POLITECNICO DI TORINO

Fundamentals of Information Systems Security

Student:

Gianmarco Michelini

Academic Year 2024/2025

All notes are derived from oral presentations and written papers.

Contents

List of Figures

List of Tables

Chapter 1

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".

1.1 Sociology, Really?

1.1.1 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 social order, 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

1.1.2 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]

1.1.3 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]

> 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.

1.1.4 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:

[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.

  - 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:

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

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.

1.1.5 Cybersecurity and Society

The figure 1.1 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.

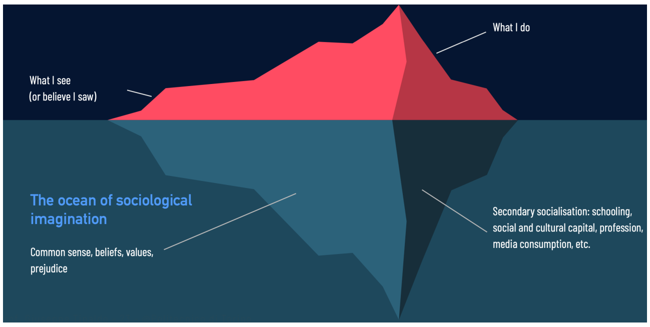

What I see
(or believe I saw)
What I do
The ocean of sociological imagination
Common sense, beliefs, values, prejudice
Secondary socialisation: schooling, social and cultural capital, profession, media consumption, etc.

Figure 1.1: The Iceberg Relation

1.2 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.

1.2.1 Overview of Cybersecurity

The diagram 1.2 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.

[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.

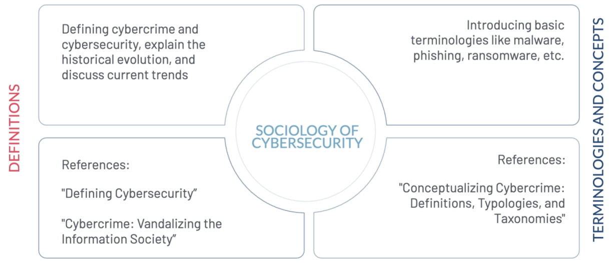
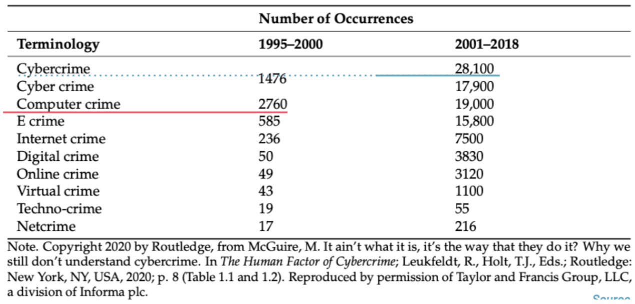

DEFINITIONS
Defining cybercrime and cybersecurity, explain the historical evolution, and discuss current trends
References:
"Defining Cybersecurity"
"Cybercrime: Vandalizing the Information Society"
SOCIOLOGY OF CYBERSECURITY
Introducing basic terminologies like malware, phishing, ransomware, etc.
References:
"Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies"
TERMINOLOGIES AND CONCEPTS

Figure 1.2: Overview of Cybersecurity from a sociological perspective

1.2.2 Definitions of Cybercrime

1.2.2.1 Vocabulary

Figure 1.3 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

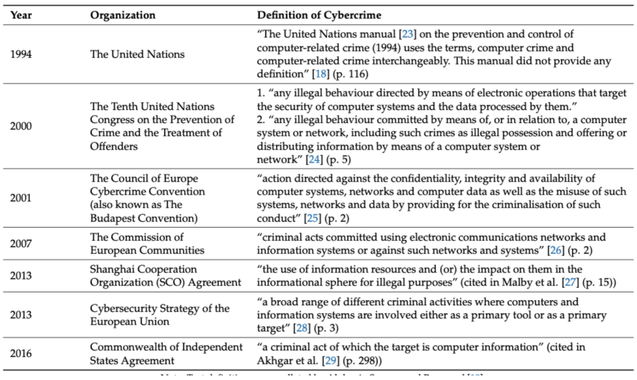
Note. Copyright 2020 by Routledge, from McGuire, M. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In *The Human Factor of Cybercrime*; Leukfeldt, R., Holt, T.J., Eds.; Routledge: New York, NY, USA, 2020; p. 8 (Table 1.1 and 1.2). Reproduced by permission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

Source

Figure 1.3: Cybercrime terminology in the periods 1995-2000 and 2001-2018

1.2.2.2 Official Definitions

Figure 1.4 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))

Figure 1.4: Organization definitions of cybercrime

1.2.2.3 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.

Categorical Approach
CYBER-ENABLED
VS
CYBER-DEPENDENT

Figure 1.5: 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.

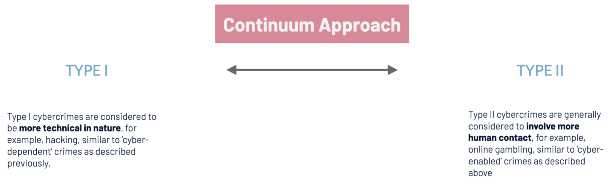

Continuum Approach
TYPE I
TYPE II
Type I cybercrimes are considered to be **more technical in nature**, for example, hacking, similar to 'cyber-dependent' crimes as described previously.
Type II cybercrimes are generally considered to **involve more human contact**, for example, online gambling, similar to 'cyber-enabled' crimes as described above

Figure 1.6: Continuum approach to cybercrime

1.2.2.4 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.

1.2.3 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

[5] Crimes concern many fields of phenomena.

> 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.

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

1.2.4 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)

[6] Craigen et al.2014

[7] 2010

[8] The *phygital* reality. A funsion of physical and digital realities

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[9] and **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 [10] - 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**.

[9] Ability to survive and adapt over time

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

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".

1.2.5 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.

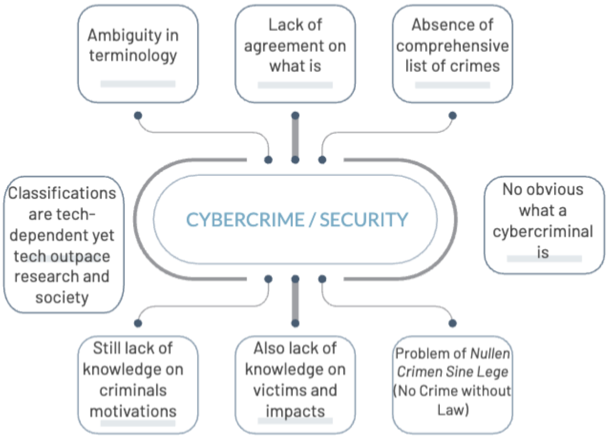

Ambiguity in terminology
Lack of agreement on what is
Absence of comprehensive list of crimes
Classifications are tech-dependent yet tech outpace research and society
CYBERCRIME / SECURITY
No obvious what a cybercriminal is
Still lack of knowledge on criminals motivations
Also lack of knowledge on victims and impacts
Problem of *Nullen Crimen Sine Lege* (No Crime without Law)

Figure 1.7: 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.

Chapter 2

Social Engineering

What is Social Engineering?

SE has two different meanings according to dictionaries:

1. **Social and Political Sciences**: the use of centralized planning in an attempt to manage social change and regulate the future development and behavior of a society.

   There is a need for experts to create social or economic policies, as these are not tasks that everyone can undertake.

   SE as Policy-making strategy.

2. **Cyberspace**: the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Common Semantic Dimensions

Hatfield, 2017.

Epistemic asymmetry

"Knowledge" asymmetry.
Occurs when one person or group enjoys a *significant advantage in terms of knowledge* over another person or group *within a specific domain* to which that knowledge applies.

|| Doesn't necessarily imply a technocratic dominance.||

For example, what we typically experience with professors.

Teleological replacement

"Purpose", "end".
Occurs when person or group A successfully substitutes the original purpose or goal of individual or group B's behavior with their own.

We can say, "My goals become your goals" (implementing a social strategy that contradicts your aims).

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[1] domain is the *Knowledge Deficit* Model: The more ignorant you are, the more you fear and refuse to accept advancements.

A side effect of an originally very good solution (which clashes with the ideas of liberal democracy), referencing the San Mathews effect[2].

|| It is a choice, based on your knowledge.||

2.1 The Definition

Political social engineering and technological social engineering are different phenotypical expressions of the same underlying genotype, characterized by epistemic asymmetry, technocratic dominance, and teleological replacement.
As technical security measures increased in their sophistication, "computer hackers", began to rely more and more on non-technical methods to achieve their goals.

Key features of social engineering attacks

1. Psychological manipulation.
2. Tech illiteracy and lack of critical sense (Naivety or curiosity).
3. Exploitation of trust.
4. Use of fear or urgency: self/business-protection.
5. Impersonation.
6. Propaganda and misinformation.

   "The scandal becomes the message itself."

7. Organizational/Cultural level: exploitation of group dynamics (Sometimes, the dynamics of power hierarchies suppress people's instinct to protect others).
8. Media arena: exploitation of the media to spread false information (Also decontextualizing).

   "How nothing becomes everything."

9. Procedural failures: lack of security protocols or poor implementation.

Preventing Social Engineering Attacks

To prevent social engineering attacks, individuals and organizations can:

- Educate employees about the risks and signs of social engineering.

The Human is the weakest part of a modern system.

[1] Multidisciplinary field that studies the conditions under which science and technology develop, and how these developments shape society, politics, and culture.

[2] In the context of social sciences, the term is sometimes used to describe the negative consequences of rapid, unplanned urban development, such as increased social stratification, lack of infrastructure, or economic disparity.

- Implement strict verification processes for sensitive information requests.
- Use multi-factor authentication to add an extra layer of security.
- Regularly update and patch systems to protect against vulnerabilities.
- Encourage a culture of skepticism and caution regarding unsolicited communications.

"The greatest asset of a hacker is not their computer, but their ability to manipulate people."

A technician or security professional must indeed study aspects of human behavior and psychology.

2.2 Cialdini's Principles

The book *"Influence: Science and Practice"* (by Robert Cialdini, 1984) outlines six principles of persuasion that can be used to influence people's behavior. These principles are:

1. **Reciprocity**: People feel obligated to return a favor (it's not a simple exchange of resources, but a social norm).

   Example: An attacker might offer a gift to a target, making the target feel obligated to reciprocate by providing personal information.

2. **Commitment and Consistency**[3]: Once people commit to something, they tend to follow through to remain consistent with their commitment. When someone's mindset or behavior is not aligned with their actions or beliefs (cognitive dissonance), they will often change their beliefs to match their actions. Protecting behaviors by ignoring inconsistencies (neglecting the truth) is a common defense mechanism to maintain psychological stability.

   Example: Attackers might use a small request (foot-in-the-door technique) to make a target agree to larger requests later. The initial small agreement sets a commitment, which makes further compliance more likely.

3. **Social Proof**: People look to others to determine how to behave, especially in ambiguous situations.

   Example: Attackers might use fake testimonials or reviews to make the scenario as credible as possible, convincing the target that others have benefited from their scam.

4. **Authority**: People tend to obey authority figures, even if they are asked to perform objectionable acts.

   Example: Attackers might impersonate a figure of authority, such as a police officer or IT technician, to gain the target's trust and compliance.

[3] Consistency is not intended to be morally adequate or coherent, but rather as a proxy for believing and trusting someone else. Consistency is treated as a strategy, requiring effort to maintain or escape from.

5. **Liking** ("influencers principle" in the digital age): People are more likely to be influenced by people they like.

   Example: Attackers might build rapport with the target by finding common interests or using flattery to make the target more receptive to their requests.

6. **Scarcity**[4]: People are more likely to desire something if they believe it is scarce or in limited supply.

   Example: Attackers might create a sense of urgency by claiming that an offer is available for a limited time (scarcity) or that a product is in high demand, prompting the target to act quickly.

2.3 SE - Old and New Techniques

In order to configure a taxonomy of social engineering attacks.

- Impersonation ("faking an identity"): pretending to be someone else to gain access to sensitive information.
- 3RD Party Authorization: occurs when authentication details are stolen by or given to a third party.
- Phishing: sending fraudulent emails or messages to trick people into revealing personal information.
- POP-UPS: fake alerts or notifications (grab immediate attention) that trick users into clicking on malicious links.
- Dumpster Diving: Searching through trash to find sensitive information. An upgrade could involve searching through social media.
- Improper Use of Social Media: Sharing sensitive content (often poorly protected) on social media platforms.
- Shoulder Surfing: observing someone over their shoulder. This method exploits the physical proximity to the target to gather sensitive data without the need for technology.
- In Person Attack: on-site impersonation or simply utilizing someone's terminal.
- Internal SE ("rebalancing the epistemic asymmetry"): occurs when system administrators use social engineering techniques against their own organization.
- Reverse Social Engineering: occurs when the attacker convinces the victim to initiate contact.
- Automated Social Engineering: uses automated tools (e.g. botnets) to perform social engineering attacks.
- Semantic Attacks: unlike direct technical attacks, semantic attacks focus on exploiting misunderstandings or misinterpretations of language, such as word choice, phrasing, or context to manipulate the target.

[4] Not just a material scarcity, but also a psychological one (e.g. toxic relationships).

2.4 Developing a Framework for Social Engineering Attacks

2.4.1 SE - Kevin Mitnick's Attack Cycle

Kevin Mitnick's Social Engineering Attack Cycle, prototype of a social engineering attack.

The typical cycle involves four stages:

1. **Research**: gathering information about the target, such as personal details, interests, and relationships.
2. **Developing Rapport and Trust** (the social part): building a relationship with the target to gain their trust and cooperation.
3. **Exploiting Trust**: using the established rapport to manipulate the target into divulging sensitive information or performing actions that benefit the attacker.
4. **Utilize Information**: using the information obtained to further exploit the target or carry out additional attacks.

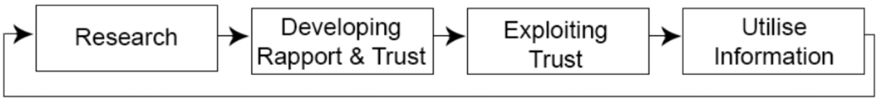


Figure 2.1: Kevin Mitnick's Social Engineering Attack Cycle

2.4.2 SE - Ontological Model

The diagram 2.2 outlines the components and relationships involved in a social engineering attack. The core of the schema is the attack itself, referred to as "the event."
This central event connects key elements, including the social engineer (the attacker), the target (the victim), the medium (the communication channel), the techniques employed, the compliance principles exploited, and the goal of the attack. Each component plays a distinct role in the orchestration and execution of the attack.

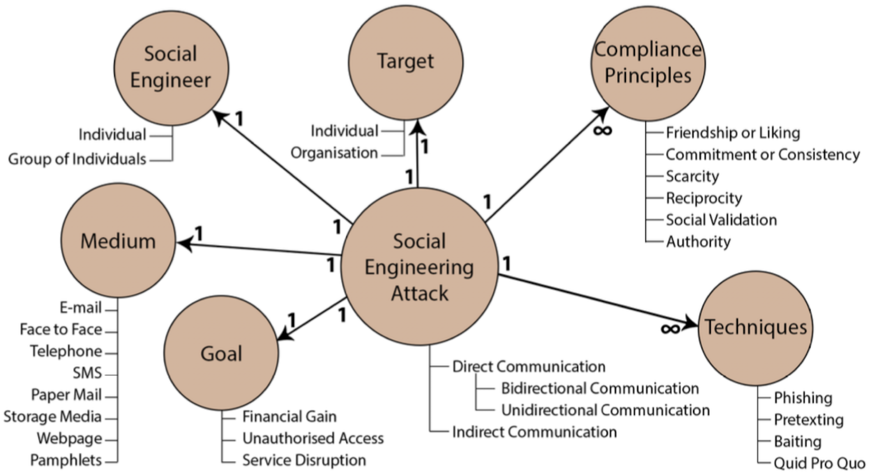


Figure 2.2: Ontological Model of Social Engineering

2.4.3 SE - Attack Framework

The figure 2.3 illustrates a comprehensive framework for social engineering attacks, which includes the following components:

- **Preparation**: analyzing and synthesizing gathered information.
  - Combination and analysis of gathered information.
  - Development of an attack vector: The attacker formulates a specific strategy or approach to exploit the target effectively.
- **Information Gathering**:
  - Identify potential sources.
  - Gather information from sources.
  - Assess gathered information: Evaluating the quality, relevance, and utility of the collected data.
- **Attack Formulation**: This stage transitions from data collection to defining the objectives and scope of the attack.
  - Goal identification.
  - Target identification.

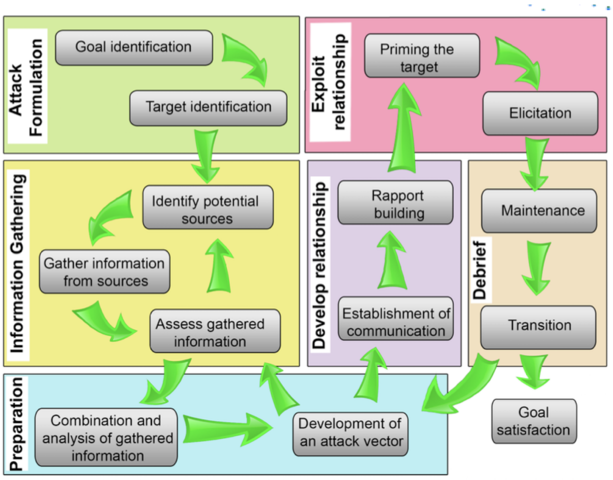


Figure 2.3: Social Engineering Attack Framework

- **Develop Relationship**: Establishing trust and rapport with the target to facilitate manipulation.
  - Establishment of communication.
  - Rapport building.
- **Exploit Relationship**:
  - Priming the target: Preparing the target to act in a way that benefits the attacker, often using psychological principles.
  - Elicitation: Drawing out sensitive or useful information from the target without their awareness.
- **Debrief**: Ensures that the attacker successfully transitions out of the operation and confirms that their goal has been achieved.
  - Maintenance: Keeping the relationship or access open for potential future attacks.
  - Transition: Shifting focus once the primary objective is achieved.

2.5 More than Tech

Considering critical infrastructures as sociotechnical systems.

2.5.1 Sociotechnical Studies

Interdisciplinary field that explores the interactions between people (social systems) and technology (technical systems). This approach recognizes that technology and society are interdependent and that changes in one system can have significant impacts on the other.

Sociotechnical studies aim to provide a comprehensive understanding of how technology and society coevolve and to inform the design and implementation of technologies that are socially responsible and beneficial.

Cybersecurity and S-T Systems - A Brief History

The advent of personal computing and the internet in the late 20th century introduced the first major cybersecurity concerns. Initially, efforts were focused **primarily on technical solutions**, such as firewalls and antivirus software, to combat cyber threats. However, as technology became increasingly embedded in all aspects of society, the scope of cybersecurity expanded to encompass social, cultural, and organizational dimensions.

From early on, the sociotechnical systems (S-T) perspective emphasized that cybersecurity challenges **cannot be resolved through technical measures alone**. Social factors—such as user behavior, organizational practices, and policy frameworks—play an equally critical role in ensuring robust cybersecurity defenses.

The 2000s saw a dramatic increase in cybercrime. This period underscored the need for a more integrated approach to cybersecurity that incorporates both social and technical dimensions. Research began to focus on issues like user education, insider threats and the socio-economic drivers of cybercrime.
The S-T systems approach became more prominent in cybersecurity research, emphasizing the need to **design systems that are resilient to both technical exploits and social engineering attacks**.

The current era is characterized by rapid digital transformation, with technologies such as AI, IoT, and big data. As organizations undergo digital transformation, cybersecurity challenges have become more complex and persuasive. There is an increasing focus on the **ethical implications** of cybersecurity practices, data privacy and the balance between security and civil liberties.

2.5.2 Emergent Properties

Behavior of sociotechnical system cannot be fully understood by analyzing its components in isolation; **interactions** between components generate **new properties**.
In ICT (Information and Communication Technology) systems, the interaction between users, technologies and organizational processes can **lead to unexpected outcomes**.

Bibliography

[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. Security of ip networks, 2024.

[5] Antonio Lioy. Firewall and ids/ips, 2024.

[6] Antonio Lioy. Security of network applications, 2024.

[7] Antonio Lioy. Lab, network security, basic attacks, 2024.

[8] Antonio Lioy. Lab, cryptography with openssl, basic operations, 2024.

[9] Antonio Lioy. Lab, cryptography with openssl - applications, 2024.