrate rigorous and logical understanding of the sociological material, using of precise terminology (e.g. "epistemic asymmetry","technocratic dominance","teleological replacement","norms, values, roles").
- **Application to Practical Case(s):** focus on apply theory to a real-world scenario or scenatio-based question. You have to identify latent fators in social engeneering (urgency, authority, impersionation, etc.) and reference relevant theoretical ideas (e.g. Cialdini's principles, sociological definitions).

An answering strategy is to be structured and coincise to connetc the general theoretical knowledge to the specific question.

1.2 Goal of the course

This module is complementary to the main part of the class, which is strongly tech-oriented. You will identify sociotechnical vulnerabilities and help mitigate their consequences.The technical aspect is necessary but not sufficient for cybersecurity, the humans are structural points of every security system, but not only weakpoints.This part will teach to analyze complex social mechanism, such as the social construction of knowledge, risk, trust, manipulation and communication.

2 Social Engeneering

2.1 First definition

- ***The science of social phenomena subject to natural and invariable laws, with the goal of discovering these laws.*** - This definition was made in the 1839 by Auguste Comte, inventor if the word "Sociology".
- ***Sociology is the study of human social life, groups and societies.*** - This definition was made by Giddens.
- ***Sociology is the scientific study of society, including the intricate patterns of social behaviour, relationships and human interactions. Is an examination of social institutions, cultural norms and social change using empirical and criticar research and analysis. Those in sociology investigate various aspects of human life, including social stratification, movement and change, with an emphasis on how collective and individual behaviour shapes and is shaped by the broader social context.*** - This is the definition of ChatGPT.

Weber's Wertfreiheit (principle of Value-freedom to be intended as scientific neutrality) states that researchers must refrain from introducing personal value judgments when conducting scientific analysis.
From Weberian neutrality to responsibility:
don't pretend to be apolitical or indifferent (social research has to clarify risks, trade-offs and consequences helping society make informed decisions) be cause in cybersecurity it's not only about protecting systems but also about protecting society (rights, trust and human dignity), mitigating digital and epistemic asymmetries as well as inequalities.

2.2 What is social engeneering.

The use of **decption** in order to induce a person to divulge private information or unwittingly provide unauthorized access to a computer system or network.
Decption social performances, relies on trust rituals, impression management, symbolic manipulation. We study how people interpret intentions, asess credibility and react under uncertainty.
Induce implies **persuasion**, **framing** and **nudge techniques.**

After all, cybersecurity is fundamentally about an adversarial engagement. Humans must defends machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engeneering and mathematics perspectives from other fields are needed.
Craingen et al., 2014, Defining Cybersecurity.

2.3 Ethics and Epistemics

- **Avalutativity**: The principle of refraining from value judgments in sociological analysis.
- **Extensivity**: A macro-level approach focused on generalisation, stimulus invariance, quantification, and the recognition of limits in broad patterns.
- **Intensivity**: A micro-level approach aimed at understanding the meaning behind actions, qualification of phenomena, and the limits of interpretation.
- **Creative gift of the intellect**: The capacity to generate novel insights and connections beyond immediate observation.
- **The 'Martian' look**: A form of cognitive training that encourages detached observation, as if from an outsider's perspective.

Sociologists are trained to observe both micro- and macro-social phenomena without awe or wonder, even when these phenomena appear distant or disconnected from their own experience.They must avoid taking everyday life and what is considered 'normal' (i.e., institutionalised and seemingly familiar) for granted.The goal is to offer explanations of social phenomena that are less biased and more analytically grounded.In both approaches, the epistemic status of data remains uncertain; information is always partial and context-dependent.

2.4 Basic sociological vocabulary

- **Norms:** rules and expectations by which a society guides the behavior of its memmbers.
- **Values:** collective ideas about what is good, desirable and proper.
- **Role:** set of norms, behaviors, and expectations that are associated with a particular social status or position whitin a society. Roles guide how individuals are supposed to act and interact with others specific contexts.
- **Social Structure:** the organized pattern of social relationships and social institutions that together constitute society.
- **Culture:** shared bielifs, values and practices.

2.5 Iceberg Principle

The *iceberg principle* in social engineering suggests that the visible part of an attack represents only a small fraction of the overall operation. Most of the preparation, psychological manipulation, and information gathering happens beneath the surface, making the threat far more extensive than what the victim initially perceives.

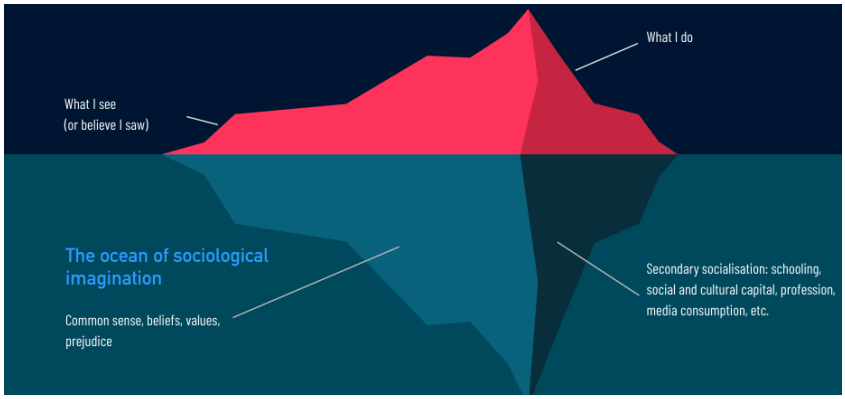

Figure 1: Iceberg's principle

2.6 Overview of Cybersecurity

The name of the "rose". The passage highlights that the absence of clear and shared definitions makes it difficult to measure and classify cybercrime. Barn and Barn argue that without a consistent vocabulary, professionals cannot reliably describe or compare the same phenomena. The reference to Shakespeare's line about the rose works as a contrast: unlike in poetry, in the study of cybercrime the name truly matters. How we label an act determines whether it is recognised, counted, and addressed. Precise terminology is therefore essential for producing reliable data, shared understanding, and effective responses.

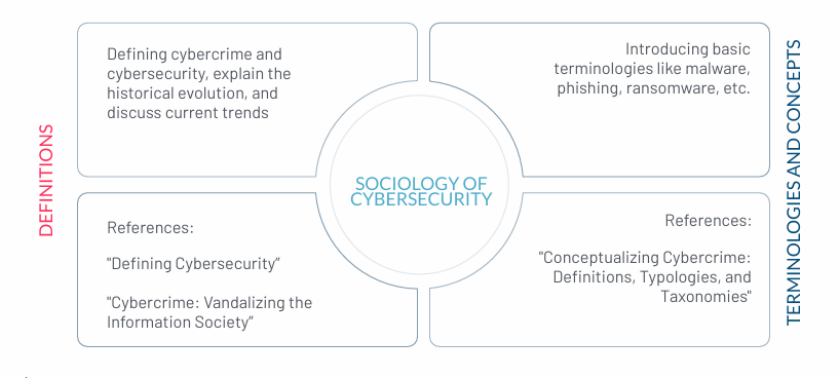

Figure 2: Iceberg's principle

What is? "A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, 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.

2.7 Cybercrime.

2.7.1 Dichotomic definitions

We could have two different approaches: categorical vs continuum.
In a Categorical Approach we could distinguish

- **Cyber-enabled:** are traditional crimes that predate the advent of the technology, and are now facilitated or have been made easier (i.e., enabled) by cyber technology. Crimes range from white-collar crime to drug trafficking, to online harassment, terrorism and beyond.
- **Cyber-dependent:** are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside of the digital world, e.g., hacking, such as ransomware attacks or hacktivism

In a Continuum Approach

- **Type I:** cybercrimes are considered to be more technical in nature, for example, hacking, similar to 'cyberdependent' crimes as described previously.
- **Type II:** are generally considered to involve more human contact, for example, online gambling, similar to 'cyberenabled' crimes as described above.

2.7.2 Trichotomic definitions

Cybercrime is commonly divided into three categories:

- **Crimes Against the Machine** (computer integrity crimes): hacking, cracking, DoS/DDoS.
- **Crimes Using the Machine** (computer-assisted crimes): piracy, fraud, robbery.
- **Crimes In the Machine** (computer content crimes): hate speech, harassment, pornography.

Cybersecurity Foundations Cybersecurity is a contested, multidisciplinary field involving adversarial dynamics:

- Humans defend machines from other humans using machines.
- Requires input from computer science, engineering, law, philosophy, and sociology.
- Incidents often arise from misalignment between *de jure* (legal) and *de facto* (actual) property rights.

Some definitions. Here the definitions by Craigen et al. 2014.

#	Focus	Keywords
1	Intrusion detection	defensive methods
2	Network protection	malicious damage
3	Holistic toolkit	policies, safeguards
4	Cyber-attack defense	cyberspace protection
5	Legal framing	unauthorized use
6	System integrity	modification, exploitation
7	National continuity	infosociety, infrastructure
8	CIA principles	confidentiality, integrity, availability
9	Risk reduction	authentication, encryption
10	Property rights	de jure vs de facto misalignment

2.8 What is cybersecurity?

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 gap that cybercrime makes, broadly construed, is an occurrence the main result of which is to make a gap (misalignment) between a de-jure right and a factual situation.For example ransomwares jeopardize access and property of data (asset).Still people sometimes fail to catch that conduct in the cyberspace has real implications in the analogical world. But digital is not detached from the "real world". Laws from the physical world are not suspended online.

2.9 Paradigms and Dimensions

- **Continuity**: preserving the digital society.
- **Ecosystem**: human-system interactions.
- **Risk**: managing uncertainty.
- **Ownership**: access, control, exclusion.
- **Unpredictability**: threats can be accidental or unknown.

Cybercrime Categories (Extended Table) The table summarizes the five-category typology of cybercrimes.

Category	**Subtypes**
Cyberbullying & Stalking	Denigration, Exclusion, Flaming, Harassment, Outing, Cyberstalking, Dating abuse
Digital Piracy	Piracy
Hacking & Malware	Unauthorized access, viruses, file destruction, service theft, credit card fraud, malware
Identity Theft	Identity fraud
Sex-Related Crimes	Grooming, sexting, CSAM, revenge porn, sextortion

2.10 Limits and key challenges

There is a need to scrutinize the evolving landscape of technology that brings with it new cybercriminal behaviors. Need for further empirical studies regarding the criminal use of advanced technologies such as AI, Machine/Deep Learning, Deep Fakes and Virtual Reality, which are relatively unaccounted for by current classification frameworks, as well as the use of technology for terror-related activities including extremism and radicalization.

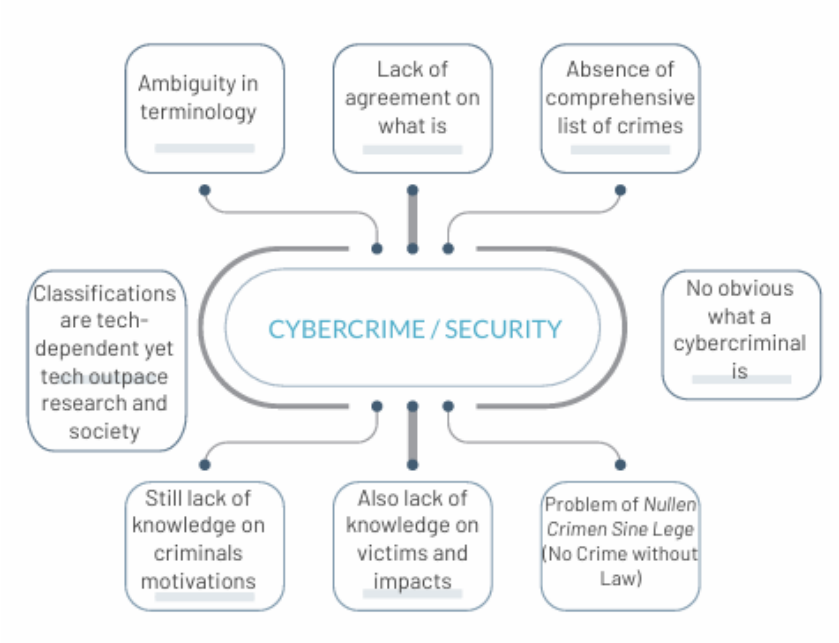

Figure 3: Iceberg's principle

3 Technical languages

3.1 Common semantic dimensions

We could see two different meanings according to dictionary. Social and political sciences use centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society. On the other hand, the use of deception is praticate to induce a person to divulge private information or exposing unauthorized access to an information system. The common semantic dimensions are:

- Epistemic asymmetry
- Technocratic dominance
- Teleological replacement

Epistemic asymmetry: occurs when one person or group enjoys a significant advantage of knowledge over another person or group within a specific domain to which that knowledge applies.

Technocratic dominance: occurs when a person or group possessing a high-degree of technical knowledge uses that knowledge to enact changes in the behavior of others, where such behaviors place those affected in a position of decreased power or authority relative to the former within the affected domain. One consequence of this in the STS domain is the so called «Knowledge deficit» model.

Teleological replacement: occurs when person or group A manages to substitute, in individual or group B, the original purpose or goal of their behavior with that of A.

Deception: social performance, relies on trust rituals, impression management, symbolic manipulation. We must study how people interpret intentions, assess credibility and react under uncertainty. Induce implies persuasion, framing, and nudge techniques.

According to the Oxford English Dictionary, the term "Social Engieering" has two distinct meanings depending on the context in which it is used. In the field of social and political sciences, SE refers to the use of centralized planning as a strategy to manage social change and regulate the future development and behavior of a society. This involves guiding societal progress through structured decision-making and policy implementation. In contrast, within the realm of cyberspace, SE stands for the use of deception to manipulate individuals into revealing private information or providing unauthorized access to computer systems or networks. Despite these differences, both applications share common semantic dimensions identified by Hatfield 2017, including epistemic asymmetry, where one party possesses knowledge that others do not; technocratic dominance, reflecting control by experts or specialized systems, teleological replacement, which involves substituting one set of goals or processes with another to achieve desired outcomes. These shared dimensions highlight the underlying conceptual parallels between SE in social regulation and in cybersecurity, despite their different practical contexts.Social engineering used to be about political action to fix society ills.

3.2 Cialdini's principles

Robert Cialdini outlines six key principles of **persuasion** which are fundamental to understanding how social engineering tactics can be effective.

Reciprocity The principle of **reciprocity** is based on the idea that individuals feel a natural obligation to return favours or concessions they have received. When someone performs a helpful action, offers support, or provides a small benefit, the recipient typically experiences social pressure—often unconscious—to reciprocate. In the context of social engineering, attackers exploit this psychological mechanism by offering small gifts, assistance, or seemingly valuable information. This creates a sense of indebtedness in the target, who may then feel compelled to "give something back," potentially by disclosing sensitive or confidential information. Reciprocity thus becomes a powerful lever for manipulating behaviour and lowering a victim's resistance.

Commitment and consistency The principle of **commitment and consistency** refers to the human tendency to align future behaviour with previous decisions or statements. Once individuals commit to something—especially if the commitment is explicit or public—they feel internal and social pressure to act in ways that remain consistent with that initial choice. This mechanism is frequently exploited in social engineering. An attacker may begin by eliciting a small, seemingly harmless agreement from the target. This initial compliance increases the likelihood that the target will later accept a larger request, a dynamic known as the *foot-in-the-door* technique. By leveraging the desire for consistency, attackers gradually escalate their demands while reducing the victim's psychological resistance.

Social proof The principle of **social proof** describes the human tendency to look to others when deciding how to behave, particularly in situations of uncertainty or ambiguity. When individuals observe that many people are performing a specific action, they often interpret that behaviour as appropriate or correct, relying on the group as a guide for their own decisions. Social engineers exploit this psychological mechanism by fabricating scenarios in which a behaviour appears widespread or commonly accepted. For example, an attacker may create the illusion that numerous users have already clicked on a particular link or followed a certain procedure. Faced with this perceived consensus, the target becomes more inclined to imitate the behaviour, lowering their guard and increasing the likelihood of compliance.

Authority The principle of **authority** highlights the human tendency to comply with requests made by individuals perceived as legitimate authority figures. Titles, uniforms, professional roles, and other

symbols of status significantly increase the likelihood that people will obey instructions without questioning them. Social engineers frequently exploit this psychological bias by impersonating authoritative roles, such as company executives, IT administrators, or security personnel. By presenting themselves as figures with institutional power or technical expertise, attackers reduce the target's resistance and create a context in which compliance feels both expected and justified. This manipulation enables them to extract sensitive information or gain unauthorized access with minimal scrutiny.

Linking The principle of **liking** is grounded in the idea that people are more easily influenced by individuals they find appealing or relatable. Factors such as physical attractiveness, perceived similarity, genuine compliments, and a sense of familiarity all contribute to increasing interpersonal liking, which in turn enhances compliance. Social engineers routinely exploit this mechanism by deliberately building rapport with their targets. They may highlight shared interests, mirror the target's attitudes, or offer flattering remarks to create a positive emotional connection. Once the attacker is perceived as likable or trustworthy, the target becomes significantly more susceptible to influence, making it easier to extract information or persuade them to take harmful actions.

Scarcity The principle of **scarcity** is rooted in the idea that people tend to assign greater value to things that appear limited or difficult to obtain. When an opportunity, resource, or piece of information is framed as scarce, individuals often experience a heightened sense of urgency and a fear of missing out, which can drive them to act more quickly and with less deliberation. Social engineers exploit this psychological bias by fabricating situations in which time, access, or availability seems restricted. For example, an attacker may claim that a particular offer, security update, or internal request is only available for a short period, pressuring the target into responding immediately. This artificially induced urgency reduces critical thinking and increases the likelihood of impulsive, risky decisions.

3.3 Old and new Techniques

Impersonation May be used in an attempt to gather authentication information (e.g. usernames and passwords) to gain access to a targeted network.

3RD Party Authorization Occurs when authentication details are stolen by or given to a third party

Phishing Attempt to trick the recipient into performing some action, usually clicking on a link or downloading an attachment, by masquerading as legitimate requests for information, security warnings, or normal e-mails from friends or co-workers.

Pop-ups Can be a potent tool for social engineering tactics due to their ability to appear unexpectedly and grab immediate attention.

Dumpster Diving refers to searching through physical trash or recycling bins to recover sensitive information. This may include personal data (names, addresses, phone numbers, social security numbers) or corporate documents (internal memos, financial reports, strategic plans). *Example: An attacker retrieves discarded employee records and uses them for identity theft or social engineering.*

Shoulder Surfing involves observing someone over their shoulder to capture confidential information, such as PINs or passwords. Attackers may also record keystrokes using small cameras or direct observation. *Example: While standing behind a person at an ATM, the attacker memorizes their PIN.*

In-Person Attack includes physical presence tactics like impersonating staff or exploiting unattended workstations. These attacks rely on proximity and trust to gain unauthorized access. *Example: An intruder enters a company office pretending to be IT support and accesses a logged-in terminal.*

Improper Use of Social Media occurs when individuals share sensitive content online, use weak passwords, or neglect two-factor authentication. This can expose personal or professional details that attackers exploit. *Example: A user posts a photo of their work badge on Instagram, revealing their full name and company ID.*

Internal Social Engineering occurs when system administrators or internal security teams simulate attacks (e.g., phishing emails, spam) within their own organization. The goal is to identify vulnerable individuals and improve overall security awareness. This method helps expose weak points in the human element of cybersecurity. *Example: A company sends fake phishing emails to its employees to test who clicks on malicious links, then provides targeted training to those who failed.*

Reverse Social Engineering flips the traditional dynamic: instead of the attacker initiating contact, the victim is manipulated into reaching out to the attacker. This technique exploits trust and curiosity, often leveraging social media or misleading prompts. *Example: An attacker posts online claiming to offer tech support for a common issue, prompting users to contact them and unknowingly share sensitive information.*

Automated Social Engineering leverages botnets, algorithms, and automated programs to replicate traditional SE attacks at scale. These methods reduce the need for direct attacker-victim interaction and can target thousands of users simultaneously. *Example: A botnet sends personalized phishing messages to employees across multiple companies, exploiting known vulnerabilities in email filters.*

Semantic Attacks aim to deceive victims by manipulating the appearance or meaning of objects, rather than directly breaching systems. These attacks exploit trust and perception. *Example: A spoofed website mimics a legitimate banking portal but is hosted on a malicious server. Victims enter their credentials, unknowingly handing them to the attacker.*

Sybil Attack is a subtype of semantic attack where an attacker creates multiple fake identities on a social network. These personas are used to flood the platform with coordinated messages, giving the illusion of consensus. *Example: An attacker uses dozens of fake profiles to promote misinformation, making it appear as the dominant viewpoint and suppressing dissent.*

Scareware is another semantic tactic that frightens users into taking harmful actions. It typically presents fake alerts about malware infections and prompts users to download malicious software disguised as antivirus tools. *Example: A pop-up claims "Your system is infected!" and urges the user to install a fake antivirus, which is actually spyware.*