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.

2.2 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.

2.3 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.

2.4 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.

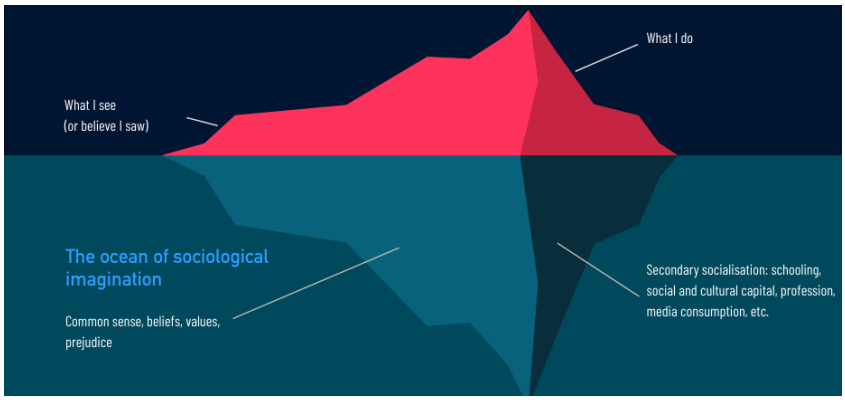

Figure 1: Iceberg's principle

2.5 Overview of Cybersecurity

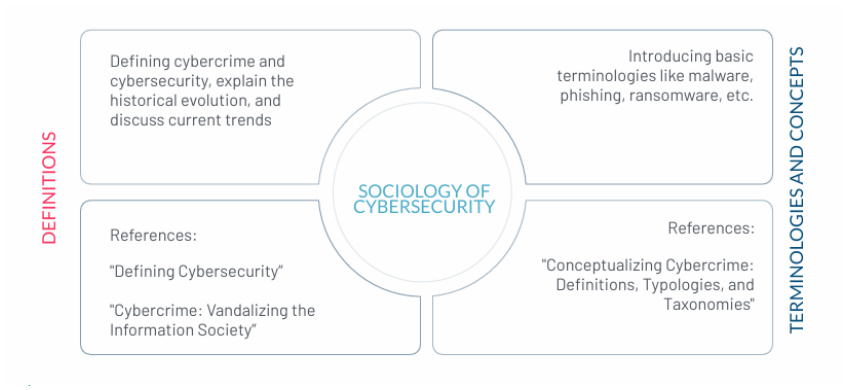

Figure 2: Iceberg's principle

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.

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.

Cybercrime definitions. Dichotomic definitions (in research and policy making). 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.

Security is a contested concept, but it generally refers to a condition of being free from danger or threat. According to Buzan, Wæver and Wilde, security discourse requires identifying who performs securitization, which threats are addressed, for whom protection is intended, why it occurs, with what outcomes, and under which structural conditions. In cybersecurity, the lack of a single shared definition has led to multiple interpretations that emphasise risk, control, defence, continuity, and the broader digital ecosystem.

Paradigm	**Summary of Focus**
Risk & Control	Cybersecurity as the management of threats, intrusions, and vulnerabilities through defensive methods, monitoring, and protective measures.
Defence	Cybersecurity as the protection of networks, data, and infrastructures through technologies, safeguards, and response mechanisms ensuring confidentiality, integrity, and availability.
Continuity	Cybersecurity as the preservation of the functioning and stability of the information society, ensuring resilience and uninterrupted operations.
Ecosystem	Cybersecurity as a complex environment involving tools, policies, training, best practices, and organisational processes that collectively protect digital assets.

Table 1: Synthesis of cybersecurity paradigms

Across these perspectives, cybersecurity can be understood as the set of practices, technologies, and organisational processes aimed at protecting digital environments, reducing risks, and ensuring the continuity and resilience of information systems.

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.

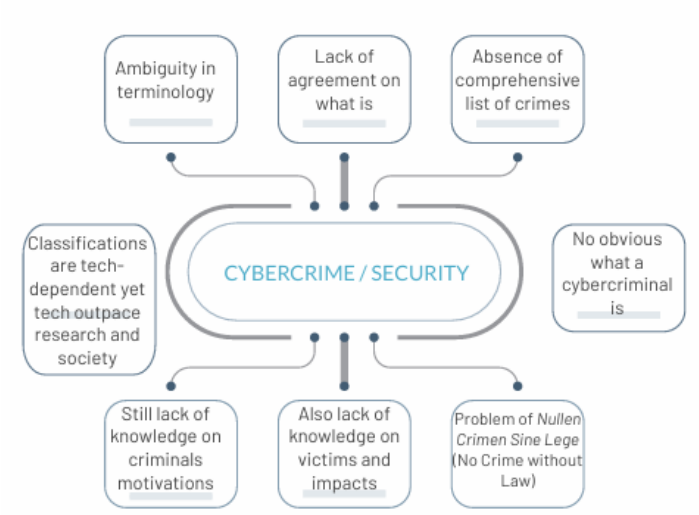

Figure 3: Limits and key challenges