The Power of Words in The Digital Era: The Impact of Terminology on Responses and Security Mechanisms in Combating Phishing

Costinel-Valeriu GONCIULEA
Information security specialist, Bucharest, Romania
costi.gonciulea@yahoo.com.

In the digital era, words have a significant influence on how cyber threats are defined and perceived. This article examines the impact of framing phishing and other cybercrimes as „cyberattacks" on user responses and the legal and security mechanisms triggered. Confusing these concepts may discourage reporting incidents to authorities, leading users to delete messages and destroy evidence, which allows criminals to continue undisturbed. The study emphasizes the need for a clear distinction between cyberattacks, which threaten national security, and common cybercrimes, to ensure appropriate responses and effective protection measures. Moreover, this article seeks to clarify the essential differences between cyberattacks and cybercrime, highlighting their legal and strategic implications. Through a comparative analysis and a review of recent legislation, the study underscores the challenges and opportunities in managing these complex and dynamic threats.

Keywords: *Cyberattacks, Cybercrime, Computer fraud, National security, Cyber legislation, Cyber warfare, Computer offense, Phishing, Cybersecurity, Authorities, Digital era.*
DOI: 10.24818/issn14531305/29.3.2025.06

1 Introduction

The increasing global interconnectedness and reliance on cyber infrastructures have complicated the typology of threats to both national and individual security. While cyberattacks and cybercrime are frequently conflated due to their technical nature, they are distinct. These differences must be clarified from the perspectives of legislation, defense mechanisms, and the resources involved.

Technological advancements and the growing dependence on digital infrastructures have introduced new risks. In media and professional debates, computer crimes are often confused with cyberattacks. Although both involve technology, they fundamentally differ in nature, purpose, and legal and strategic consequences.

In the cyber era, how cyber threats are defined and communicated has a direct impact on user actions and the legal mechanisms triggered. Defining *phishing* and other cybercrimes as „cyberattacks" can influence how users respond to and report them. As a result, instead of treating *phishing* as mere fraud, the current approach discourages households and companies from reporting incidents to the proper authorities. Typically, they choose to delete messages, destroying evidence and allowing criminals to continue their illegal activities undisturbed. This pattern highlights the direct influence of the language used in the cyber domain on the effectiveness of responses. Therefore, a clear distinction between distinct types of threats becomes essential, acknowledging that metaphors in the cyber domain are indispensable.

Cyberattacks are deliberate actions, usually orchestrated by states or organizations/entities aiming to destabilize or compromise critical or nationally significant infrastructures, such as defense systems or energy networks. Conversely, cybercrime targets financial gains or personal advantages through deception, data theft, or fraud.

This study adopts established definitions of these concepts and provides a comparative summary analysis of how legislation addresses them and the specific response mechanisms. It also highlights who may benefit from the confusion between these categories and what consequences inappropriate classification may have.

The purpose of this study is to highlight the essential differences between cyber aggression and cybercrime, emphasizing their legal and strategic implications for national security, as well as the impact of misclassification – likely unintentional – of certain events on legal and strategic responses.

The premise of this material is that how we define and communicate cyber threats is not merely a semantic issue but one with real consequences for security and response effectiveness. This is especially crucial as internet users become increasingly younger and need to recognize and understand the situations they encounter. Terms like „cyberattack" or „attacker" have strong resonance, commonly associated with attacks on critical infrastructures, military operations, and national security. In contrast, *phishing* and other attempts at computer fraud should be perceived as less severe crimes that require different responses, such as reporting to the police.

The problem arises when these two types of threats are mixed under the „umbrella" of cyberattacks. Thus, it becomes necessary to determine to what extent, in public communication, including *phishing* in the same category as attacks on critical infrastructures may generate confusion, leading to a misunderstanding of the real severity of incidents. This confusion has a direct impact on user behavior, which might result in them not considering it necessary to report such incidents to the police.

2 Defining Terms

Clarifying the essential differences between cyberattacks and cybercrime, based on established definitions, can provide a reference framework for understanding the specific nature of each.

Firstly, a *cyberattack* is defined as a coordinated action, typically carried out by states or organizations with strategic interests, aimed at compromising, disrupting, or destroying critical infrastructures or other strategic assets. Such attacks are often part of broader campaigns of cyber warfare or cyber terrorism. Notable examples include attacks on energy grids, banking systems, or military networks. Cyberattacks are frequently considered acts of undeclared warfare and may be triggered during international conflicts.

Secondly, *computer fraud* involves the unauthorized use of computer systems to deceive victims with the purpose of obtaining financial benefits. Examples of such fraud include *phishing*, bank data compromise, identity forgery, or fund diversion through digital means.

Thirdly, *computer deception* involves misleading victims through information technologies without necessarily seeking immediate material gain. Examples include distributing *ransomware* to obtain ransoms or other forms of cyber manipulation leading to the acquisition of sensitive information.

Returning to the topic of this article, according to the National Cyber Security Directorate (DNSC), *phishing* involves misleading users to obtain sensitive information such as authentication, personal, or financial data. This definition practically associates *phishing* with both computer fraud and cyberattacks. [1]

3 Cyberattacks vs. Cyber Fraud

A. Legislative perspective

In Romanian legislation, there is a separation between cyberattacks and cyber fraud, although these concepts are not always clearly delineated in practical and legal terms. Applicable regulations address each of these categories with different approaches depending on the nature and severity of incidents. Below, we will explore relevant legislation, the distinctions between cyberattacks and cybercrime, and how they are investigated and/or sanctioned.

Cyberattacks - are considered threats to national security and are primarily regulated by laws addressing national and cyber security. In Romania, three key laws establish the regulatory framework for cyberattacks:

Law no. 58 of March 14, 2023

- ✓ Defines the legal and institutional framework for organizing and conducting activities in cybersecurity and cyber defense.
- ✓ Establishes mechanisms for cooperation and responsibilities of institutions in these domains.
- ✓ Introduces terms such as „cyber defense",

„cyberattack" and „cybersecurity incident".

Law no. 362/2018 (implementing the EU NIS Directive)

- ✓ Regulates the security of critical network and information systems.
- ✓ Mandates strict security measures for operators of essential services and digital service providers, requiring notification of cybersecurity incidents affecting critical infrastructure.
- ✓ Attacks on these infrastructures are considered national security threats and may trigger military responses or even be treated as cyber terrorism.

Law no. 51/1991 on Romania's national security

- ✓ Includes cyber threats in the scope of national security.
- ✓ Grants the Romanian Intelligence Service (SRI) the authority to intervene in cases endangering critical infrastructures and coordinates national responses to large-scale hostile cyber actions.

Under current legislation, cyberattacks are addressed as national security issues and are investigated by multiple national security authorities, including SRI, which can act in cases of compromised critical infrastructures or other strategic state assets.

Cyber fraud and cybercrime - these are distinctly regulated, mainly through the Romanian Penal Code, which defines and sanctions various cybercrimes. Specialized units of the Romanian Police investigate offenses such as unauthorized access to computer systems, data theft, or cyber fraud, based on the following legal framework:

Romanian Penal Code

- ✓ Article 249 defines cyber fraud as the „unauthorized introduction, modification, deletion of data, or restriction of access to such data for material gain".
- ✓ Article 244 defines deception as misleading a person by presenting false information as true to obtain advantages.
- ✓ Offenses like *phishing* or data theft are treated as forms of deception or cyber fraud.

Law no. 161/2003 on the prevention and combatting of cybercrime

- ✓ Regulates unauthorized access to computer systems and cyber fraud.
- ✓ Applies to *phishing* or other deceptive methods in the digital environment.

A particular nuance in these situations is that there is a specific legislative tool for sanctioning ***the attempt of fraud****, emphasizing that the offense is not conditioned by the occurrence of a material result. This legislative tool is the Penal Code, specifically Article 248, which is particularly relevant in the context of phishing. Through this article, the legislator aimed to highlight the essential condition that the existence of a concrete result, such as the actual theft of data or the obtaining of illicit gain, is not necessary for the attempt to be punished.*

Specifically, the offenders attempt to obtain sensitive data, such as the victims' banking information, by deceiving them, usually through the use of electronic correspondence addresses or fake websites. Even if the victim does not end up providing this data, the mere attempt to deceive them is enough for the provisions of Article 248 to apply. Therefore, *phishing*, per se, represents a deliberate attempt to deceive the victim, and Article 248 clarifies that „intention and deception" are the key elements for incrimination, not the actual realization of harm. This reflects a proactive approach in criminal law, aimed at preventing and deterring fraud attempts before they cause major damage, with the mandatory condition that these attempts must be reported to the Police.

In addition to national legislation, Romania is a signatory to the Budapest Convention on Cybercrime, which provides an international framework for investigating and combating cyber fraud. Furthermore, Directive 2013/40/EU on attacks against information systems, The General Data Protection Regulation (GDPR) strengthen laws on cybercrime and data protection. By combining national and international measures, Romania seeks to comprehensively address cyber threats and criminal activities in the digital sphere.

B. Phishing as a form of computer fraud

Although *phishing* is often associated with or categorized as a “cyberattack” we have demonstrated that Romanian legislation provides sufficient arguments to treat it as a form of computer fraud. Generally, *phishing* cannot be considered a cyber aggression that constitutes a direct threat to national security but should be classified under general computer crime. However, *phishing* can also serve as the initial step in a more complex cyberattack, such as an Advanced Persistent Threat (APT), where the data obtained through *phishing* is used to compromise a larger IT system.

As such, *phishing* should be appropriately managed by the specialized units of the national police based on the explicit provisions of the Penal Code and Law 161/2003, as well as in accordance with European and international regulations.

C. Analysis based on relevant studies

The fundamental difference lies in the fact that cyberattacks are frequently treated as military operations with consequences that impact national security or critical infrastructures. Thus, legislation tends to treat them as acts of aggression requiring a national security response. On the other hand, fraud or computer-related deception is more often seen as economic or personal crimes addressed through legal mechanisms and criminal investigations.

Significant research explores the differences between cyberattacks and computer crime, highlighting how legislation and cybersecurity specialists respond to these threats. Below are some relevant examples that support this differentiation:

I. Cyberattacks and national security

The study *„Cyber Warfare: A Multidisciplinary Analysis”* (2012) emphasizes that cyberattacks are often tools of warfare used by states, targeting critical infrastructures and having major strategic implications [2]. Similarly, the book *„The Fifth Domain”* (2019) offers a practical perspective on how states and large organizations defend themselves against cyber threats, stressing the need for adequate responses at national and international levels [3].

II. Legislation on computer crime

The Budapest Convention (2001) is a key document in combating computer crime, establishing the legal framework for international cooperation in this regard. It clearly defines terms associated with computer crime and regulates ways to address it [4]. Additionally, the study *„A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments”* highlights the complexity of defining and legally addressing cyberattacks. The lack of a clear and universally accepted definition of what constitutes a cyberattack complicates the application of existing laws and the development of effective legal frameworks. This ambiguity can lead to varied and sometimes contradictory interpretations in practice, undermining efforts to combat cybercrime. The study underscores the need for a comprehensive definition of cyberattacks to clarify legal responsibilities and facilitate the uniform application of the law. Without such a definition, there is a risk that legal efforts will be ineffective, allowing cybercriminals to exploit legislative gaps and increase their gains [5].

III. The distinction between cyberattacks and computer crime

The article *„A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments”* (2021) differentiates between cyberattacks and computer crime. While cyberattacks are often initiated by states, computer crimes are usually committed by individuals or groups with financial motivations [5].

Additionally, another study from 2020 highlights the difficulty of accurately attributing a cyberattack, which complicates the distinction between state-sponsored attacks and computer crimes [6].

IV. Specialists' capacity to respond to incidents

Research into the skills required for specialists to respond to cyber incidents reveals significant differences in how cyberattacks and computer crimes are managed. For instance, the study *„Skills, Capabilities, and the Impact of Training in Cybersecurity"* (2020) emphasizes that professional training and specialized education are essential for correctly triggering response measures based on the type of incident [7].

At the same time, coordination between agencies and the importance of continuous training are discussed in numerous articles. A relevant example is the collection of studies compiled in the work *„Cyber Warfare and Cyber Terrorism"* [8].

V. Case studies

The 2007 cyberattacks on Estonia and the Stuxnet incident have led to notable case studies illustrating the differences between cyberattacks and computer crime. While the attacks on Estonia are considered the first major cyberattack against a NATO member state, Stuxnet is a classic example of a state-sponsored cyberattack targeting critical infrastructures.

Several papers and case studies analyze these incidents and underscore the fundamental differences between cyberattacks, which generally have a strategic or state-sponsored component, and computer crime, which more frequently involves criminal groups or individuals with financial motivations:

- The book *„Cyber War and Cyber Terrorism"* provides a comprehensive analysis of the differences between cyber warfare, cyber terrorism, and computer crime. Among other aspects, the authors highlight the fundamental differences in the objectives and techniques used in each type of attack [8].
- The paper *„Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack"* focuses on the Stuxnet case as an example of a state-sponsored attack. It emphasizes the risks of cyber warfare and its impact on national security and critical infrastructure. The author discusses the use of sophisticated malware as a method of industrial sabotage, which sets Stuxnet apart from traditional cyberattacks [9].
- The study *„An Examination of Estonia 2007 Cyber Attacks and the Effects on National Cyber Security Policies of Countries"* analyzes the 2007 attacks on Estonia, highlighting their nature as a national-level cyberattack. It points to the need for developing global cybersecurity policies, coordinated strategies, and a more effective international response to cyber threats [10].

VI. Phishing as part of a cyberattack

Phishing becomes part of a cyberattack when it is used in a chain of coordinated actions aimed at compromising critical infrastructures or strategic assets. In such scenarios, *phishing* is often the initial step, employed to gain initial access before launching more complex attacks, such as deploying *malware* or *ransomware*.

Example: Advanced Persistent Threat (APT) attacks orchestrated by groups such as APT28, where *phishing* was used to access government officials' email accounts and collect sensitive data [11].

The international, european, and national legislative frameworks provide clear regulations for addressing computer fraud and cyberattacks. However, the lack of distinction between *phishing* and cyberattacks, perpetuated in practice by Romanian national authorities, may result in the omission of reporting incidents. Therefore, a clear differentiation between these types of threats is essential to trigger the appropriate legal mechanisms and effectively protect users.

4 Diversion of Meaning and Purpose

Phishing and deception are closely related by their nature as acts of fraud and manipulation, each with specific characteristics depending on the context in which they occur [12].

Deception, at its core, is an act of misleading to distort perception of reality. It can manifest through false promises, distortion of truth, or manipulation of emotions and trust. Thus, *phishing* is a modern form of deception based on social engineering techniques, exploiting users' trust and negligence to obtain sensitive information such as passwords, banking details, or other personal data.

In the physical space, deception often occurs through *traditional means*, such as verbal persuasion, document falsification, or scenarios creating a false sense of security, relying on convincing the victim that the presented actions or information are real and authentic. In the digital space, *phishing* uses *digital tools* like emails, fake websites, text messages, or other electronic channels designed to appear legitimate, misleading the victim into disclosing personal information [13] [14].

While in the physical realm, *the goal* of deception is to manipulate the victim's perception, potentially leading to material, emotional, or intellectual losses, the primary purpose of *phishing* in the digital domain is the unauthorized collection of confidential information. Although it is a form of fraud, *phishing* focuses on stealing digital data or gaining unauthorized access to accounts or financial resources [15].

At the same time, *the ultimate goal* of deception in both domains is to obtain personal or material advantages, exploiting weaknesses.

Given this essential aspect of *phishing*, it becomes evident that this form of fraud and cyberattacks are distinct concepts, although they may be interconnected in certain situations. Key characteristics that differentiate cyberattacks from *phishing* include [8]:

- *Objectives*: Obtaining sensitive information or access to resources for destruction, disruption, unauthorized access, sabotage, or digital espionage on systems, networks, or infrastructures.
- *Methods*: Use of advanced tools, malware, exploitation of software vulnerabilities, or distributed attacks like DDoS.
- *Complexity*: Requiring deep technical knowledge, financial resources, and sometimes coordination between multiple entities.
- *Entities involved*: Organized criminal groups, nation-states, or entities with significant resources, including political, economic, or military motivations.
- *Impact*: Massive financial losses, compromise of critical infrastructures, or destruction of organizational data.
- *Legal and legislative consequences*: Acts of cyber warfare, espionage, or digital terrorism with complex political and legal implications.

In conclusion, *phishing* is a specific example of a threat based on social engineering, while cyberattacks represent a much broader and more diverse category of hostile actions that often involve advanced technologies and extensive coordination.

To provide a clear understanding of how confusion between *phishing* and cyberattacks is perpetuated in public and professional spaces, here are concrete examples from official documents and guides from authorities and the private sector:

Example 1: Articles on the DNSC (National Cybersecurity Directorate) website [16] about *phishing* campaigns label these actions as “cyberattacks” without distinguishing between computer fraud and attacks compromising critical infrastructures. The term “cyberattack” is used generically, potentially creating confusion for regular users.

Example 2: Guides [17] for home users and small businesses present *phishing* as a “cyberattack” that can affect personal and financial safety. While preventive measures are encouraged, there is no mention that *phishing* is a distinct form of computer fraud requiring specific legal actions.

Example 3: Bitdefender [18] uses the term “cyberattack” in its warning and protection materials against *phishing*. *Phishing* is treated as a typical cyberattack, often "packaged" with malware or ransomware. While the protection tips are helpful, the terminological confusion can affect clarity regarding the responsibilities of users and authorities.

Example 4: In Kaspersky Lab's security guides [19], *phishing* is frequently referred to as a “cyberattack” in sections on threat prevention. This can confuse users, who may not realize that *phishing* constitutes computer fraud requiring police reporting.

This confusion between *phishing* and major cyberattacks is perpetuated by public and private institutions through the generalized use of the term “cyberattack” for any malicious digital activity. This term, as defined in Law No. 58 of March 14, 2023, refers to hostile actions conducted in cyberspace that disrupt normalcy achieved through proactive and reactive measures ensuring the confidentiality, integrity, availability, authenticity, and non-repudiation of electronic information in public or private cyber resources and services. As previously mentioned, this approach may discourage users from reporting *phishing* attempts to the police, assuming it is neither necessary nor effective. Instead of clarifying *phishing* as computer fraud requiring specific legal actions, this confusion exacerbates the problem, allowing perpetrators to continue and expand their activities unimpeded.

Nevertheless, in a glossary of terms [20] compiled by the Romanian Intelligence Service and a guide [21] from the same authority, *phishing* is associated with criminal activity and linked to an offender. The methods related to *phishing*, such as spear *phishing*, vishing, and smishing, are attributed to an attack or attacker. This implies the existence of a criminal behind these methods, although the term *„cyberattacker”* is not clarified anywhere in Romanian legislation.

Let us assume that it would not be necessary to define the term *„cyber attacker”* and that it would be sufficient to state that the attacker is any person who carries out a cyber attack. In this case, we must revisit the definition of a cyber attack – a hostile action carried out in cyberspace, likely to affect the state of normality resulting from the application of a set of proactive and reactive measures ensuring the confidentiality, integrity, availability, authenticity, and non-repudiation of electronic information in public or private resources and services within cyberspace. In order to understand this definition and assess its applicability and to whom it applies, we must also clarify what is meant by public or private services in cyberspace. In the context where there is no clear definition of these, I believe we should refer to the normative acts related to the field of cybersecurity, previously mentioned (Law no. 362/2018 and Law no. 58/2023), which establish sectors of activity and types of entities, providers of essential services, such as *operators, authorities, carriers, companies,* etc. Therefore, from this list of terms, citizens are deliberately or accidentally excluded from the legislation, from which we can infer that the authorities' messages do not target them, meaning there is no responsibility on the part of either the citizens or the authorities in ensuring or protecting their interests in the digital environment.

However, Article 40 of Law no. 58 of 2023 establishes responsibilities for DNSC and authorities in defense, public order, and national security to issue notifications to raise citizens' *awareness* about the need to report cyberattacks and develop a national framework for public awareness in cooperation with public, private, and academic sectors.

These normative inconsistencies regulate the obligation to notify security incidents, yet this obligation does not extend to citizens, nor are there reporting tools or guidance available. These inconsistencies are certainly amplified by classifying *phishing* attempts as cyberattacks.

5 Shifting the Focus from Fundamental to Accessory

The classification of *phishing* attempts as cyberattacks represents a significant issue in the current approach to cybersecurity, especially in terms of shifting the focus from the fundamental to the accessory. In practice, misinterpreting the primary distinctions between *phishing* and cyberattacks leads to the application of erroneous or inadequately calibrated mechanisms, raising critical issues at both strategic and operational levels.

Conceptual and terminological confusion

Phishing has been shown to be a form of computer fraud, designed to deceive users into providing sensitive information (passwords, financial data, etc.). Essentially, it is a type of computer crime involving fraud, without necessarily compromising critical IT systems or targeting infrastructure of national importance. By categorizing *phishing* as a cyberattack, authorities contribute to conceptual confusion between large-scale cyberattacks and individual fraud attempts. *This approach dilutes the correct understanding of what constitutes a real cyberattack, shifting the focus from fundamental risks to incidents with limited impact*.

Inadequate resource allocation

Another consequence of this shift is the risk of misallocating resources. Instead of focusing institutional attention and resources on protecting critical infrastructures and combating state-sponsored attacks, this approach broadens the scope to include minor incidents such as *phishing* attempts. At the same time, the role of citizens in this process, particularly in reporting *phishing* attempts, is paradoxically overlooked. Misclassifying *phishing* as a cyberattack risks wasting resources and public attention on less urgent issues, potentially affecting the ability to respond quickly and effectively to genuinely critical attacks.

Discouraging accurate reporting

Another effect of this misclassification is that internet users may become confused about how to properly report *phishing* incidents. Labeling *phishing* as a cyberattack may lead users to believe that such incidents must and will be handled exclusively by institutions such as DNSC or SRI. However, *phishing* should be reported directly to the Romanian Police, as it is a form of fraud. Additionally, the Police should coordinate with other national authorities responsible for cybersecurity and cyber defense, such as the Ministry of National Defense. The lack of a clear distinction between *phishing* and actual cyberattacks can result in underreporting of incidents or their misdirection to institutions that are not competent to handle such cases. Furthermore, underreporting directly impacts the allocation of human and logistical resources within the Police, which in turn benefits entities or individuals using *phishing*.

Failing to differentiate phishing from cyberattacks at a conceptual, operational, and institutional level not only undermines the correct handling of these incidents but also creates inefficiencies in resource management and public understanding. It is essential to address these distinctions to improve the strategic and operational responses to both phishing and genuine cyberattacks.

6 Contamination through Exposure

An additional dimension of the issue surrounding the classification of *phishing* as a cyberattack is contamination through exposure. In this context, the term refers to the influence cybersecurity professionals – both in the public and private sectors – experience from messages disseminated by authorities or other entities involved in cybersecurity (commercial enterprises, professional associations, educational and academic environments, etc.). These professionals, in turn, adopt and propagate this conceptual confusion in their interactions with users, companies, and/or clients.

Transmission of confusion through communication chains

Cybersecurity professionals, whether in the private or public sector, typically rely on guidance from authorities to understand and communicate the nature of cyber threats. When authorities issue warnings that include *phishing* under the broad term “cyberattack” this message becomes the professional standard for many specialists. As a result, they not only accept this classification uncritically but also further disseminate this confusion through their own communication channels.

This “contamination” has two major effects:

Systemic confusion: Professionals adopt and relay messages from authorities within their own organizations, potentially leading to a generalized misunderstanding of the difference between computer fraud and a cyberattack. This shifts the focus to minor threats, while attacks involving critical infrastructures or national security may be deprioritized.

Fragmentation of response measures: Treating *phishing* as a cyberattack on par with targeted attacks against institutions or critical infrastructures can dilute security measures and resources, making it harder to concentrate on real, strategically significant attacks. Instead of providing precise, targeted solutions for each type of incident, professionals tend to generalize their approaches, creating an inadequate framework for responding to truly severe threats.

<u>Impact on companies and end users</u>

This contamination through exposure has direct consequences for companies and end users, who rely on professionals for guidance in navigating the complex landscape of cyber threats. If specialists perpetuate the confusion between *phishing* and genuine cyberattacks, companies may allocate disproportionate resources to combating threats that, while important, do not pose critical risks to infrastructure security.

On the other hand, individual users may become either excessively alarmed or desensitized, believing that all *phishing* attempts are major cyberattacks. This can lead to a reactive and chaotic approach to security incidents, either through unnecessary reporting to national security authorities or by disregarding the importance of reporting *phishing* as fraud to the Romanian Police.

<u>The need for clear and coherent messaging</u>

To avoid such contamination and prevent the perpetuation of confusion, it is essential for authorities to revise their communication strategies. They must provide clear and coherent messages that reflect the distinct realities of computer fraud and large-scale cyberattacks. Only by correctly differentiating these threats can a conceptual, organizational, and operational framework be created in which protective and response measures are appropriately adapted to real risks.

Additionally, industry professionals must adopt a critical role, characterized by skepticism, in verifying and disseminating accurate information. This includes prioritizing the proper education of target groups and delivering messages that clearly distinguish between different types of cyber threats. A joint effort between authorities and experts is necessary to prevent the perpetuation of confusion that diverts attention and resources from true risks and vulnerabilities. Such confusion is currently being transmitted even in schools, affecting the youngest and most vulnerable users.

7 The Risk of Lack of Response and Its Impact on Security Mechanisms

Given the distinct nature and different manifestations of cyberattacks and computer crime, the responses they generate must also differ depending on the nature and impact of the incident. These differences should drive the mobilization of diverse resources and competencies essential for effectively addressing each type of threat.

Cyberattacks

Cyber defense actions: Cyberattacks targeting critical infrastructures or states can trigger defense actions at national and international levels. Within NATO, a significant cyberattack on a member state could activate Article 5, equating the attack to an act of war or cyber terrorism [3].

Identifying the attack's origin: Specialists must quickly determine the source of the attack, whether it originates from a state, entity, or terrorist organization. This step is crucial to differentiate a military attack from one generated by criminal groups [2].

Evaluating objectives: Understanding the purpose of the attack is essential. Attacks targeting critical infrastructures, such as energy or water networks, require rapid intervention from armed forces or national security agencies [4].

National and international response: Specialists must communicate swiftly with national and international authorities (NATO, EU) to coordinate responses to large-scale cyberattacks. Cooperation is especially crucial in the case of cross-border attacks [3].

Cyber counterattacks: In some situations, a state may respond with a defensive or offensive cyberattack. Specialists must evaluate the legality and strategic implications of such decisions [22].

Key Issues:

- What criteria indicate the manifestation of a cyberattack?
- How and where are data correlated?
- Which authorities are competent?
- Who are the specialists, and what training should they have?
- Which complementary or external fields to cybersecurity need to be involved in the decision-making chain?

Computer crime (fraud and deception)

Criminal investigations: Computer crimes are handled by law enforcement agencies through criminal investigations. These do not involve mobilizing national defense forces but focus on identifying perpetrators and recovering damages [4].

Incident investigation: Specialists collaborate with the police to analyze the nature of the fraud, how it was committed, and to initiate an investigation. This is a common response to financial fraud or scams [22].

Damage recovery: In financial fraud cases, specialists work to identify patterns and anomalies in financial transactions, leading to recovery efforts and cooperation mechanisms between financial institutions [23].

Improving security: After an incident, prevention measures become a priority, including strengthening security systems and educating users about existing threats [7].

Key Issues:

- ✓ Which terms or phrases hold users accountable or make them aware of an attack or fraud?
- ✓ Are „attack" and „attacker" more associated with military contexts or civil society?

One of the most serious consequences of defining *phishing* as a cyberattack is that regular users may become confused about the appropriate actions to take. Instead of reporting *phishing* incidents to authorities, they might simply delete the message, believing that filing a complaint is unnecessary – something authorities have often encouraged. This leads to the destruction of evidence, complicating the prosecution of criminals and allowing them to continue and expand their activities without restrictions.

Phishing is not merely an isolated attempt at fraud; it is often part of a broader campaign targeting multiple victims simultaneously. Every *phishing* attempt reported could provide valuable information to authorities, helping to identify the criminal groups involved. However, if users do not file complaints, perpetrators will continue sending *phishing* messages until they successfully obtain financial benefits illegally.

Treating *phishing* as a major cyberattack risks failing to activate the appropriate legal and security mechanisms. While *phishing* is essentially a form of computer fraud and should be investigated by the police, targeted users or victims may believe it to be a cyberattack requiring management by government cybersecurity agencies. This misconception could lead to a lack of formal complaints to the police, resulting in underreporting of computer crimes and a lack of evidence needed to track and stop criminals.

Coordination between authorities may be disrupted. Normally, *phishing* is managed by the police and other law enforcement institutions. However, if *phishing* is seen as a cyberattack, other agencies might become unnecessarily involved, leading to overlapping competencies and delays in investigating incidents.

Classifying minor computer crimes as "cyberattacks" may unnecessarily escalate situations, leading to disproportionate responses. Conversely, underestimating a real cyberattack could compromise national security.

Advantages of correct classification - By treating incidents according to their actual nature (military versus criminal), appropriate, efficient, and proportional responses can be ensured.

Disadvantages of incorrect classification - Misclassification can lead to excessive security measures or, conversely, neglect of a real threat.

Malicious entities exploit the lack of clarity in defining and handling these cases. For example, treating a military cyberattack as mere fraud can reduce the state's response capacity, leaving vulnerabilities exploitable. Conversely, labeling an economic fraud as a “cyberattack” can provide individuals with undue strategic advantages.

Correct classification and communication are crucial to ensuring a coherent, effective, and secure cybersecurity framework.

8 Decision Models

Incorrect initial information, such as the confusion between phishing and cyberattacks, can have a significant impact on the decision-making process. Cognitive *biases*, decision theory, emotions, and trust in authorities influence the misreporting, insufficient reporting, or failure to report these incidents to the authorities. Therefore, a clear understanding of the nature of *phishing* and how it can affect individual and collective security is essential for an adequate and effective response.

The system of standards and rules regarding cyberspace that governs human behavior and is universally applicable, regardless of individual opinions, is primarily outlined by technical experts, thus being based in reality. This leads to an excessively technological attitude, overlooking the inappropriate effects that this approach may have.

In this context, users have learned to perceive “cyberattacks” as sophisticated, large-scale malicious actions targeting critical infrastructures. This initial belief influences how they perceive other types of incidents.

Thus, when users encounter a *phishing* message, influenced by the authorities' messages describing the activity as a cyberattack, they update their beliefs and perceive that they are subjected to a major cyberattack. As a result of receiving these messages and updating their perception, users will treat *phishing* attempts as complex attacks, leading to inadequate decisions (for example, failure to report to the police or competent authorities). In this process, the misconception is amplified by the expert community that adopts the authorities' confusing message.

Conceptual contamination does not stop with regular users. Another effect is contamination through exposure, a phenomenon whereby specialists adopt the authorities' messages and pass them on without critical reassessment. Thus, companies and cybersecurity experts (including those in the private sector) adopt and perpetuate the ambiguous messages transmitted by the authorities. Bitdefender, for example, classifies *phishing* as a cyberattack in its security guides for the general public, further reinforcing this confusion. [24]

Thus, contamination through exposure becomes a phenomenon that complicates not only users' understanding but also professionals' responses to these threats. This “spiral of collective confusion” undermines the effectiveness of measures to prevent cyberattacks and cyber fraud.

Applying established decision-making models in this context helps explain how confusion spreads within the community and how a misperception of *phishing* can affect individual and collective decisions. The misclassification perpetuated by authorities and experts leads to inappropriate actions in response to real threats, which often remain unreported or are treated superficially.

8.1. Cognitive errors: confirmation bias and anchoring bias

Cognitive errors: Cognitive biases, such as confirmation bias and anchoring bias, suggest that incorrect initial information can distort the decision-making process. In the case of *phishing*, citizens/users who have a mistaken understanding of this threat may seek evidence that confirms that incorrect perception, ignoring the evidentiary elements that could help in making a correct assessment.

Confirmation and anchoring *biases* directly influence the way people process information and integrate it into their own evaluations. If the initial information is incorrect, these errors can perpetuate a mistaken judgment in the long term, leading to misreporting or insufficient reporting.

Relevant study: Judgment under Uncertainty: Heuristics and Biases (1974) [25].

8.2. Decision theory and the impact of initial errors

Decision Theory: In the decision-making process, citizens/users use subjective probabilities to assess risks and make decisions. If they perceive *phishing* as a cyberattack (rather than a fraud attempt), this will distort their risk assessment and affect their decision to report the incident to the authorities.

Incorrect initial information can affect the decision-making reasoning of citizens, leading to incorrect decisions regarding the reporting of attacks to the authorities.

Relevant study: Advances in Prospect Theory: Cumulative Representation of Uncertainty (1992) [26].

8.3. Affective decision model and emotional impact

Affective Decision Model: Emotions and perceptions influence the decision-making process, and citizens who are not properly educated about the nature of *phishing* may be less motivated to report the incident, considering it a technical issue beyond their understanding, one they are certain the authorities already know about. This becomes a situation of underestimation or overestimation, leading to insufficient, incorrect, or even non-reporting.

In this case, incorrect or insufficient initial information can create a low emotional reaction to *phishing*, which reduces the likelihood of considering it a serious fraud and reporting it properly to the authorities.

Relevant study: The Role of Emotion in Decision-Making (2003) [27].

8.4. Trust theory and confidence in authorities

Trust Theory: suggests that, for citizens/users to report *phishing* incidents correctly to the authorities, they must trust them. If the perception of *phishing* is incorrect (i.e., they consider it a cyberattack rather than fraud), trust in the importance of reporting may decrease significantly.

People who do not understand the seriousness of *phishing* attempts may be less motivated to report this type of fraud, undermining the effectiveness of fraud prevention measures and cybersecurity.

Relevant study: Trust: Making and Breaking Cooperative Relations (2008) [28].

The propagation of confusion – whether through incorrect initial information or the contamination of professional and public perceptions – has profound implications for decision-making in cybersecurity. Recognizing and addressing these cognitive and emotional factors, alongside providing clear and accurate information about threats, is essential to improve incident reporting and overall security.

9 Recommendations for a Clear and Differentiated Approach

To avoid confusion and ensure an adequate response to each type of cyber threat, it is essential for cybersecurity entities (both public and private) to clearly communicate the differences between major cyberattacks and ordinary computer crimes. Below are several measures that can be implemented to improve this situation:

Clarification of terminology: It is important that *phishing* and other attempts at cyber fraud be correctly defined as cybercrimes, distinct from cyberattacks targeting critical infrastructures or national security. This will help users better understand what actions they need to take and their relevance in the communication chain.

Public education: Awareness campaigns must explain to users the importance of reporting *phishing* attempts and other cyberfraud to the police, regardless of their possible assumptions. Personal beliefs are not relevant; rather, it is about activating a reporting chain where they are the first, and most important, element. Furthermore, users must be informed that competent authorities can intervene and prevent future fraud attempts only if they receive complaints and reports.

Improving the reporting process: Institutions should facilitate the process of reporting phishing attempts so that users can file complaints in a simple and fast manner, through an online system directly on platforms managed by the police through the responsible components. This would encourage more reports and help collect valuable data for investigating and combating the phenomenon.

The power of words in the cyber era cannot be underestimated. The way we define cyber threats directly influences users' actions and the response of competent institutions.

Let us not forget that *phishing* can be part of a cyberattack when it is part of a broader strategy aimed at compromising critical infrastructures, government systems, or other strategic assets, for example as part of coordinated attacks, such as those of the Advanced Persistent Threat (APT) type. However, this is transparent to the user and does not change the correct reporting attitude.

Organizations such as Europol, ENISA, or NIST emphasize that *phishing* is not always a cyberattack. It is defined as cyber fraud, except in cases where it is part of a coordinated attack against critical infrastructures. *Examples include:*

- Europol: In its reports, Europol classifies *phishing* as computer fraud but notes its potential role in larger cyberattacks [29].
- ENISA: Treats *phishing* as an isolated fraud in most cases but explains its use in complex cyberattacks [30].
- NIST: Clearly distinguishes between *phishing* as fraud and *phishing* as a social engineering method in cyberattacks [31].

By adopting these recommendations, authorities and cybersecurity entities can improve user understanding, streamline response mechanisms, and enhance the overall effectiveness of cybercrime prevention and mitigation. Clear communication, targeted education, and accessible reporting systems are essential to building a secure and resilient digital environment.

10 Training Response and Reaction Capacity

An essential component in ensuring cybersecurity at the national level is the proper training of specialists who must distinguish between situations and classify them correctly. This involves training both public and private sector professionals. Specialists must possess technical skills, but they also need to be able to properly manage different types of cyber incidents, from sophisticated state-sponsored attacks to cybercrimes like *phishing*. Additionally, an important role is played by the police officers who receive reports from users, companies, or institutions, as they are the first point of contact for reporting cyber incidents. At the same time, effective cyber incident management training involves not only the police and other responsible institutions but also the end users. This integrated approach is essential to reduce risks and ensure a coordinated response to any cyber incident. Moreover, communication through dedicated channels is crucial, and the language must be recalibrated to correctly express the factual reality while being adapted to the users' ability to understand, regardless of age, education, or occupation.

A. Training specialists in public and private sectors

Training cybersecurity specialists in both the public and private sectors requires a comprehensive approach that includes practical exercises and simulations of real scenarios. A 2020 study, *"Skills, Capabilities, and the Impact of Training in Cybersecurity"* highlights the importance of continuous training for security experts, showing that only through simulations and constant drills can they effectively respond to complex and emerging attacks [7].

For example, training for responding to attacks on critical infrastructures, such as those in energy or telecommunications, requires advanced knowledge of how these systems operate and the attack tactics used by state entities or organized criminal groups. On the other hand, combating cybercrimes, such as *phishing* or online fraud, requires skills related to investigating financial crime and cyber deception.

B. Importance of simulations and cyber exercises

In order to respond adequately to cyber incidents, simulations and practical exercises play a crucial role in preparing specialists. These simulations provide an opportunity to practice rapid and coordinated responses to complex attacks. According to a study conducted by Dewar R. (2018), cyber simulations are essential for testing and improving collaboration between agencies and institutions [32].

A well-known example is the 2007 cyberattack in Estonia, which highlighted the importance of prior preparation. The massive DDoS attacks on the country's digital infrastructure forced the government to reassess and improve its cybersecurity capabilities, including by organizing exercises and simulations at the national level [10].

C. Challenges of attribution and competence limits

One of the biggest challenges for cybersecurity specialists remains the correct attribution of an incident. According to *"Cyber Attribution: Technical and Legal Approaches and Challenges"* (2020), accurately identifying the source of a threat/attack is often complicated by the tactics used to conceal the identity [6].

This is a major issue within the institutions that handle cyber incidents, as incorrect attribution can trigger inappropriate measures, escalating minor incidents or neglecting major threats. For example, a state-sponsored attack may require the involvement of the Romanian Intelligence Service (SRI) or the Ministry of National Defense (MApN), while a cybercrime such as phishing should be managed by the Romanian Police and the Directorate for Combating Organized Crime.

D. Training law enforcement in incident reporting

In addition to the technical training of cybersecurity specialists, it is essential that police officers who receive reports from users, companies, or institutions are well-prepared. They represent the first point of contact in the case of cyber incidents, and their ability to understand the nature and severity of the incident is crucial.

It is obvious that, during their training, police officers must be instructed to differentiate between various types of incidents, from cybercrimes to sophisticated cyberattacks, based on the idea that a lack of preparation in this field can lead to incorrect classifications and inefficient allocation of resources.

E. Coordination and competence transfer

The training of specialists is also linked to coordination between agencies. The lack of a coherent framework for collaboration between authorities and responsible institutions can lead to delays in responding to incidents or overlapping areas of responsibility. For example, according to *"A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments"* (2021), this type of coordination is essential for the effectiveness in combating cybercrime [5].

The proper transfer of responsibilities between national and international agencies is also a major challenge. In the European Union, member states have implemented various frameworks for collaboration, but challenges remain in their consistent application. In Romania, the overlap/conceptual confusion between cyberattacks and cybercrime can be amplified by the lack of a clear delineation of responsibilities.

F. Role of end users in building reaction capacity

An important component in increasing the response capacity to cyber frauds/cyberattacks is the end users. They are often the first to be affected by crimes such as *phishing*, but they can also play an active role in protecting digital infrastructures by quickly reporting incidents.

End users must be trained to recognize and report attempts, especially as their age decreases. Better education and involvement in cybersecurity processes can improve the speed and efficiency of the overall response. Additionally, they can be actively involved in cyber exercises or simulations, providing them the opportunity to learn how to handle different or crisis situations and how to avoid common traps such as *phishing*.

An example is the study *"An Examination of Estonia 2007 Cyber Attacks and the Effects on National Cyber Security Policies of Countries"* which highlights that well-informed and educated end users become a crucial part of the response process to large-scale cyberattacks. This study emphasizes the importance of the active involvement of everyone using digital infrastructure, not just specialists, as well as the component of international cooperation and cyber diplomacy. [10]

Training the response capacity to cyberattacks must include not only specialists and the police but also end users, who are the first to be affected by cybercrimes. Proper education and involvement of end users, along with constant training of specialists and efficient coordination between institutions, can ensure strong defense against cyber threats. Joint exercises and simulations, along with continuous training of the police in handling and managing reports, will significantly contribute to improving the national response to cyber incidents.

11 Conclusions

Inadequate communication from authorities, lack of cybersecurity education, and unclear public policies perpetuate the confusion between *phishing* and cyberattacks, directly reducing the ability to effectively counter and combat crimes.

Authorities have frequently issued recommendations to delete suspicious phishing messages in order to protect users from risks. However, this approach has negative consequences, as it: destroys essential evidence for criminal investigations, hinders the identification of criminals, eliminates or diminishes evidence for investigations, encourages offenders, and erodes trust in authorities.

To effectively combat *phishing*, users should be encouraged to report incidents, preserve, and provide evidence. Authorities must clarify the importance of reporting *phishing* to the police and offer clear guidelines to maximize the chances of success in investigations.

Classifying *phishing* as a cyberattack creates confusion among users, leading them to not report incidents and to destroy essential evidence. A more balanced approach that distinguishes between cyberattacks and ordinary computer fraud would encourage reporting and facilitate better coordination between responsible institutions. This way, the spread of criminal activities could be prevented, and adequate responses could be ensured for each type of cyber threat.

Furthermore, bringing *phishing* under the "umbrella" of cyberattacks shifts the focus from fundamental threats to national security to the accessory aspects of computer crime. This approach dilutes the correct understanding of cyber risks and contributes to inefficient allocation and scaling of resources (human, material, logistical), discouraging proper reporting of *phishing* incidents to the competent authorities.

Classifying *phishing* as a cyberattack by authorities not only shifts the focus from fundamental threats but also contributes to contaminating and misdirecting the messages transmitted by specialists to companies and users. Moreover, as digital services and resources are used from an increasingly younger age, training efforts face the difficulty of misused terminology, leading to a distorted understanding of concepts and a deviation from the original protective and educational goals. This propagation of confusion risks undermining national cybersecurity efforts, generating inadequate responses, improper resource allocation, and ultimately exposing users to increased risks.

Cyberattacks and computer crime trigger distinct response mechanisms, highlighting the need for specialists well-trained in specific areas. Cyberattacks that threaten national security require a coordinated response between security agencies and military forces, while computer frauds are addressed through criminal investigations and damage recovery, with citizens playing a vital role. It is crucial that the national cybersecurity strategy makes clear distinctions between the different types of threats, focusing resources and attention on them according to their specific characteristics.

References

[1] DNSC, "Ghid de protejare și recuperare conturi social media". Available: https://dnsc.ro/vezi/document/dnsc-ghid-retele-sociale-ro

[2] R. L. Deibert, J. G. Palfrey, R. Rohozinski, and J. Zittrain, "Cyber Warfare: A Multidisciplinary Analysis", in Routledge, 2012.

[3] R. A. Clarke and R. K. Knake, "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats", in Penguin Press, 2019.

[4] Council of Europe, "Convention on Cybercrime", Budapest Convention, 2001.

[5] L. Yuchong , L. Qinghui, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", in Energy Reports, Volume 7, Pages 8176-8186, 2021. Available: https://doi.org/10.1016/j.egyr.2021.08.126

[6] N. Tsagourias, M. Farrell,"Cyber Attribution: Technical and Legal Approaches and Challenges", in European Journal of International Law, Volume 31, Issue 3, August 2020, Pages 941–967. Available: https://doi.org/10.1093/ejil/chaa057

[7] L. Roberts, "Skills, Capabilities, and the Impact of Training in Cybersecurity", in Journal of Information Security, vol. 10, 2020, pp. 78-92.

[8] L. J. Janczewski, A. M. Colarik, „Cyber Warfare and Cyber Terrorism", in Information Science Reference, Hershey, 2008.

[9] R. L. Lendvay, "Shadows of Stuxnet: recommendations for U.S. policy on critical infrastructure cyber defense derived from the Stuxnet attack", California, Naval Postgraduate School, 2016.

[10] E. Dilek, Ö. Talih, T. Kaya Bensghir, "An Examination of Estonia 2007 Cyber Attacks and the Effects on National Cyber Security Policies of Countries", in Information Management Journal, Ankara University Information Management Systems Documentation and Information Security Center, 2023, pages 332 – 347. Available: https://doi.org/10.33721/by.1392577

[11] FireEye Threat Intelligence, "APT28: A Window into Russia's Cyber Espionage Operations?", 2014.

[12] K. D. Mitnick, W. L. Simon, „The Art of Deception: Controlling the Human Element of Security", Wiley, 2011.

[13] R. B. Cialdini, „Influence: The Psychology of Persuasion", in Harper Business, 2006.

[14] M. Jakobsson, S. Myers, „Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Wiley, 2007.

[15] S. Grazioli, S. L. Jarvenpaa, „Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers", IEEE Transactions on Systems, Man, and Cybernetics, 2000. Available: https://oz.stern.nyu.edu/seminar/fa02/Perils_of_Internet_Fraud_IEEE2000.pdf.

[16] DNSC, „Avertismente și alerte cibernetice". Available: https://dnsc.ro/cat/alerte

[17] DNSC, „Ghiduri de securitate cibernetică". Available: https://dnsc.ro/cat/ghiduri

[18] Bitdefender, „Ghiduri și avertismente". Available: https://www.bitdefender.com/business/support/

[19] Kaspersky Lab, „Alerte și ghiduri". Available: https://www.kaspersky.com/resource-center/threats

[20] SRI, „Glosar de termeni pentru domeniul securității cibernetice", 2019. Available: https://www.sri.ro/assets/files/publicatii/GLOSAR-TERMENI-CYBER-12-09-2019.pdf

[21] SRI, „Ghid de bune practici pentru securitate cibernetică". Available: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

[22] W. Banks, „Cyber Attribution and State Responsibility", in International Law Studies, 2021, pages 1038 – 1072.

[23] A. Olamiposi, L. Tope, S. Oladele, "The Role of Artificial Intelligence", in Finan-

cial Transaction Security, 2024. Available: https://www.researchgate.net/publication/386425222_The_Role_of_Artificial_Intelligence_in_Financial_Transaction_Security

[24] Bitdefender, „Ghiduri de securitate pentru utilizatori", 2023. Available: https://www.bitdefender.com/

[25] D. Kahneman, A. Tversky, "Judgment under Uncertainty: Heuristics and Biases", in Science, 185(4157), 1124-1131, (1974). Available: https://www2.psych.ubc.ca/~schaller/Psyc590Readings/TverskyKahneman1974.pdf

[26] A. Tversky, D. Kahneman , "Advances in Prospect Theory: Cumulative Representation of Uncertainty", in Journal of Risk and Uncertainty, 5(4), 297–323, 1992.

[27] G. Loewenstein, T. O'Donoghue, M. Rabin, "The Role of Emotion in Decision-Making", in Handbook of Affective Sciences, 619–642, 2003.

[28] D. Gambetta, „Trust: Making and Breaking Cooperative Relations", in Oxford University Press, 2008.

[29] Europol, "Internet Organised Crime Threat Assessment (IOCTA)", 2022. Available: https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2022

[30] ENISA, "Threat Landscape Report 2022". Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[31] National Institute of Standards and Technology, "Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations", 2020. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[32] R. Dewar, "Cybersecurity and Cyberdefense Exercises", in *CSS Cyberdefense Reports*, Center for Security Studies (CSS), 2018.

Costinel-Valeriu GONCIULEA graduated from the Faculty of Mathematics and Computer Science at the University of Bucharest in 2005. He pursued two master's courses in technical fields: one at the same faculty from 2005 to 2007 and the second at the Faculty of Electronic and Military Informatic Systems from 2009 to 2012. Since the beginning of his career, he has dedicated his resources and time to the field of information security, actively participating in various training programs and obtaining certifications in the field, one of the most important being CISM (Certified Information Security Manager) within ISACA, where he has been an active member since 2015.