LEGAL AND ADMINISTRATIVE STUDIES, www.jlas.upit.ro
e-ISSN: 2344-6900, ISSN-L: 1583-0772
No.2 (33), Year XXIV, 2025, pp. 120-128

DIGITAL CRIME. ANALYSIS OF THE PHENOMENON AND ITS IMPACT

Cătălin Ionuț BUCUR
ORCID [ID]: https://orcid.org/0000-0003-1606-1978
E-mail: bucurc2000@yahoo.com
Affiliation: Faculty of Economic Sciences and Law, National University of Science and Technology Politehnica Bucharest, Pitesti University Center

Abstract: *This article provides an in-depth analysis of digital crime, a complex and constantly evolving phenomenon that is redefining the global criminal landscape. It explores its origins and historical development, detailing the types and methods of attack, with a particular focus on social engineering as the predominant vector.*

Keywords: *digital crime; typologies; attack methods; social engineering; digital criminals; organized crime groups.*

Introduction

In an era marked by accelerated digitization, digital crime has transcended traditional boundaries of criminality, becoming a major global concern. This complex phenomenon, often referred to interchangeably as "computer crime", "cybercrime", "electronic crime", or "online crime" initially covered all crimes involving computers or other similar devices, including networks and other means of access. However, despite the widespread use of these terms, a universally accepted definition of "cybercrime" remains elusive, complicating its study and legal examination worldwide. This lack of standardization contributes to a wide range of forms and types of acts included under this umbrella.

The semantic ambiguity and legal challenges associated with defining digital crime are not simply matters of terminology; they have direct implications for legislative harmonization across jurisdictions.

When different countries define the same crime differently, it creates legal loopholes that criminals can exploit, making it harder to cooperate effectively in investigations and prosecutions. This conceptual fluidity underscores the need for continued efforts to harmonize legal frameworks and develop clear and consistent operational guidelines for law enforcement agencies globally.

It also highlights the importance of robust academic discourse in refining conceptual boundaries and informing public policy.

1. The fundaments of cybercrime

1.1. Key Definitions and Concepts

Defining cybercrime is inherently challenging, given the broad spectrum of offenses it encompasses. For a better understanding of the phenomenon, it is essential to make the critical and widely accepted distinction between "cyber-dependent crimes" (also known as "pure cybercrime") and "cyber-facilitated crimes", which provides a clearer framework for understanding the phenomenon (Mungiu-Pippidi, 2017, p. 25).

Dependent cybercrimes are those acts which, by their nature, can only be committed through the use of a computer, computer networks, or other forms of information and communications technology (ICT).

Examples include the spread of viruses or other malware, unauthorized access (hacking) to systems, and Distributed Denial-of-Service (DDoS) attacks. These activities are primarily directed against the integrity or availability of computer or network resources, although they may have various secondary results, such as the use of data obtained through hacking to subsequently commit fraud (Ruse, 2018, p. 40).

On the other hand, facilitated cybercrime refers to traditional crimes whose scope, coverage, or efficiency are significantly enhanced by the use of computers, computer networks, or other ICT. Unlike

dependent cybercrime, the underlying criminal act could theoretically be committed without the use of ICT.

Prominent examples include various forms of fraud and theft, often facilitated by email scams (Bucur, 2020, p. 55).

Although the terms "cybersecurity" and "cybercrime" are interdependent and their interests often overlap, their meanings are not identical. The scope of "cybersecurity" and "cybercrime" varies significantly depending on technical, legal, and political perspectives.

An important observation is that, despite the technical nature of threats, the human element remains the most common vulnerability. Most breaches involve some form of human interaction, often unintentional, as we are all susceptible to manipulation through increasingly sophisticated criminal techniques (Manolescu, 2019, p. 110).

This persistent vulnerability of the human factor, even in the context of highly technical threats, underscores that purely technological solutions are insufficient. Human factors, such as susceptibility to manipulation, remain central. Therefore, any truly effective cybersecurity strategy must allocate substantial resources to human education, ongoing awareness programs, and the cultivation of a resilient security culture. This recognizes that technological solutions, while indispensable, are ultimately incomplete without addressing the human factor (Popescu, & Neagu, 2020, pp. 88-105).

1.2. Brief History and Evolution

The history of digital crime mirrors technological progress, a symbiotic evolution between innovation and exploitation. What could technically be considered the first "cyberattack" took place in France in 1834, involving the hacking of the French telegraph system to steal information from the financial market. Over the years, other early "hackers" have emerged who disrupted telephone services and wireless telegraphy, preceding modern computers.

The 1940s were, in digital terms, "the time before crime" characterized by limited access to the first digital computers and a lack of interconnection between them.

However, in 1949, computer pioneer John von Neumann first

speculated on the theory underlying the ability of computer programs to reproduce themselves, thus foreshadowing the emergence of viruses. In the late 1950s, the phenomenon of "phone phreaking" emerged, in which individuals passionate about telephone systems hijacked protocols to make free calls, representing a significant technological and subcultural root of hacking. In 1962, MIT implemented the first passwords for computers, mainly to limit student usage time and ensure data confidentiality. The year 1969 marked the appearance of what is considered to be the first computer virus, the "RABBITS Virus" at the University of Washington Computer Center, which replicated itself until the system was overloaded.

The actual birth of "cybersecurity" took place in 1972, with a research project on ARPANET, the precursor to the internet, which developed protocols for remote computer networks and explored the security of operating systems. Kevin Mitnick, often cited as the "first cybercriminal" was active between 1970 and 1995, managing to access some of the world's most secure networks, including those of Motorola and Nokia (Dicu, & Rădulescu, 2021, pp. 45-60).

The 1980s and 1990s brought transformative change with the popularity and widespread use of personal computers, leading to an explosion in the number of new viruses and malware programs. A significant increase in data breaches has been observed since 2005, correlating directly with the widespread migration of businesses and governments from paper to digital records.

This historical timeline illustrates a continuous and parallel evolution: as technological capabilities expanded, new vulnerabilities inevitably emerged, giving rise to innovative forms of criminal activity. In direct response, cybersecurity measures and concepts such as passwords, antivirus software, and research into operating system security have also developed[1].

---

[1] European Union, European Union Agency for Cybersecurity (ENISA), Report on the cyber threat landscape. Published annually.

2. Typologies and Means of Attack

2.1. Classification of cybercrime

The fundamental framework for classifying digital crime distinguishes between dependent and facilitated cybercrimes, a distinction recognized by major cybersecurity agencies such as Interpol and Europol. Beyond this basic classification, digital crime manifests itself through a multitude of specific types of crimes and attack vectors, each with its own particularities.

Hacking and **cracking** refer to unauthorized access to computer systems or networks, often with malicious intent. These activities can range from exploring systems for vulnerabilities to compromising them for the purpose of data theft or sabotage.

Malware is a generic term for malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, worms, Trojan horses, and spyware.

One particularly widespread type is **ransomware**, which encrypts a victim's personal or organizational data and demands payment, often in hard-to-trace cryptocurrencies, for the decryption keys or to restore access. Ransomware attacks have become a major global threat, affecting both individuals and companies.

Distributed Denial-of-Service (DDoS) attacks are malicious attempts to disrupt the normal traffic of a targeted server, service, or network by overloading it with a massive flow of internet traffic from multiple compromised computer systems, known as botnets. These attacks may target critical infrastructure, such as hospitals or public authorities, sometimes without financial gain, but rather for ideological or political reasons.

Online fraud is a broad category that encompasses various deceptive practices carried out through digital means.

Computer fraud involves using a computer to illegally alter electronic data or gain unauthorized access to a system. Specific types of online fraud include scams related to online shopping, internet auctions, and credit card fraud.

Romance and online dating scams are deceptive schemes in

which criminals fake romantic interest to extract money or personal information from victims.

Business Email Compromise (BEC) is a form of fraud with a particularly high impact, in which criminals pose as directors or trusted partners to trick employees into diverting payments to fraudulent accounts, often generating losses of millions of euros.

Fraud can also involve virtual currencies, including cryptojacking (the unauthorized use of computing power to mine cryptocurrencies) and exit scams (where sellers on darknet markets collect buyers' money and close accounts without delivering the products).

There is also advertising fraud, classified into identity fraud (audience simulation through bots), attribution fraud (imitating real activities through click farms) and ad fraud services (creating spam sites or fraudulent pages) (Bucur, 2020, p.70).

Online identity theft involves the illegal acquisition and use of another person's identifying information (e.g., name, email address, password) to commit fraud, open accounts, or make unauthorized purchases.

Phishing is one of the most common and dangerous methods of cyber fraud, involving deceptive attempts (via email, SMS, phone calls) to trick users into disclosing sensitive personal or financial information by impersonating legitimate and trusted organizations. Variations include spear phishing (highly targeted attacks), vishing (voice phishing), smishing (SMS phishing), and whaling (targeting high-profile individuals) (Ionescu, 2022, pp. 112-128).

Sexual abuse and exploitation of children via the Internet is a serious category that includes online sexual abuse of children, exploitation, live abuse, grooming (criminals pretending to be children to lure minors), and distribution of child sexual abuse material.

Cyberbullying, cyberstalking, and other forms of online aggression include various forms of harassment, threats, and aggression committed in digital human interactions.

Cyberterrorism consists of terrorist acts carried out through cyberspace, which may include the widespread dissemination of viruses, worms, phishing campaigns, and malware attacks.

Cyberextortion occurs when websites, servers, or computer systems are threatened with attacks (e.g., denial-of-service attacks) by hackers who demand money to stop the attack.

Skimming involves organized crime groups compromising and defrauding electronic payment instruments, often planning their illicit activities domestically but executing them abroad.

2.2. Social engineering as a vector of attack

Social engineering is defined as a wide range of activities designed to exploit human error or behavior, using various forms of manipulation to trick victims into making mistakes or divulging sensitive information or granting access to services. The human element remains the most common vulnerability, with a 2023 Verizon Data Breach Investigations Report (DBIR) indicating that 82% of breaches involve some form of human interaction (Manolescu, 2019, p. 75).

Among the most common and effective social engineering techniques are:

- **Phishing**: This is a fundamental method of social engineering. Attackers send fraudulent emails, messages, or links that appear to come from legitimate sources (e.g., banks, coworkers, well-known websites). The goal is to obtain login credentials, banking information, or to convince the victim to download infected files. These messages are designed to look extremely realistic, often incorporating legitimate logos, names, and addresses similar to the official ones. This type of scam is not limited to emails, but also occurs via text messages (smishing), phone calls (vishing), or social media.
- **Pretexting**: The hacker creates a credible, often elaborate, fictional scenario to trick the victim into divulging private information. For example, the attacker may pose as an IT employee requesting login details for "routine checks" or claim to represent a well-known institution such as a bank or telephone company. The victim, believing they are interacting with a trustworthy person, provides the information without

suspicion. Pretexting requires patience and convincing communication on the part of the attacker, who often constructs a detailed scenario, sometimes based on information previously obtained about the victim from social networks or public data.

- **Baiting**: The victim is lured with a "bait" such as an apparently lost USB stick containing malware or an attractive downloadable file. Curiosity or the desire to obtain something for free motivates the user to connect the device to the computer or download the file, thereby granting access to the attacker. Baiting can also occur in digital form, for example through websites that promise free access to movies or applications, but which actually infect the device with Trojans or spyware.
- **Quid Pro Quo**: The attacker promises something in exchange for information or access, such as free technical support, an important software update, or a fictitious prize. The victim, attracted by the proposed benefits, willingly provides personal data or performs actions that compromise the security of the device or network. This method is common via telephone or email, especially in office environments, where attackers claim to be providing technical support and request passwords or authentication codes.
- **Tailgating**: This technique involves gaining unauthorized physical access to a restricted area by closely following an authorized employee or by inventing a reason for entry, such as claiming to have forgotten one's access badge (Mungiu-Pippidi, 2017, p. 50).

Social engineering is particularly effective because it exploits fundamental human traits such as trust, curiosity, and the natural inclination to act in certain ways to establish strong social structures. Criminals understand human behavior and how to manipulate individuals by feigning trust or building relationships (Popescu, & Neagu, 2020, pp. 88-105).

Conclusions

Digital crime has evolved from a marginal phenomenon to a systemic threat, deeply integrated into the fabric of modern society. In-

depth analysis has shown that its nature is multifaceted, blurring the boundaries between traditional and purely cybercrimes, and that it is fuelled by diverse motivations, ranging from financial gain to ideological and geopolitical objectives. The professionalization and democratization of cyber capabilities, through crime-as-a-service platforms and accessible tools, have significantly broadened the pool of potential offenders, transforming cybercrime into a macroeconomic force with estimated annual losses in the trillions of dollars.

The impact of this phenomenon goes far beyond the economic dimension, generating profound social consequences by eroding public trust and facilitating the spread of illegal content, and leaving invisible psychological scars on victims, who face anxiety, loss of control, and, in severe cases, mental health disorders.

The vulnerability of critical infrastructure to cyber-attacks also highlights direct risks to public safety and national security.

References

Bucur, C. I. (2020). *Criminalitatea digitală. O abordare multidisciplinară.* Universul Juridic.

Ionescu, P. (2022). Tacticile de inginerie socială în era digitală. De la phishing la deepfake-uri. *Revista de Studii Juridice și Administrative*, 25(1), 112-128.

Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as subsequently amended and supplemented. (Crucial legislative basis)

Mungiu-Pippidi, R. (2017). *Securitatea cibernetică și provocările lumii moderne.* National Intelligence Academy Press.

Manolescu, C., I. (2019). *Ingineria socială și vulnerabilitatea umană.* Lumen.

Romanian Criminal Code, Title IV – Offences against the security and integrity of computer systems and data. (Main source for the national legal framework)

Ruse, C. (2018). *Criminalitatea informatică. Dreptul penal al tehnologiei informației și comunicațiilor.* C.H. Beck.