South American Publishing

SAP Netnography. 2024;2:69
doi: 10.62486/net202469

REVIEW

Criminal Behavior Analysis of Cybercriminals: Profiles, Motivations, and Trends in Cybersecurity

Análisis del Comportamiento Criminal del Ciberdelincuente: Perfiles, Motivaciones y Tendencias en la Ciberseguridad

Cecilia Elizabeth Checchia[1]
Francisco Gabriel Bolzan[1]

[1] Universidad Siglo 21, Licenciatura en Criminología y Seguridad. Buenos Aires, Argentina.

Submitted: 03-05-2023 | Revised: 10-08-2023 | Accepted: 01-01-2024 | Published: 02-01-2024

ABSTRACT

Within the vast territory of the digital world, a challenge has emerged in recent years, that of the cybercriminal. This agent, with perplexing technical skills, transcends physical borders, threatening the security and privacy of individuals, businesses, and institutions alike. In this context, the need to unravel the mysteries surrounding their behavior becomes evident. Thus, this research becomes a source of knowledge in the midst of this complex digital environment by addressing the modus operandi of these malicious actors and, in doing so, aspiring to understand their psychological profiles, motivations, and patterns of action within the broad field of cybersecurity. Through the exploration of cases that have occurred in our country and the analysis of literature, this study aims to provide a comprehensive overview of how these figures maneuver in the virtual space. The goal is not only to observe their actions but also to decipher the background of their intentions. As we investigate this scenario, the need to implement both preventive and corrective approaches that are effective in mitigating their impact becomes evident. This research represents a commitment to expanding the spectrum of knowledge regarding criminal behavior in the digital realm. The objective is undoubtedly to strengthen the sphere of cybersecurity through the substantial contribution it makes to the understanding of these actors and, consequently, to the development of mitigation strategies. However, its implications go beyond lines of code and security protocols. By providing a solid foundation of understanding, the aim is to protect not only systems but also individuals, organizations, and institutions facing these digital threats. The convergence of psychology, criminology, and cybersecurity provides us with a more comprehensive view that goes beyond the purely technical and delves into underlying motivations. This union, at its core, aims to establish a robust defense in this ongoing digital battlefield. This study presents itself as a concrete effort to explore the most enigmatic aspects of the interaction between humans and machines, where malice, intention, and vulnerability intertwine. Through this research, we embark on a journey toward understanding and, consequently, toward preparing for a safer coexistence in the digital environment.

Keywords: Cybercrime; Cybersecurity; Cybercriminal Profiles; Cybercrime Motivations; Cybersecurity Trends.

RESUMEN

En el inmenso territorio del mundo digital, surge un desafío que en los últimos años ha cobrado un notable crecimiento, hablamos del ciberdelincuente. Este agente con habilidades técnicas desconcertantes trasciende las fronteras físicas, amenazando la seguridad y privacidad de individuos, empresas e instituciones por igual. En esta coyuntura, surge la necesidad de desentrañar los misterios que rodean su comportamiento. De este modo, esta investigación se convierte en una fuente de conocimiento en medio de este entorno digital complejo al abordar el modus operandi de estos actores maliciosos y, con ello, aspirar a comprender sus perfiles psicológicos, motivaciones y patrones de actuación dentro del amplio campo de la ciberseguridad. A través de la exploración de casos ocurridos en nuestro país y el análisis de bibliografía, este estudio tiene por objeto presentar una panorámica completa de cómo estas figuras maniobran en el espacio virtual. Se busca no solo observar sus acciones, sino también descifrar el trasfondo de sus intenciones. A medida que investigamos este escenario, se hace evidente la necesidad de implementar enfoques tanto preventivos como correctivos que sean efectivos en la mitigación de su impacto. Esta investigación, representa un compromiso con la ampliación del espectro del conocimiento en lo que respecta al comportamiento criminal en el ámbito digital. La meta es, sin lugar a duda, reforzar la esfera de la ciberseguridad a través del aporte sustantivo que brinda al entendimiento de estos actores y, por ende, al desarrollo de estrategias de mitigación. No obstante, sus implicaciones trascienden las líneas de código y protocolos de seguridad. Al proporcionar una base sólida de comprensión, se busca proteger no solo sistemas, sino también a individuos, organizaciones e instituciones que se enfrentan a estas amenazas digitales. La convergencia de la psicología, la criminología y la ciberseguridad nos proporciona una visión más integral, que va más allá de lo puramente técnico y se adentra en las motivaciones subyacentes. Esta unión, en su esencia, tiene como objetivo establecer una defensa sólida en este continuo campo de batalla digital. Este estudio se presenta como un esfuerzo concreto para explorar los rincones más enigmáticos de la interacción entre humanos y máquinas, donde se entrelazan malicia, intención y vulnerabilidad. Mediante esta investigación, emprendemos un viaje hacia la comprensión y, por ende, hacia la preparación para una convivencia más segura en el entorno digital.

Palabras clave: Ciberdelito; Ciberseguridad; Cibercrimen; Perfiles de Ciberdelincuentes; Motivaciones del Ciberdelito; Tendencias de Ciberseguridad.

INTRODUCTION

Currently, the field of cybersecurity has become an increasingly complex and challenging landscape. The growing dependence on technology and the global interconnection of computer systems have led to the emergence of a form of crime that transcends physical borders, namely cybercrime.(1,2,3) This form of criminal activity, carried out by individuals known as cybercriminals, poses significant threats to both individuals and organizations of various kinds, ranging from governments to companies and ordinary users. This phenomenon requires adequate attention and response to safeguard security in the digital environment.(4,5,6)

Technological evolution has driven changes that have reconfigured our daily routines, our work environments, and our ways of communicating. Despite the advantages and conveniences that this evolution has brought, it has also given rise to a digital domain in which individuals with a high level of technical expertise operate. These individuals use their skills to carry out illicit actions, giving rise to the phenomenon known as cybercrime.(7,8,9)

Cybercrime operates in a highly sophisticated and constantly evolving environment, which poses ongoing challenges for its detection and prevention. This dynamic environment requires an equally agile and advanced response to ensure security in the digital world.(10,11,12)

It is essential to understand cybercriminal behavior in depth in order to develop effective cybersecurity strategies and counteract their activities.

The relevance of this research is evident in a constantly evolving digital environment, where cyber threats can have devastating consequences in terms of data loss, disruption of critical services, and privacy breaches. Understanding who cybercriminals are, what motivates them, and how they operate is essential to minimize the risks associated with technology.(13,14,15)

Throughout these pages, the results of a rigorous analysis of information, the identification of cybercriminal profiles and their motivations, and emerging trends in cybersecurity, such as the use of AI (Artificial Intelligence), will be examined.(16,17,18)

This research approach involves the intersection of fields such as psychology, criminology, and cybersecurity. Through this comprehensive perspective, the aim is to obtain a complete view of the cybercriminal mind and the factors that influence their actions.(19,20,21)

This research aims to contribute to existing knowledge in the field of cybersecurity and to serve as a valuable tool for professionals, researchers, and policymakers seeking to address the ongoing challenge of protecting cyberspace in an increasingly interconnected world. The findings and conclusions presented here will not only enrich understanding of cybercrime but will also provide guidance for the development of effective prevention and response strategies in the digital era.(22,23,24)

The first chapter presents the context and justification for this research. It highlights the importance of analyzing cybercriminal behavior within the current cybersecurity landscape and emphasizes the need to address this challenge from a multidisciplinary perspective, thereby offering a solid foundation for addressing this topic.(25,26,27)

The second chapter constructs the necessary theoretical framework, which provides a complete and unified understanding of cybercrime and cybersecurity in the analysis of criminal behavior.(28,29,30,31)

The following chapters delve into the multiple facets of cybercriminals' criminal behavior. The typical psychological profiles, the technical skills that distinguish these malicious individuals, and the factors that influence their target selection are examined. Furthermore, the varied motivations driving their actions are analyzed, ranging from financial incentives to ideological and political motivations and the simple desire to face challenges. This analysis provides a more comprehensive understanding of the complexity of cybercrime.(32,33,34,35,36)

The fourth chapter introduces the analysis of trends and behavioral patterns that emerge from cyberattacks and how these criminals evade detection through social engineering techniques and psychological manipulation. Through the study of real cyberattack cases, a detailed view of the strategies used by these individuals is provided.(37,38,39,40,41)

The fifth chapter explores the connection between cybercrime and cyberterrorism. It analyzes how certain cybercriminals may be influenced by the online radicalization process, leading them to engage in activities with clearly defined terrorist motivations. This analysis will enrich understanding of the intersection between these two fields and their repercussions in both academic and professional spheres.(42,43,44,45,46)

Finally, the sixth chapter addresses prevention and mitigation strategies for confronting cybercriminal behavior. It highlights approaches for strengthening cybersecurity, education, and awareness, as well as the importance of collaboration between the public and private sectors to

address this challenge comprehensively.(47,48,49,50,51)

This analysis aims to improve the understanding of the criminal behavior of cybercriminals. (52,53,54) It seeks to provide effective tools to strengthen cybersecurity and to protect against cyberattacks. In doing so, it examines the complexities of their profiles, motivations, and patterns, thereby contributing to a safer and more resilient digital environment for all who participate in this ongoing exchange of information and power.(55,56,57,58)

Background and Rationale

Currently, we are immersed in an era of digital transformation that has had a major impact on our daily lives. The digitalization and global interconnection of computer systems have driven a technological revolution that has permeated all aspects of our existence: how we live, how we work, and how we communicate. Although this technological change has brought countless benefits and conveniences, it has also posed a series of complex and diverse challenges. Among these challenges, the rapid increase in cybercrime stands out for its growing urgency. This phenomenon requires special attention and an effective response from society and the academic community. (59,60)

Cybercrime is a concept that encompasses a broad and diverse range of criminal activities carried out in the vast and complex territory of cyberspace.

“They are illegal behaviors carried out by cybercriminals in cyberspace through electronic devices and computer networks.

It consists of scams; theft of personal data and strategic commercial information; identity impersonation; computer fraud; and attacks such as cyberbullying, grooming, and phishing, committed by cybercriminals who act in groups or work alone.”

Background: Over the years, numerous incidents and alarming trends have been documented in the field of cybersecurity, supporting the urgent need to address this phenomenon. According to recent statistics from ESET in its report “Security Report Latinoamérica 2023”, cyberattacks have multiplied and diversified, causing significant economic losses globally. Organizations and ordinary citizens have experienced the direct impact of cybercrime in the form of data theft, extortion, ransomware attacks, and other cybercrimes.(61,62,63,64)

Previous research and reports in the field of cybersecurity have clarified different aspects of this problem, from identifying vulnerabilities in computer systems to implementing technical solutions. However, despite sustained efforts in this direction, multifaceted challenges persist in preventing and mitigating technological threats.(65,66,67)

In this digital environment without physical borders, cybercriminals deploy their advanced technical knowledge to commit a variety of illegal acts. Their actions range from the theft of confidential data and extortion.(68)

cybernetics, to the sabotage of critical infrastructures and the execution of espionage operations. Cybercriminals, mostly invisible to the human eye, operate in a virtual space where borders blur and jurisdictions overlap and unfold in a matter of milliseconds.

As society enters an increasingly connected era dependent on technology, threats emerge as a global security problem. This concern encompasses a varied range of actors, from multinational corporations to government agencies responsible for safeguarding security, and even ordinary citizens who entrust their digital lives to online platforms. Cybercrime, in its essence, not only has the potential to cause significant economic losses but also poses much greater threats, including vulnerabilities in our security, loss of privacy, and risks to the integrity of critical data that sustain the functioning of our current society.(69,70,71)

The central problem addressed in this thesis is the urgent need to understand and analyze in detail the behavior of cybercriminals. Despite continuous and sustained efforts in cybersecurity, identifying and mitigating threats remains a perpetual and multifaceted challenge. To confront cybercrime efficiently and effectively in all its dimensions, it is imperative to decipher the complex dynamics of who these actors are, what drives their illegal online actions, and how they evolve and adapt their tactics and strategies over time.(72,73,74)

The behavior of cybercriminals is an essential piece in the intricate puzzle of cybersecurity. Who are these individuals who operate behind the screens? What underlying factors, motivations, and triggers lead them to commit criminal acts in cyberspace? How do they organize and coordinate in this digital world, seemingly without limits or defined borders? What emerging trends in cybercrime must we monitor and understand in depth to anticipate and confront the threats taking shape on the horizon? These are only some of the fundamental questions that this research aims to address with the greatest depth and meticulousness.(75,76,77)

The knowledge acquired about the criminal behavior of cybercriminals is not only fundamental for active prevention and effective response to ongoing cyberattacks but also essential for formulating and executing solid and proactive cybersecurity policies and strategies. By understanding the motivations and social dynamics underlying the actions of cybercriminals, we can create more effective strategies to discourage, prevent, and deter their criminal activity.(78,79,80)

Understanding and characterizing cybercriminal behavior is important to guarantee security, integrity, and trust in a constantly evolving digital world. This research aims to contribute to knowledge and to the design of effective strategies to address cybercrime, transcending current limitations and building a safer future in the digital environment. Trust in technology is shown to be an essential element for the widespread adoption of technological innovations. For society to continue taking advantage of the countless benefits of technology, it is imperative to maintain trust in digital platforms and systems.(81,82,83)

Research Objectives

General Objective

The general objective of this research is to deepen understanding of cybercrime and cybersecurity in order to strengthen online security and contribute to knowledge in this field.

Specific Objectives

- Identify and categorize psychological profiles that characterize cybercriminals through a multidisciplinary approach integrating elements of psychology and criminology.
- Investigate the various motivations that drive cybercriminals to commit online crimes, encompassing financial incentives, political and ideological objectives, among others.
- Analyze emerging trends and behavioral patterns through the detailed study of real-world cyberattack cases to identify repetitive sequences of actions and tactics used by cybercriminals.
- Develop effective strategies for the prevention and mitigation of cyberattacks, based on understanding of cybercriminal behavior, including technical measures and good security practices.
- Contribute to knowledge in the field of cybersecurity and cybercrime prevention by presenting new data, approaches, and perspectives that enrich the existing knowledge base.
- Promote collaboration and awareness in cybersecurity by highlighting the importance of cooperation among various actors involved in online security and fostering awareness of cyber threats to address this challenge jointly and effectively.

METHODS

This research will be conducted using a qualitative methodology. The aim is to obtain a comprehensive perspective that allows the exploration of both the psychological and motivational aspects of cybercriminals and the trends and behavioral patterns that arise from their online actions.

The main stages of the methodology are described below:

- Literature review: a review of scientific and technical literature related to cybercrime, cybersecurity, and criminal psychology will be conducted. This review will provide a solid understanding of the fundamental concepts and relevant theories in the field.
- Analysis of practical cases: a detailed examination of real cases of cyberattacks, as well as the activities carried out by cybercriminals, will be carried out to study their tactics, techniques, and procedures. These cases will serve as examples for understanding the motivations that drive these attacks and how cybercriminals evade detection.
- Recommendations: the results obtained from the analysis will be used to formulate recommendations that effectively address cybercrime and strengthen cybersecurity. Prevention and mitigation strategies based on the analysis of cybercriminal behavior will be proposed.

DEVELOPMENT

Cybercrime and Cybersecurity

Cybercrime and cybersecurity are closely related concepts that play essential roles in the digital environment. Despite their importance, the precise conceptualization of these terms has not

yet achieved universal consensus. For this reason, various definitions proposed by experts in the field have been used to approach a more precise understanding by interpreting their approaches and perspectives. Both terms are described below:

Cybercrime

Cybercrime is a term that encompasses a variety of concepts and meanings, which can make its definition somewhat complex. To better understand it, it is useful to break it down in terms of whom it targets, who originates it, and the nature of the offense in question.

In general terms, cybercrime can be defined as the set of actions carried out through computer systems or digital assets that result in acts considered unlawful. In other words, it is an extension of traditional crime that uses new technologies to expand and develop broadly.

To elaborate further on this definition, cybercriminal actions can be considered those that put at risk the confidentiality, integrity, and availability of computer systems, networks, and data, as well as the fraudulent use of such systems. This definition is based on the Budapest Convention on Cybercrime of 23 November 2001, which establishes an international framework for addressing cybercrimes.

Although much of cybercrime revolves around obtaining confidential information for unauthorized purposes, it is important to recognize that this phenomenon also encompasses criminal acts familiar in the non-digital world. We refer to crimes such as theft, identity theft, fraud, harassment, and a series of other criminal acts that, in this context, are carried out via the Internet.

Cybercrime is not limited solely to the sphere of technology but encompasses a wide range of illegal activities that can have serious consequences in both the virtual and real worlds. The constant evolution of online threats makes it crucial to address this issue comprehensively.

Drawing on the information provided by the Ministry of Justice and Human Rights5, the most common cybercrimes and infractions constitute a series of criminal activities carried out in the digital environment that encompass various forms of intrusion into and manipulation of computer data for the purpose of obtaining financial gains and causing harm. These actions, characterized by their unlawful nature, can be grouped into several categories:

- Navigation attacks: These attacks consist of redirecting web browsers to malicious sites that can infect systems with malware, such as viruses, worms, and trojans. The effects of such programs include data deletion, infection of devices, unauthorized activation of cameras and microphones, and extraction of confidential information.
- Server attacks: Cybercriminals may direct their efforts at servers in order to damage or steal data, as well as to deny legitimate access to the information stored on such servers.
- Database corruption: This type of cybercrime involves interfering with databases, both public and private, to generate false information or steal sensitive data.
- Computer viruses: Computer viruses encrypt files, lock systems, and even steal money by sending fraudulent text messages that appear to come from legitimate companies.
- Spyware programs: These programs can access and use cameras and microphones on devices without authorization, in addition to secretly collecting personal information.

In the execution of these cybercrimes, social engineering is frequently used to deceive, threaten, and obtain personal data or sensitive information from individuals or organizations, obtain economic benefits, impersonate identities, engage in digital harassment, or commit sexual assaults online. Some examples of these practices are:

- Phishing or vishing: Cybercriminals impersonate legitimate entities, such as service companies or government institutions, in order to obtain personal information with which to impersonate identities and carry out illicit activities in bank accounts, on profiles on digital platforms and social media, and in online services.
- Cyberbullying: Online harassment, known as cyberbullying, manifests as stalking, harassment, and defamation of individuals through instant messaging and social networks, with the aim of affecting their moral integrity and reputation.
- Grooming: In this case, adults attempt to covertly obtain sexual images or videos of minors for purposes of blackmail or subsequent sexual abuse.
- Sextortion: This involves requesting money in exchange for not disseminating images generated in the context of a consensual erotic exchange.
- Cyberhate: This includes inappropriate content that harms people, such as the promotion of violence, hate, xenophobia, racism, discrimination, and animal abuse.
- Child pornography: This refers to the sexual exploitation of minors and the production and commercialization of explicit content related to these acts.

In addition to the aforementioned categories of cybercrime, there is another dimension that involves the violation of people's privacy, which includes:

- Unlawful espionage of citizens' private communications.
- Violation of privacy by Internet service providers without user consent, in order to obtain information about their preferences and facilitate the aggressive sale of related products and services.
- Unauthorized access to employees' private communications, such as emails and social media profiles.

The growth of cybercrime has been notable in recent years, significantly driven by the unstoppable advancement of technology and the growing interconnection of our systems. Cybercriminals have demonstrated a remarkable capacity for adaptation, not only to take advantage of new technologies but also to refine their tactics, making them increasingly sophisticated and difficult to detect.

Artificial intelligence (AI) has become a key tool for both cybercriminals and cybersecurity professionals. Malicious actors use AI to automate tasks such as identifying vulnerabilities in systems and networks, phishing, and generating highly personalized malware. This automation streamlines their operations and allows them to scale their attacks efficiently.

The complexity and severity of cybercrimes continue to increase. Ransomware attacks, for example, have evolved into an even more dangerous form, known as "double extortion," in which attackers not only encrypt the victim's data but also threaten to disclose confidential information if a ransom is not paid. This adds an additional dimension of pressure on victims. Cybercriminals have also become more selective in choosing their targets.

Government organizations, large companies, and critical infrastructure are prime targets due to the potential economic and social impact of attacks against them.

In this scenario, promoting education and awareness on cybersecurity issues is imperative. Individuals and organizations must understand the threats they face and adopt robust security practices, such as the use of strong passwords, MFA, and regular updates of software and systems.

Cybersecurity

Cybersecurity encompasses a set of measures, technologies, and strategies aimed at safeguarding computer systems, networks, and data from cyber threats and online criminal acts. Its fundamental purpose is to preserve the integrity, confidentiality, and availability of digital information, while ensuring the protection of assets and resources in the digital environment.

In the field of cybersecurity, various measures are implemented to protect systems and sensitive data. These measures include:

- Intrusion Detection and Prevention Systems: systems are installed to detect and prevent unauthorized intrusions into networks and computer systems, providing active defense against potential threats.
- Firewalls and Malware Protection: firewalls and malware protection software are used to filter network traffic and prevent malicious software from infecting systems.
- Authentication and Encryption: strong authentication methods and robust encryption are applied to safeguard access to confidential information, ensuring that only authorized individuals can access it.
- Training and Awareness: staff receive training in safe online practices, promoting awareness of cyber risks and the importance of maintaining digital security in the workplace.
- Collaboration and Information Sharing on Threats and Vulnerabilities: Cooperation among different actors is essential to exchange information on cyber threats and vulnerabilities, enabling a more effective response.

Additionally, it is essential to consider other cybersecurity practices, such as:

- Data Backup: safeguard critical data in secure locations and ensure the ability to restore tested copies in the event of file loss or corruption.
- Safe Cyber Habits: avoid opening unexpected links or attachments in emails or text messages, even if they come from trusted senders, to prevent potential phishing attacks.
- Updated Software Maintenance: update operating systems, applications, and browsers with the latest revisions and patches provided by manufacturers, thereby reducing exploitable vulnerabilities.
- Strong and Unique Passwords: use strong passwords with at least 14 characters, avoid English words, and avoid reusing them across multiple accounts, thereby strengthening online security.

- Multifactor Authentication: enable multifactor authentication whenever possible, adding an additional layer of security in both home and work environments.
- Device Locking: configure devices to require a password, PIN, or biometric authentication, such as fingerprints or facial recognition, to access them, reducing the risk in case of loss or theft.

These practices, when applied consistently and efficiently, contribute significantly to strengthening cybersecurity and protecting digital assets.

On the other hand, cybersecurity experts have also adopted artificial intelligence as a valuable tool in combating cybercrime. The application of machine learning algorithms enables them to analyze traffic patterns in search of suspicious activities, identify unusual behaviors, and anticipate potential threats. Artificial intelligence plays an essential role in detecting and mitigating attacks in real time, which has become indispensable in a constantly evolving digital environment.

With technology constantly advancing and cybercrime representing a persistent threat, cybersecurity remains in a state of continuous evolution and adaptation to confront emerging challenges and threats.

Fundamental concepts in the analysis of criminal behavior

In the analysis of criminal behavior, several essential concepts play a fundamental role in understanding the motivations, patterns, and distinctive traits of offenders. These concepts establish a solid theoretical foundation that supports research in the field of criminal behavior, including the criminal behavior of cybercriminals. Next, some of the most prominent concepts in this field of study will be presented:8

Motivations: In the analysis of criminal behavior, it is essential to explore the reasons that drive one person to commit an unlawful act. Understanding these motivations plays a fundamental role in this discipline. These motivations can be diverse, encompassing economic, social, and political aspects, as well as personal and emotional impulses. In the specific case of cybercrime, motivations may include the pursuit of economic gain, the desire for recognition, adherence to a political ideology, or an interest in overcoming technical challenges.

Psychological Profiles: Psychological profiles represent detailed descriptions of the characteristics, personality, and behavioral patterns typical of a given type of offender. In the field of criminal behavior analysis, the objective is to identify recurring trends in offenders' conduct that help understand their motivations and criminal strategies. These profiles may include information on age, gender, educational level, criminal record, and other characteristics that may be related to criminal behavior.

Criminal Cycle: The concept of the criminal cycle refers to the various stages or phases that an offender may go through, from the conception of a crime to its execution, and in some cases, recidivism. These stages may encompass planning, target selection, execution of the crime, and escape. Understanding the criminal cycle provides valuable information for preventing and reducing crime, as well as for understanding how offenders prepare for and carry out their actions, both in the traditional context and in cyberspace.

Social Engineering Techniques: Social engineering techniques comprise strategies employed by criminal individuals with the purpose of manipulating people in order to obtain confidential information or gain unauthorized access to systems and data. These tactics are based on the understanding of human psychology, including aspects such as trust, fear, and curiosity, to induce victims to make mistakes that allow them to achieve their illicit objectives. In the context of analyzing the criminal behavior of cybercriminals, research into these techniques is highly relevant, given that they are widely used in cyberattacks.

By analyzing these dimensions, a more complete view can be obtained of the factors that drive criminals to commit crimes and, consequently, to design more effective strategies to prevent and address cybercrime.

Psychological Profiles of the Cybercriminal and Motivations

The analysis of the criminal behavior of cybercriminals involves the evaluation of psychological profiles that characterize these individuals involved in criminal activities in the digital environment. It is relevant to highlight that psychological profiles can be diverse, and it is not possible to apply a single pattern to all cybercriminals. However, certain common characteristics have been identified that provide a more complete view of online criminal behavior. Below, some of the psychological profiles that have been observed in certain cybercriminals are presented, starting with the profile known as hacker, since it is important to recognize that not all hackers are cybercriminals.

Hacker Profile

A hacker is a highly skilled individual well-versed in computer science and information technology, whose main focus is the exploration, understanding, and manipulation of computer systems and networks. Hackers use their technical knowledge to identify vulnerabilities in computer systems, develop creative solutions to technical problems, and, in some cases, to bypass security restrictions.

White Hat Hacker: the Ethical Hacker, also known as "White Hat Hacker" or "White Hat Hacker," is an individual highly trained in computer security who uses their skills for an ethical and legal purpose. Their main focus is to identify and correct vulnerabilities in systems, networks, and applications to protect the integrity and security of information.

Ethical Hackers adhere to a strict ethical code that prohibits the use of their skills for malicious purposes. They are committed to legality and integrity in their work. They possess in-depth knowledge of computer systems, programming, and network protocols. This allows them to identify and understand security vulnerabilities.

Hacker Motivated by Technical Challenge: Hackers motivated by technical challenge, often called "amateur hackers" or "hackers for fun", are individuals who engage in hacking activities primarily due to an interest in exploring and overcoming technical challenges. These hackers are motivated by curiosity and the desire to learn about systems, networks, and technology in general.

The primary motivation of hackers motivated by technical challenge is their curiosity about technology. They enjoy exploring computer systems, solving problems, and understanding how things work.

They see hacking as a form of continuous and self-taught learning. They believe that, by challenging their technical skills, they can constantly improve and stay up to date in a constantly evolving field.

Often, hackers motivated by the technical challenge operate within ethical boundaries. They do not intend to cause harm or violate the law; rather, they seek to explore systems and networks in a responsible and ethical manner.

These hackers can participate in activities such as setting up testing laboratories, analyzing vulnerabilities in applications and systems, and participating in ethical hacking competitions or CTFs (Capture The Flag) with the aim of solving technical challenges.

They often engage in online communities or local hacking groups, where they share knowledge, collaborate on technical projects, and discuss topics related to security and technology.

Although their main motivation is the technical challenge, these hackers can make valuable contributions to the information security community. Their ability to identify vulnerabilities and weaknesses in systems can help improve security in general.

Black Hat Hacker: Malicious hackers, commonly referred to as Black Hat Hackers or black hats, are individuals who use their computer skills for illicit and malicious purposes. Unlike their ethical and gray hat counterparts, these hackers engage in activities that violate laws and often seek to obtain personal benefits or cause harm to individuals, organizations, or systems.

Some of the motivations of Black Hat Hackers are economic interests. Their main objective may be the theft of financial information, such as credit card numbers or bank account passwords, with the intention of selling this information on the black market or committing financial fraud.

Some malicious hackers are dedicated to causing damage to computer systems, networks, or websites. They use various techniques, such as denial-of-service (DDoS) attacks, the insertion of malware or ransomware into vulnerable systems, or the theft and destruction of valuable data.

Obtaining confidential information, trade secrets, or government data is another common motivation for Black Hat Hackers. This information can be used for espionage purposes or to gain competitive advantages.

Sometimes, malicious hackers seek personal revenge. They use their computer skills to cause harm in retaliation for personal, professional, or ideological reasons.

Black hat hackers employ a wide range of techniques and tools to carry out their illegal activities. This includes the use of malware (such as viruses, Trojans, and ransomware), the exploitation of vulnerabilities in software or systems, phishing to deceive individuals and gain access to their accounts, as well as social engineering to manipulate individuals and obtain confidential information.

Grey Hat Hackers (Gray Hat Hackers): Gray hat hackers are individuals who operate in an intermediate space between ethical hackers (White Hat Hackers) and malicious hackers (Black Hat Hackers). Their approach is characterized by a mixture of intentions, which makes their position less clear in ethical terms. Some of their motivations may be, for example, the discovery of vulnerabilities; gray hat hackers share with ethical hackers the motivation to discover vulnerabilities and

weaknesses in systems and applications. However, unlike ethical hackers, they can carry out these activities without the explicit consent of the affected organizations.

Gray hat hackers often seek to expose the vulnerabilities they discover so that system owners can take corrective measures. This is known as “responsible disclosure” and is intended to improve cybersecurity rather than exploit vulnerabilities.

Some gray hat hackers may request rewards or recognition for vulnerability disclosure. This may include monetary rewards or public mentions for their contribution to security.

Gray hat hackers can have variable ethical boundaries. Although their primary intention is to improve security, the ambiguity in their actions can lead to certain ethical controversies.

They use techniques similar to those of ethical hackers to identify vulnerabilities in systems and applications. This can include security scanning, penetration testing, and code analysis.

The legality of the actions of gray hat hackers can vary depending on the jurisdiction and the specific circumstances. While some may operate within the limits of the law, others may be in a legal gray area.

Despite the ethical ambiguity, gray hat hackers play an important role in improving security. Their ability to identify and report vulnerabilities helps organizations strengthen their cyber defenses and protect end users.

Hacktivists: Hacktivists are individuals or groups that combine hacking skills with political, social, or ethical motivations to carry out online actions that seek to promote social or political change. The term “hacktivism” derives from the combination of the words “hacking” and “activism”.

They are shown to be motivated by a variety of causes, which can include freedom of expression, online privacy, the fight against censorship, social justice, government transparency, and many others. Their online actions are usually aligned with their beliefs and political or social objectives.

They use a variety of hacking techniques to achieve their objectives, which may include website defacement, the disclosure of confidential information, the carrying out of denial-of-service attacks (DDoS), and other actions aimed at drawing attention to their causes.

Hacktivists often communicate publicly through online channels, such as websites, forums, social media, and press releases, to explain their motivations and objectives. They may also use hacktivism as a way to attract media attention and generate public discussion about the issues that concern them.

Notable hacktivist groups include Anonymous, WikiLeaks, and LulzSec. These groups have carried out significant online actions that have impacted politics and online security.

Hacktivism is a controversial field because hacktivists’ actions can be perceived as illegal and ethically questionable by some, while others regard them as defenders of freedom and justice. Perceptions of the legitimacy of hacktivism vary according to circumstances and individual perspectives.

Hacktivists may face legal consequences for their activities, including charges of hacking, data theft, online vandalism, and other cybercrimes.

Profile of the Organized Cybercriminal

The Organized Cybercriminal is a profile that stands out in the world of cybercrime due to their participation in criminal groups with a defined organizational structure and their focus on obtaining financial gain through illicit online activities.

In contrast to individual or amateur cyber actors, the Organized Cybercriminal is integrated into criminal groups that usually have a hierarchical structure. These groups have leaders, specialists in different areas, and members who perform specific roles in cyber operations.

The main motivation driving these cybercriminals is economic profit. They carry out illegal activities online to obtain significant economic benefits. These activities can range from the theft of financial data and online fraud to the use of ransomware, online extortion, and the sale of stolen information on the black market.

Organized cybercriminals employ a variety of cyber tactics to achieve their objectives. These include the use of social engineering techniques, the creation of advanced malware, targeted phishing attacks, brute-force attacks on passwords, and other methods.

These groups operate with considerable discretion and seek to maintain their anonymity. They employ techniques aimed at hiding their digital footprints and evading detection by authorities and companies specializing in online security.

Many of these Organized Cybercriminal groups operate globally and can carry out their attacks from various locations around the world. This allows them to circumvent national legal restrictions and hinders their tracking and prosecution.

Insider Threat Cybercriminal Profile

The "Insider Threat" (Internal Threat) represents a particularly complex cybercriminal profile, as it involves employees or former employees who possess privileged access to an organization's systems and networks. These individuals commit criminal acts from within the organization, which often makes them difficult to detect. The motivations driving Insider Threats can be diverse. Some may commit criminal acts for financial reasons, such as the theft of confidential data or the sale of information to third parties. Others may have personal motivations, such as revenge against the organization or colleagues.

The Insider Threat is especially challenging to detect, as these individuals often avoid drawing attention. Their illicit activities may appear legitimate at first glance, making them difficult to identify until the damage is already done. Insider Threats often abuse the trust that the organization has placed in them. Such abuse may include misuse of sensitive information, data manipulation, or the creation of intentional vulnerabilities.

The prevention and mitigation of insider threats require specific strategies, such as appropriate oversight of access privileges, the implementation of robust security policies, and training personnel to identify suspicious behaviors.

Profile of the Cybercriminal Motivated by Economic Profit

Cybercriminals motivated by economic profit are individuals or groups that carry out criminal activities online with the primary objective of obtaining financial gain. These cybercriminals use a variety of techniques and strategies to conduct their illegal activities and generate income.

The central motivation of cybercriminals driven by economic gain is to obtain economic benefits. They seek opportunities to steal money, financial data, or valuable information that can be sold on the black market.

These cybercriminals may engage in activities such as identity theft, in which they obtain personal and financial information from victims to commit financial fraud, such as the unauthorized use of credit cards or fraudulent loans.

Ransomware is a common tactic used by financially motivated cybercriminals. They encrypt victims' data and demand a ransom in exchange for the decryption key.

Cybercriminals can carry out online scams, such as phishing schemes, in which they trick people into disclosing confidential information, such as passwords or credit card numbers.

They use a variety of techniques and tools, such as malware, Trojans, viruses, and botnets, to carry out their criminal activities online. These tools allow them to infiltrate systems, steal data, and conduct cyberattacks.

Profit-motivated cybercriminals often sell stolen information on the online black market. This market includes personal data, credit card information, login credentials, and other valuable digital assets.

These activities are illegal and can lead to serious legal consequences if cybercriminals are identified and captured by the authorities. Cybercrime laws vary by jurisdiction, but charges for identity theft, fraud, unauthorized access to systems, and other cybersecurity-related crimes are often filed.

Profile of the Vengeful Cybercriminal

Vengeful cybercriminals are individuals or groups who carry out malicious cyber activities with the main objective of taking revenge on a specific person, company, or entity. These cybercriminals seek to cause harm, disruption, or damage to their targets, and one of the most pernicious and harmful tactics that some of these cybercriminals employ is "revenge pornography".

Revenge pornography involves the non-consensual dissemination of sexually explicit material involving the victim, often with the intention of damaging their reputation, privacy, and emotional well-being. This material is generally shared online through websites, social media, or forums, and often includes the victim's personal information, such as their full name, address, or contact details. This practice, in addition to being immoral and of questionable legality in many places, can have serious emotional and psychological consequences for the victim.

The central motivation of vengeful cybercriminals is revenge. They may feel aggrieved by a previous action or event and seek to harm the responsible party in some way, whether an individual, an organization, or a government entity.

Vengeful cybercriminals often perceive that they have been treated unfairly or that they have suffered harm or losses due to the actions of another party. They consider their actions to be a way of balancing the scales.

They use various tactics and cyber actions to carry out their revenge. These may include the disclosure of confidential information, data theft, online vandalism, denial-of-service attacks (DDoS), and other methods designed to cause harm or damage to their targets.

The targets of vengeful cybercriminals can be diverse. They may target individuals, companies, organizations, or even public figures, depending on their motive and perception of injustice.

Cybercriminal Profile Based on Cyberterrorism

Cyberterrorism-based cybercriminals are individuals or groups that carry out cyber actions with the intention of causing terror, panic, disruption, or significant damage at a political, economic, or social level. These cybercriminals use technology and cyber tactics to achieve their terrorist objectives.

The central motivation of cyberterrorists is to cause fear and alarm in society or in one specific group. They seek to sow chaos and insecurity through their cyber actions.

Cyberterrorism-based cybercriminals often have political, ideological, or religious motivations. Their attacks may be intended to promote their beliefs or agendas, and they often seek to destabilize governments or organizations.

They may also be motivated by the desire to cause economic damage through attacks on critical infrastructure, companies, or financial institutions.

They use advanced cyber tactics, such as denial-of-service attacks (DDoS), intrusions into critical systems, cyber sabotage, and the spread of malware, to achieve their objectives.

The objectives of cyberterrorists can vary widely and include government institutions, critical infrastructures (such as power plants or water systems), companies, religious or political organizations, and any entity they consider relevant to their objectives.

The actions of cyberterrorists can have serious consequences, such as electrical blackouts, loss of critical data, disruptions in essential public services, economic damage and, in extreme cases, loss of human life.

The fight against cyberterrorism often involves cooperation between security agencies and government bodies from different countries. International collaboration is essential to address large-scale cyber threats.

Common characteristics and technical skills

Common characteristics and technical skills are distinctive aspects that are usually found in the profile of numerous cybercriminals. These particularities and skills enable them to carry out their illicit online actions with greater effectiveness and a higher degree of sophistication.

Generally, they possess solid knowledge of computer science and technology, ranging from an understanding of operating systems to networks, Internet protocols, and related software. In addition, they commonly have skills in programming and software development.

Among their main objectives is to keep their identity and location anonymous, for which they use concealment techniques. To this end, they resort to tools such as virtual private networks (VPN), proxies, and anonymity services in order to hide their IP address and make tracing them difficult.

Occasionally, some cybercriminals may acquire knowledge in ethical hacking and employ these skills in an unethical manner.

Social engineering is a recurring technique used by these individuals to manipulate people and obtain confidential information or unauthorized access to systems. They are notable for their expertise in the art of deceiving their victims through psychological tactics to achieve their objectives.

The arsenal of specialized tools and software they employ is diverse and includes malware such as viruses, Trojans, ransomware, and botnets, among others. These tools enable them to infiltrate systems, steal information, or cause damage.

They are highly adaptable and spare no effort in changing their tactics and techniques in order to avoid detection and remain a step ahead of security measures.

They assiduously search for new vulnerabilities in software and systems that can be exploited to gain unauthorized access or cause damage.

Some cybercriminals are members of online communities in which they share knowledge, tools, and strategies. These communities can serve as learning and collaboration environments for refining their skills and techniques.

It is important to note that not all cybercriminals possess these characteristics to the same extent, and some may have more specialized skills than others. Furthermore, as technology and cyberspace constantly evolve, the skills and tactics of cybercriminals adapt and evolve to address new circumstances and challenges. Additionally, it is relevant to highlight that artificial intelligence

has become an ally that enhances their attacks and allows them to perfect their techniques.

Factors Influencing Their Choice of Objectives

Cybercriminals can select their targets online based on various factors that offer them opportunities to carry out their attacks successfully or that align with their specific motivations.

Cybercrime is a dynamic and diverse field, and the factors influencing target selection may vary depending on the type of crime and the individual motivations of cybercriminals.

Some of the factors that influence their choice of objectives are:

Value of Information: They seek targets that host valuable information, such as personal, financial, or commercial data. Companies, government organizations, and e-commerce websites are often attractive targets due to the amount of confidential data they handle.

Technical Vulnerabilities: They seek to exploit vulnerabilities in systems and networks to gain unauthorized access. Targets with outdated systems or that lack security measures are more susceptible to attacks.

Profit Potential: Many cybercriminals are motivated by economic benefits and, therefore, choose targets that provide opportunities to obtain financial gains. This can include e-commerce websites, online banks, or online payment systems.

Ideological or Political Motivations: Some may have political or ideological motivations and select targets that are related to their beliefs or that they consider representative of a particular cause. In such cases, they may target websites of government, corporate, or specific organizations.

Impact and Recognition: They may choose targets that allow them to cause a significant impact or that grant them recognition within the hacker community. Attacks on popular websites or critical systems can increase their reputation among their peers.

Extortion Opportunities: Some use ransomware to hijack data or systems and then demand a ransom for their release. They choose targets that can pay the ransom and that have critical information or systems that victims need to recover urgently.

Search for Sensitive Information: They may seek specific information, such as trade secrets, intellectual property, or confidential data that they can sell or use to blackmail the victim.

Risk and Probability of Detection: They assess the risk associated with their objectives and select those that have a lower probability of being detected and tracked by authorities or cybersecurity experts.

Motivations for Hacktivism: Targets may be selected with the aim of promoting a cause or making a political statement. They may direct their attacks against websites or systems related to government institutions, corporations, or groups they consider opposed to their ideologies.

Differences and Similarities with Other Types of Offenders

The characteristics and motivations of cybercriminals can differ significantly from those of other types of criminals who operate in the physical world. Below are some differences and similarities between cybercriminals and other types of traditional criminals:

Differences

Scope of Operation: Cybercriminals operate mainly in cyberspace, using computer technologies and networks to carry out their attacks. On the other hand, traditional criminals usually commit crimes in the physical world, such as theft, assault, or vandalism.

Identity and Anonymity: Cybercriminals can hide their identity and location through online anonymity techniques, which makes it difficult for authorities to track them. In contrast, traditional criminals are more easily identified and arrested by police.

Scale and Scope: Cybercriminals can operate on a global scale and carry out massive attacks that affect a large number of victims in different parts of the world. Traditional criminals, by contrast, tend to operate locally and affect a more limited number of victims in a specific location.

Nature of the Crime: Cybercriminals typically commit crimes in a virtual manner, such as data theft, online fraud, and ransomware attacks, among others. Traditional criminals commit physical crimes, such as armed robbery, assault, and vandalism, among others.

Technical Skills: Cybercriminals require technical skills in computing and technology to carry out their online attacks. Traditional criminals, on the other hand, may rely more on their physical strength or traditional tactics to commit crimes.

Similarities

Criminal Motivations: Despite differences in the nature of crimes, both cybercriminals and traditional criminals may be motivated by obtaining economic benefits, power, recognition, revenge, among other reasons.

Acquisition of Benefits: Both cybercriminals and traditional criminals seek to obtain benefits from their criminal actions. These benefits can be economic, social, or emotional.

Search for Opportunities: Both cybercriminals and traditional criminals seek opportunities to commit crimes. Cybercriminals look for vulnerabilities in systems and networks, while traditional criminals look for suitable times and places to carry out their actions.

Risk and Probability of Detection: Both cybercriminals and traditional criminals assess the risk associated with their actions and select targets and methods that minimize the probability of being detected and captured.

Although important differences exist between cybercriminals and traditional criminals, both groups share certain criminal motivations and strategies for achieving their objectives. Cybercrime is a form of crime that has become increasingly prominent in the digital era, and its constantly evolving nature presents unique challenges for law enforcement authorities and cybersecurity experts.

Trends and Behavior Patterns

Trends and behavioral patterns in cybercrime are dynamic and change because of the constant evolution of technology, security policies, and the response of authorities. However, some general trends and patterns have been observed in the world of cybercrime in recent years:

Rise of Financial Cybercrime: Financially motivated cybercrime remains a leading trend in cybercrime. Attacks aimed at stealing financial data, committing online fraud, distributing ransomware, and carrying out scams continue to increase because of their lucrative potential.

Cyberattacks on Critical Infrastructure: There has been a significant increase in cyberattacks targeting critical infrastructure, such as energy, transportation, healthcare, and government systems. These attacks can have devastating consequences for national security and the economy.

Increase in Ransomware Attacks: Ransomware attacks have grown considerably. Cybercriminals use ransomware to lock systems and demand cryptocurrency ransoms in exchange for the release of hijacked data or systems.

Use of Artificial Intelligence and Automation: Cybercriminals are increasingly employing artificial intelligence and automation technologies to carry out more sophisticated and extensive attacks. AI can be used to identify vulnerabilities, automate phishing attacks, and adapt strategies based on the victim's response. This creates an additional challenge for cybersecurity, since defenses must also use AI to combat these threats.

Social Engineering Threats: Social engineering remains among the most effective tactics in the arsenal of cybercriminals. The use of psychological manipulation techniques to deceive people and gain access to confidential information or passwords remains a major concern.

Expansion of the Internet of Things (IoT): The growing adoption of Internet-connected devices, such as cameras, thermostats, and smart appliances, has opened new possibilities for IoT attacks and the creation of botnets.

Cloud Attacks: With the massive migration of data and services to the cloud, cybercriminals are also focusing their attacks on cloud platforms.

Identity Falsification and Identity Theft: Identity theft and the use of stolen personal data to commit crimes continue to pose a significant threat to individuals and organizations.

Focus on Zero-Day Vulnerabilities: Cybercriminals are increasingly interested in exploiting zero-day vulnerabilities, which are security flaws unknown to the manufacturer and therefore do not have an available security patch.

In the Allianz risk report, which ranks the most important corporate concerns, "ranked by 2 712 risk management experts from a record 94 countries and territories," the top concerns for companies globally, for the second consecutive year, are cyber incidents and loss of profits, both representing 34% of all responses.

Among the main risks of our country, cybercrimes are identified as No. 1 in the ranking in that report.

Figure 1. Risks in Argentina

Top risks by region

Top 10 risks in Argentina

Source: Allianz Global Corporate & Specialty

Figures represent how often a risk was selected as a percentage of all responses for that country
Respondents: 17. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*	41%	*2 (32%)*	↑
2	Climate change *(e.g. physical, operational and financial risks as a result of global warming)*	24%	*5 (19%)*	↑
2	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	24%	NEW	↑
2	Fire, explosion	24%	*3 (29%)*	↑
5	Business interruption *(incl. supply chain disruption)*	18%	*1 (58%)*	↓
5	Political risks and violence *(e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)*	18%	*3 (29%)*	↓
5	Shortage of skilled workforce	18%	NEW	↑
8	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	12%	*7 (16%)*	↓
8	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	12%	NEW	↑
8	Natural catastrophes *(e.g. storm, flood, earthquake, wildfire, extreme weather events)*	12%	*5 (19%)*	↓

Analysis of cyberattack cases

The analysis of cyberattack cases is a fundamental part of understanding how cybercriminals operate and what techniques they use to carry out their actions. Studying real cases of cyberattacks allows identifying patterns, exploited vulnerabilities, and possible mitigation measures. Below are some examples of notorious cyberattack cases that have occurred in the past:

Hacking of the National Directorate of Migration

In September 2020, the National Directorate of Migration (DNM) of Argentina was the target of a cyberattack that used a type of malware known as Netwalker ransomware. This malware encrypted the DNM's systems and demanded a ransom initially of 76 million dollars, which was later reduced to 2 million and then to 4 million dollars, requesting payment in bitcoins, a cryptocurrency that allows untraceable transactions. Instead of giving in to the attackers' demands, the DNM chose to file a complaint with the judicial authorities.

As a result of the cyberattack, cybercriminals made public a score of stolen folders on the "Deep Web". Although some of the file names suggested the possible presence of sensitive information, the DNM denied that the leak compromised the security of the Federal Intelligence Agency (AFI) or other government agencies. The Specialized Prosecution Unit for Cybercrime (UFECI) collaborated in the investigation efforts aimed at identifying those responsible for the attack.

The incident gave rise to various hypotheses, including the possibility that the attack was intended to expose vulnerabilities, manipulate or damage data, or facilitate the commission of a conventional crime. In addition, there was speculation about the existence of possible deficiencies in the system's security or the involvement of a disloyal employee in introducing the ransomware, although until that time there was no conclusive evidence in this regard.

The stolen files covered a variety of information, including documents related to embassies such as those of the United States, Mexico, and Romania, as well as Interpol data and AFI requests. The DNM stated that, prior to the leak, it had notified the relevant agencies about the information that could be disclosed and that it did not represent a threat to intelligence security.

Hacking of RENAPER

In October 2021, a concerning leak of personal data involving Argentine citizens occurred, in which a user accessed the database of the National Registry of Persons (Renaper) and published sensitive information, including documents with photos and procedure numbers. This individual claimed to possess data on the 45 million Argentines. Although the Government identified unauthorized accesses to the Renaper database from a user at the Ministry of Health, it has not yet

confirmed whether all the information was downloaded.

The file containing these data is in “json” format and was published on an online forum used by cybercriminals for transactions involving stolen information. To date, it has received around 15 000 views. The user also demonstrated that they possessed information from documents of famous personalities, such as politicians and celebrities, and shared these data on a Twitter account.

The Government suspects that the improper access was carried out using VPN (Virtual Private Network) credentials between Renaper and the Ministry of Health, which led to ruling out the hypothesis of a massive hack in favor of considering an unauthorized access for illicit purposes. In response, access from the Ministry of Health to the Renaper database was blocked.

The internal investigation points to a limited number of individuals with high-level security credentials, although the possibility of remote access from outside the Ministry of Health using a masked IP has not been ruled out.

The user who stole the data threatened to publish more information and offered to sell the entire database for a considerable sum in bitcoins. This case is significantly broader than the leak to the Dirección Nacional de Migraciones that occurred the previous year.

Hacking of Rapipago

Two companies linked to Rapipago, Gire Soluciones and Ducit, suffered cyberattacks of the “ransomware” type. Gire Soluciones, dedicated to business payment management and owner of Rapipago, reported that they detected the activation of malware on 7 December 2022. This malware mainly affected the systems used to provide services to financial entities and encrypted sensitive data.

The attackers demanded a ransom to return control of the hijacked information, a common practice in this type of situation. Although Gire Soluciones assured that there was no indication of a data leak and that they have encryption methods to safeguard critical information, the risk persists.

Cybersecurity experts advise against paying ransoms, as they do not guarantee data recovery and can lead to additional payments. Instead, restoring the security of the compromised network is recommended to prevent future attacks.

Cyberattack on pharmacies affects millions in Argentina

An extortion-related cyberattack affected the system that validates medication discounts in pharmacies in Argentina, leaving millions of users in a difficult situation. The attack targeted the system that handles prepaid health insurance transactions and online validation services through Farmalink, affecting more than

20 social health insurance organizations. The company responsible, Bizland, reported that although no sensitive user data were compromised, the operation of its communications network was affected, preventing the online validation of healthcare consumption.

Although a prompt solution was expected, the system has not been fully restored. As a result, beneficiaries of social programs cannot receive the corresponding discounts on their medications. Although not all prepaid health plans and social security health schemes were affected, some of the largest in the Buenos Aires Metropolitan Area are experiencing difficulties. The Cámara de Farmacias de Córdoba has provided instructions to ensure manual service continuity until the situation is resolved.

Bizland managed to restore the storage system without compromising patient data. In this context, pharmacists are forced to record transactions manually and subsequently request that health service providers recognize the discounts for pharmacies. The magnitude of the cyberattack highlights the vulnerability of health systems to cyber threats, and the situation remains under investigation by the relevant authorities.

Hacking of INTA

The Instituto Nacional de Tecnología Agropecuaria (INTA) has been the target of a significant cyberattack that began in late April 2023. This ransomware attack, in which hackers blocked access to INTA’s systems and demanded a ransom of 2.5 million dollars, has had serious repercussions for the institution’s operations.

INTA authorities took immediate measures to address the situation. Security protocols were activated, and a contingency management team was formed in collaboration with cybersecurity experts and the Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de la Nación. Notably, this is not the first attack of this nature that INTA has faced; a similar incident took place in March of the previous year, although this time it was more aggressive and affected multiple services.

The severity of the incident led INTA to decide to suspend all its institutional IT services until the situation is completely under control and security is guaranteed. This measure is understandable, given that INTA is a complex institution that provides services to a vast network of more than 400 points throughout the country and to approximately 7000 people.

The cyberattack on INTA reflects the growing threat of cyberattacks in Argentina and the region. According to recent reports, Argentina leads the region in terms of cyberattacks, with an average of 2 052 attacks per week. This incident highlights the importance of cybersecurity and the need for greater collaboration between the public and private sectors to effectively address current cyber threats.

Cyberattack on the CNV

In a hack of the Comisión Nacional de Valores (CNV), the hacker group Medusa stole 500 000 confidential files that include data from banks, companies, and internal procedures. This theft was carried out through a ransomware operation in which 1,5 terabytes of CNV data were hijacked and a ransom of $500 000 was demanded. The leaked information, now available on the "dark web," contains records, emails, sanctions, fines, and details of cybersecurity campaigns and has been shared through messages on social networks, especially Telegram. The CNV had reported the attack and stated that it had preserved all its information thanks to preventive measures against cyberattacks. The leaked information includes internal databases, financial documents, complaints, hearing recordings, and private documents of CNV employees. Despite the initial threat to sell the information in parts, Medusa ultimately made it public. The CNV filed a complaint with the Unidad Fiscal Especializada en Ciberdelincuencia and has not yet expanded the complaint or provided further details due to the sensitive nature of the investigation.

These are only a few examples of cyberattacks that have significantly affected the security and privacy of individuals and organizations in our country. The analysis of these cases, together with other cyber incidents, enables cybersecurity experts and authorities to understand the tactics employed by cybercriminals and to develop strategies to prevent and mitigate future attacks.

Methods of Evasion and Detection Avoidance

Cybercriminals undoubtedly employ various strategies to evade detection by security systems and cybersecurity tools. These tactics are deployed to maintain a low profile, prolong their presence in compromised systems, and hinder the identification and attribution of their attacks. Among the most recurrent methods of evasion and detection avoidance, the following stand out:

- Code Obfuscation: They resort to obfuscation techniques to make it more difficult for detection and analysis tools to understand malicious code. Obfuscation can modify the appearance and structure of the code to conceal its true purpose.
- Polymorphism and Metamorphism: These strategies entail altering the appearance or behavior of malware in each infection instance, thereby complicating its detection and analysis by security solutions that rely on predefined signatures.
- Use of Anonymity Technologies: Cybercriminals can employ technologies such as virtual private networks (VPNs), onion networks (e.g., Tor), and proxy services to mask their location and IP address, thereby complicating their tracking and identification.
- Use of Botnets: Cybercriminals can leverage bot networks (botnets) to execute distributed attacks and disperse malicious activity across various devices and locations, which considerably complicates their detection.
- Zero-Day Attacks: Zero-day attacks exploit vulnerabilities previously unknown to both manufacturers and the security community. By using these previously unidentified vulnerabilities, cybercriminals avoid detection by conventional security solutions that lack protective measures for such weaknesses.
- Targeted Attacks and Spear Phishing: Targeted attacks are customized for specific targets, which complicates their detection by more generic security solutions. Spear phishing, by contrast, focuses on specific individuals or employees within an organization in order to deceive them and gain access to highly sensitive systems.
- Traffic Masking: To evade inspection of malicious content by security solutions, cybercriminals use traffic masking techniques, such as encryption of communications, to hinder the detection of harmful content in transmissions.
- Use of Stolen Credentials: In their strategies, cybercriminals can obtain stolen credentials, such as usernames and passwords, to access systems without raising suspicion and to bypass security measures.

The continuous evolution of the tactics and techniques employed by cybercriminals underscores the pressing need to establish a comprehensive cybersecurity strategy. Such a strategy must include regular system updating and patching, user training in safe practices, and the implementation of advanced detection tools and behavior-based security solutions. Furthermore, it is crucial to foster collaboration among the security community, organizations, and authorities, as such collaboration is essential to address the growing sophistication of cybercrime.

Use of Social Engineering Techniques and Psychological Manipulation

The use of social engineering tactics and psychological manipulation constitutes a frequent and effective strategy employed by cybercriminals to obtain confidential information, gain unauthorized access to systems, and persuade individuals to carry out actions that benefit the attackers. These tactics exploit trust, curiosity, fear, and other psychological aspects of people. Examples of social engineering techniques include:

- Phishing: Cybercriminals send fraudulent emails that impersonate legitimate entities, such as banks, online services, or well-known companies. These emails often contain malicious links or attachments with malware and seek to persuade recipients to disclose personal information or login credentials.
- Social Engineering on Social Networks: Cybercriminals can use information obtained from social media profiles to personalize their phishing attacks or to carry out targeted attacks. They can also create fake profiles to establish trusting relationships with potential victims.
- 1. Pretexting: Cybercriminals invent a false situation or scenario to obtain information from a person or to induce them to perform certain actions. They may impersonate colleagues, suppliers, or authorities to obtain confidential data or access to protected systems.
- Vishing: This technique involves manipulating people through phone calls. Cybercriminals can impersonate representatives of legitimate services to obtain personal or financial information from victims.
- Spear Phishing: This form of phishing is targeted at specific individuals or small groups, which makes it more difficult for automated security solutions to detect. Spear phishing emails and messages are personalized to appear legitimate and are tailored to the interests and roles of the victims.
- Baiting: Cybercriminals leave infected storage devices, such as USB drives, in locations where potential victims will find them. Curiosity leads people to connect these devices to their computers, allowing malware to spread.
- Quid Pro Quo: Cybercriminals offer something valuable in exchange for information or access. For example, they may offer technical assistance or discounts to obtain login credentials.

These social engineering and psychological manipulation techniques demonstrate how cybercriminals can exploit human aspects to achieve their objectives. It is important for individuals to be aware of these tactics and to educate themselves on how to identify and avoid becoming victims of social engineering attacks. Awareness and cybersecurity training are essential to protect against these threats.

Cyberterrorism and online radicalization

Cyberterrorism and online radicalization are concerning and closely related phenomena that have emerged alongside the growing dependence on technology and social media in contemporary society. These 2 concepts have a substantial impact on global security and stability and warrant particular attention; they are topics that require a multidisciplinary approach to be adequately addressed. Efforts to counter them must include cybersecurity measures to prevent attacks, as well as strategies to counter propaganda and disinformation disseminated by extremists online. Each term is explained below:

Cyberterrorism

In the field of cyberspace, as with the definition of cybercrime, no universal consensus has been reached regarding the understanding of the concepts of terrorism and cyberterrorism; this definition is also subject to various interpretations.

The term cyberterrorism has evolved from a broader approach that includes any online terrorist activity to more specific conceptions. These variations in conceptualization have been the subject of debate in the academic and security communities. Some experts refer to the more restricted notion of cyberterrorism as “pure cyberterrorism”.

This more restrictive definition considers cyberterrorism a criminal act that relies on digital technology and whose fundamental objective is to generate fear, intimidate, or coerce a government or a specific population, with the intention of causing or threatening to cause physical or material damage, such as sabotage.

Cyberterrorism encompasses the use of technology and cyberspace to carry out terrorist acts or to support, promote, and facilitate activities of a terrorist nature. Cyberterrorists employ cyber tactics that include attacks on websites, disruptions to online services, dissemination of terrorist propaganda, and infiltration of critical computer systems. Their main purpose is to incite fear or panic or to cause harm to individuals or communities.

Characteristics of Cyberterrorism

Cyberterrorism is characterized by the following facets:

Use of Cyber Techniques to Spread Terrorist Ideology and Propaganda: Cyberterrorists exploit digital tools to promote and spread their terrorist ideology and propaganda, reaching a global audience through online platforms.

Attacks on Critical Infrastructures: They target vital infrastructures, such as electrical grids, financial systems, or transportation networks, to disrupt their operations and cause significant harm to society.

Use of Online Media for Recruitment and Radicalization: Online platforms are used to recruit new followers and radicalize individuals, thereby propagating extremist and terrorist beliefs.

Coordination and Planning on Online Platforms: Cyberterrorists use online media to coordinate and plan terrorist activities, which allows them to operate more covertly and in a more organized manner.

Online Radicalization

Online radicalization is the process through which individuals adopt extremist or violent ideas and beliefs via online platforms and social media. Extremists use social media and other virtual spaces to spread propaganda, recruit followers, and facilitate the radicalization of individuals in different parts of the world.

Characteristics of Online Radicalization

Online radicalization is characterized by the following facets:

Use of Propaganda and Persuasive Messages: The dissemination of propaganda and persuasive messages is employed to attract and radicalize vulnerable individuals, leveraging the influence of such content online.

Creation of Online Echo Chambers: Online communities are created that reinforce and validate extremist beliefs, creating an environment in which radicalized individuals feel supported and justified in their beliefs.

Dissemination of Radical Content on Social Media Platforms: Social media platforms are used as dissemination channels for radical and extremist content, enabling it to reach a broad and diverse audience.

Use of Social Engineering Techniques: Extremists employ social engineering techniques to attract and recruit followers, manipulating individual psychology and exploiting vulnerabilities.

Links Between Cybercrime and Cyberterrorism

The links between cybercrime and cyberterrorism are constantly evolving because of the dynamic nature of cyberspace and the activities carried out within it. Although cybercrime and cyberterrorism have different objectives and motivations, there are areas of overlap and possible connections that require detailed understanding to effectively address cyber risks and threats. Some of the links and connections between both areas are:

Use of Similar Techniques and Tools: Both cybercriminals and cyberterrorists use similar techniques, such as malware, phishing attacks, social engineering, and other cyber tactics, to achieve their objectives. Both groups can exploit vulnerabilities in systems and networks to gain unauthorized access.

Financing and Resources: cybercrime can provide sources of financing and resources to cyberterrorist groups. Cybercriminals can carry out illegal activities, such as data theft or extortion, to obtain funds that can then be used to finance terrorist activities.

Radicalization and Propagation of Ideas: some cybercriminals can be recruited or radicalized

online, which turns them into supporters or active members of cyberterrorist groups. Furthermore, cybercrime can be used to propagate extremist ideology and the propaganda of terrorist groups online.

Hybrid Threats: there is the possibility that terrorist groups may turn to cybercriminals to carry out cyber operations on their behalf, leveraging their technical expertise and knowledge in cyberspace.

Cyberterrorism as a Means of Attack: some cyberterrorists may use cyberattacks as part of their terrorism strategies, targeting critical infrastructures, financial systems, or communications networks to cause panic, disruption, and damage.

Although there may be connections between cybercrime and cyberterrorism, both phenomena are distinct and must be addressed separately.

How cybercriminals become radicalized

The radicalization of cybercriminals is a complex process that may involve various factors and circumstances. Not all cybercriminals become radicalized, and radicalization may vary depending on each individual and their context. However, some common factors that may contribute to the radicalization of cybercriminals include:

Extremist Ideology: Some cybercriminals may be attracted to extremist ideologies that promote violence or subversion. Exposure to radical online discourse and propaganda can influence their way of thinking and acting.

Search for Recognition and Belonging: For some cybercriminals, radicalization may be related to the search for recognition and belonging to one online group or community. The feeling of being part of something larger can lead them to adopt extremist ideologies and engage in criminal actions to gain recognition within that group.

Social or Political Discontent: Cybercriminals may feel discontented with society or the political system and use cybercrime as a way to express their frustration and challenge the status quo.

Peer Influence: Interaction with other cybercriminals or online extremists can play an important role in radicalization. Peer influence can reinforce and validate extreme beliefs and encourage participation in criminal activities.

Pursuit of Adventure or Excitement: Some cybercriminals may be drawn to the excitement and challenge of engaging in criminal activities online. Cybercrime provides them with an outlet to test their technical skills and feel empowered by the anonymity offered by cyberspace.

Psychological Factors: Certain cybercriminals may have psychological vulnerabilities that make them more susceptible to radicalization. The pursuit of purpose and identity online can satisfy unmet emotional and psychological needs.

The radicalization of cybercriminals does not always follow a linear pattern and may vary in each case. Furthermore, social media and online platforms can play a crucial role in the spread of extremist ideas and the radicalization of individuals.

Implications for national and international security

The implications of the radicalization of cybercriminals for national and international security are significant and multifaceted. The convergence between cybercrime and ideological extremism poses complex challenges and requires a comprehensive and coordinated response at the global level.

Some of the implications include:

Cybersecurity Threat: The radicalization of cybercriminals can lead to an increase in the number and sophistication of cyberattacks. Cyberterrorists and extremists may use their technical skills to carry out cyber operations targeting critical infrastructure, communications networks, and financial systems, which represents a threat to the cybersecurity of countries and organizations.

Hybrid Attacks: The combination of cyber skills and extremist motivations can lead to hybrid attacks, where cybercriminals seek to combine online and offline actions to maximize the impact and spread of their message.

Cross-Border Radicalization: Cyberspace allows extremist ideas to spread beyond national borders. Online radicalization can easily cross geographic barriers and lead to the creation of terrorist cells and followers in different parts of the world.

Difficulty in Attribution: The anonymous and decentralized nature of cyberspace makes the attribution of attacks and extremist activities more challenging. Identifying those responsible behind cyber operations and radical activities may require strong international cooperation and the use of advanced intelligence tools.

Impact on Stability and International Relations: Cyberattacks and online extremist activities can have a significant impact on the political, social, and economic stability of countries and can generate tensions between nations.

Challenge for International Cooperation: The fight against the radicalization of cybercriminals and cyberterrorism requires close cooperation among countries and international organizations. The exchange of information and collaboration in law enforcement and intelligence are essential for addressing these challenges globally.

Protection of Privacy and Freedom of Expression: While measures are taken to prevent online radicalization, it is important to balance security with the protection of privacy and freedom of expression in cyberspace. It is crucial to ensure that the solutions adopted do not unduly restrict the rights and freedoms of citizens.

Prevention and Mitigation Strategies

To address cybercrime, cyberterrorism, and their repercussions on national and international security, it is imperative to implement comprehensive prevention and mitigation strategies. These strategies must address technical as well as social and educational aspects.

In this sense, promoting awareness and public education about the risks related to online radicalization and cybercrime plays a fundamental role. Awareness campaigns have the potential to inform individuals about the tactics employed by online extremists while encouraging the safe and responsible use of cyberspace.

Close collaboration between governments and online platforms is essential to address the spread of extremist content on the Internet. Working together to identify and remove radicalized content can contribute significantly to preventing radicalization and recruitment.

In this context, intelligence services play a crucial role in monitoring the online activities of potential cybercriminals and extremists, detecting early signs of radicalization and attack planning. This surveillance enables a rapid and proactive response to potential threats.

Likewise, training citizens and employees of organizations in security and cybercrime awareness can prevent them from falling into social engineering traps and protect against online attacks.

International cooperation is fundamental for addressing the transnational challenges associated with radicalization and cybercrime. Information sharing, collaboration in law enforcement, and collaboration in investigations are crucial elements in the effective fight against these problems.

To prevent radicalization, it is first essential to address the underlying causes, such as social exclusion, discrimination, and inequality. Promoting inclusion and providing opportunities for all citizens can reduce vulnerabilities to radicalization.

The application of advanced technologies, such as data analysis and artificial intelligence, can be useful for identifying patterns of online radicalization and anticipating potential threats before they materialize.

Fostering open and constructive dialogue and debate on political and social issues can provide a means to address extremism and radicalization in a peaceful and democratic manner.

When implementing prevention and mitigation strategies, it is essential to safeguard the privacy and civil liberties of citizens. Security measures must not unduly compromise fundamental rights and freedoms.

Ultimately, addressing cybercrime and its consequences for national and international security requires a coordinated and multidisciplinary response involving governments, organizations, online communities, and citizens. By working together, it is possible to build a secure and resilient cyberspace in the face of the challenges posed by cyberdelinquency and online extremism.

Strengthening Cybersecurity and Protection Measures

The strengthening of cybersecurity and the implementation of protection measures are crucial aspects of mitigating the risks associated with cyber threats in general.

An essential practice is to keep operating systems, applications, and software updated with the latest security patches. This closes known vulnerabilities and prevents cybercriminals from exploiting security gaps.

To safeguard networks and computer systems, tools such as firewalls and intrusion detection systems are fundamental. Furthermore, intrusion prevention systems can block known and unknown cyberattacks in real time, preventing the infiltration and spread of malware.

Monitoring user and system behavior through security solutions can detect anomalous and potentially malicious activities, contributing to the prevention of cyberattacks.

The encryption of confidential data and its secure storage are effective measures to prevent

the exposure of sensitive information in the event of a security breach.

Education on cybersecurity best practices, including the identification of social engineering attacks and the safe use of passwords, is essential for preventing cybercrime.

It is equally vital to have a cyber incident response plan that enables rapid and coordinated action in the event of a security breach.

Conducting vulnerability analysis and penetration testing regularly can identify weaknesses in systems and correct them before they are exploited by cybercriminals.

The protection of critical infrastructures, such as power grids, transportation systems, and emergency services, is of paramount importance due to the serious consequences that their disruption could entail.

Collaboration between organizations and governments, together with the exchange of information on cyber threats and tactics employed by cybercriminals, is essential to be better prepared and to protect oneself.

Finally, investment in cybersecurity and the implementation of best practices are investments that help reduce risk and protect both infrastructure and critical data.

Role of education and awareness in the prevention of attacks

The promotion of awareness and education plays a crucial role in the prevention of cyberattacks and the fight against cybercrime. A well-informed population, aware of risks as well as best practices in cybersecurity, becomes an effective shield against online threats.

Through training programs, people can learn to identify signs of potential cyber threats, such as phishing emails, malicious websites, and suspicious online behaviors.

These programs offer valuable lessons on how to protect personal information and online privacy, emphasizing the use of strong passwords, two-factor authentication, and verification of the authenticity of websites before sharing personal information.

Education on social engineering enables individuals to detect manipulation and persuasion attempts by cybercriminals seeking to obtain confidential information or unauthorized access.

Likewise, the importance of responsibly sharing information on social media is highlighted, and unnecessary exposure of personal data that could be used in social engineering attacks is avoided.

It is essential that people understand the importance of safeguarding their personal data and understand how it is used and shared online.

In addition, training is offered on cyberterrorism and online radicalization, which enables individuals to understand how extremists use cyberspace to spread their ideas and attract followers.

Cybersecurity awareness plays a critical role in organizations by fostering a security culture among employees and protecting the company's data and assets.

Both education and awareness motivate individuals to report suspicious activities or cybercrime incidents to the authorities and to collaborate with the community in preventing attacks.

The promotion of these measures must be a collaborative effort involving governments, educational institutions, organizations, and the private sector, with the aim of creating a more informed and resilient society against cyber threats.

Collaboration between the public and private sectors

Cooperation between the public and private sectors plays a fundamental role in addressing challenges related to cybersecurity, attack prevention, and the fight against cybercrime. These two domains have complementary skills and resources that, when combined, can significantly strengthen cyber protection and the capacity to respond to threats.

This collaboration facilitates the real-time exchange of information on cyber threats and vulnerabilities. Private companies, by being aware of various attacks and tactics employed by cybercriminals, can share such information with government agencies to improve intelligence and incident response.

In this sense, the public sector can leverage the private sector's experience in intelligence analysis and the identification of attack patterns, enabling the detection of emerging trends and threats.

Collaboration in incident response leads to more efficient coordination. Private companies can promptly notify government agencies about attacks, which expedites a more effective response.

In addition to this, cooperation between both sectors can be the catalyst for establishing best practices and cybersecurity standards that have a broader scope, encompassing different sectors and organizations.

The private sector can also play an active role in cybersecurity training and education within the business community, raising awareness of the importance of cybersecurity and attack prevention. Additionally, it can promote research and the joint development of more advanced and effective cybersecurity technologies and solutions.

In the field of critical infrastructure protection, such as electrical grids, financial systems, and emergency services, collaboration between the public and private sectors is essential, since both share responsibility for their operation and protection.

To foster this collaboration, governments can offer incentives and recognition to private companies that adopt robust cybersecurity practices and actively contribute to cyber protection.

It is essential to emphasize that this collaboration must be continuous and sustainable, involving all stakeholders, from small and medium-sized enterprises to large corporations and government agencies. Information sharing, coordination in incident response, and the joint development of solutions are essential to strengthen cybersecurity and to effectively protect society and critical infrastructure against cyber threats and the radicalization of cybercriminals.

FINAL CONSIDERATIONS

Recapitulation of findings

Throughout our research on the analysis of criminal behavior among cybercriminals, we identified significant findings that contribute to understanding the complexity of this emerging phenomenon. These findings are fundamental to obtaining a complete understanding of the dynamics of cybercrime and its relationship with security issues in an increasingly digital world.(84,85)

Among the fundamental findings is the growing convergence between cybercrime and cyberterrorism. The research revealed that some individuals involved in cybercriminal activities can be radicalized online and subsequently used by terrorist groups to carry out cyber operations. This connection poses new challenges for global security and underscores the need to address these problems comprehensively.(86,87,88)

The psychological profiles of cybercriminals are highly diverse. Their motivations range from the pursuit of financial gain to ideological impulses and the mere desire to challenge systems and organizations. These multifaceted profiles highlight the need to understand the diverse motivations behind cybercrime in order to develop effective prevention and mitigation strategies. Cybercriminals select targets based on a series of complex factors, including financial opportunities, the notoriety they would gain by attacking certain organizations, or the personal satisfaction of overcoming security systems.(89,90,91)

The motivations of cybercriminals are varied, ranging from the pursuit of financial gain to the promotion of extremist ideologies or the pursuit of technical challenges. These motivations can influence the type and scale of cyberattacks.(92,93,94)

The widespread use of social engineering techniques is another key finding. Cybercriminals use psychological manipulation and social engineering to deceive individuals and gain unauthorized access to systems or information. Knowledge of these tactics is crucial for protection against such attacks.(95,96,97,98,99)

Our research also highlights the importance of collaboration between the public and private sectors. This joint approach is essential for strengthening cybersecurity and successfully confronting cyber threats.(100,101,102,103) Collaboration enables the exchange of information about threats and tactics used by cybercriminals, resulting in a more effective response.(104,105,106,107,108)

Cybersecurity education and awareness are fundamental pillars in the fight against cybercrime.(109,110,111) Empowering individuals and organizations with solid knowledge of how to identify and prevent cyberattacks is essential. Awareness focuses on the use of secure passwords, two-factor authentication, and verification of the authenticity of websites before personal information is shared.(112,113)

To prevent and mitigate cyberattacks, it is essential to strengthen cybersecurity. This involves keeping systems and software updated with the latest security patches, using tools such as firewalls and intrusion detection systems, and applying encryption practices to safeguard confidential data.

RECOMMENDATIONS

The findings of this research generate a set of significant implications and recommendations

both for the understanding of cybercrime and for the formulation of effective prevention and mitigation strategies. These implications and recommendations emerge from the exploration of cybercriminal profiles, their motivations, the convergence with cyberterrorism, and measures to strengthen cybersecurity.

The results of this research underscore the importance of ensuring that security policies, at both national and international levels, are up to date and reflect emerging threats in cyberspace. Constant adaptation is needed to address the changing motivations of cybercriminals and their evolving capabilities.

Given the identified convergence between cybercrime and cyberterrorism, greater integration and cooperation are recommended among law enforcement agencies, intelligence agencies, and government institutions responsible for cybersecurity and counterterrorism.

The research highlights the need for public education and awareness campaigns that empower individuals and organizations to recognize and respond to cyber threats. Digital literacy and understanding of social engineering techniques are essential components of such campaigns.

Active and continuous collaboration between the public and private sectors is essential for improving cybersecurity. It is recommended that partnerships be established to facilitate information sharing and joint responses to cyber incidents.

Given the rapid evolution of technologies and cybercriminal tactics, continuous research is essential to keep abreast of emerging threats. The academic community and research institutions are urged to dedicate resources to exploring these topics.

The research underscores the importance of protecting critical infrastructures, such as electrical grids and financial systems. Greater investment in cybersecurity for these vulnerable areas is recommended.

In developing cybersecurity policies and strategies, a balance must be ensured between protection against cyber threats and respect for civil liberties and citizens' privacy.

Implications for cybersecurity and the fight against cybercrime

The analysis of cybercriminal behavior has important implications for cybersecurity and the fight against cybercrime. Through a combination of preventive measures, collaboration among different actors, awareness-raising, and technological development, it is possible to strengthen defense against cyberattacks and protect society and critical infrastructure from online threats.

The completion of this research has revealed a series of significant implications with a major impact on the field of cybersecurity and the fight against cybercrime. The findings obtained provide valuable lessons on how to address cyber threats and strengthen security in the digital environment. The following are the key implications and recommendations derived from this analysis:

The findings highlight the need to adopt a proactive approach when formulating cybersecurity strategies. Rather than reacting to cyber threats after they manifest, it is imperative to anticipate possible scenarios and develop strategies that mitigate risks before they materialize.

The effective fight against cybercrime demands an interdisciplinary approach involving cybersecurity experts, psychologists, sociologists, and intelligence professionals. Understanding the psychological profiles of cybercriminals and their motivations is essential to anticipate and prevent their activities.

Cybersecurity education and public awareness should not be isolated events but ongoing efforts. Continuous training and updates on the latest threats and techniques are essential to keep individuals and organizations aware of constantly evolving threats.

Understanding the criminal behavior of cybercriminals can help identify vulnerabilities and improve cybersecurity strategies. It is crucial to invest in advanced defense technologies and capabilities to protect critical systems and data against cyberattacks.

Collaboration between the public and private sectors is a fundamental pillar for improving cybersecurity. The creation of strong alliances and open communication enables information sharing on threats and tactics, which strengthens response and protection capacities.

Investment in research and development of advanced technologies, such as artificial intelligence and data analysis, is crucial. These technologies can be used to identify patterns of online cybercrime and anticipate threats before they become serious incidents.

The collection and analysis of intelligence on cybercriminal activities can provide valuable information about the tactics, techniques, and procedures used by cybercriminals. This can help anticipate and prevent future attacks.

Advances in cybercrime require updated and robust legal frameworks that effectively address cyber offenses and facilitate international cooperation in the prosecution of cybercriminals.

CONCLUSIONS

The analysis of the criminal behavior of cybercriminals is a complex and relevant topic in today's world, where cybercrime and cyber threats have increased significantly. This research has explored the intersection between cybercrime and cybersecurity and how the study of the criminal behavior of cybercriminals can provide valuable information for preventing and mitigating online attacks.

In the theoretical framework, fundamental concepts related to cybercrime and criminal behavior analysis were highlighted, including psychological theories that can help explain the motivations behind online criminal actions. The psychological profiles of cybercriminals, their common characteristics and technical skills, as well as the factors influencing their target selection, were analyzed.

The motivations of cybercriminals were explored in depth, ranging from financial to ideological, and the importance of understanding these factors for developing effective prevention and mitigation strategies was highlighted.

The implications for national and international security were discussed, highlighting the need for close collaboration between the public and private sectors to address cyber threats and the radicalization of cybercriminals. Education and awareness were also identified as crucial tools for empowering individuals and organizations to protect against and prevent cyberattacks.

Finally, the importance of strengthening cybersecurity and implementing protective measures was highlighted, along with the analysis of cyberattack cases and the use of social engineering techniques and psychological manipulation by cybercriminals.

In conclusion, the analysis of cybercriminal behavior is a constantly evolving field of study; however, it is essential to understand the motivations and tactics behind online criminal actions. Through a multidisciplinary approach, collaboration among different actors, and solid education in cybersecurity, it is possible to strengthen cybersecurity and protect society against cyber threats. Only through joint and proactive efforts can these challenges be addressed and a safer and more resilient cyberspace be ensured for all.

REFERENCES

1. Amenazas Híbridas: Ciberseguridad, Ciberterrorismo y Ciberguerra. Cuadernos de Seguridad. 2022 Jul 28. https://cuadernosdeseguridad.com/2022/07/amenazas-hibridas-ciberseguridad-ciberterrorismo-y-ciberguerra/
2. Allianz Global Corporate & Specialty. Allianz Risk Barometer: Identifying the major business risks for 2023. The most important corporate concerns for the year ahead, ranked by 2,712 risk management experts from a record 94 countries and territories. 2023. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf
3. Allianz Global Corporate & Specialty. Allianz Risk Barometer: Identifying the major business risks for 2023. The most important corporate concerns for the year ahead, ranked by 2,712 risk management experts from a record 94 countries and territories. 2023. p. 18. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf
4. Ámbito Financiero. Hackeo de la CNV: el grupo hacker difundió información tras no recibir el pago de rescate. 2023. https://www.ambito.com/economia/hackeo-la-cnv-el-grupo-hacker-difundio-informacion-no-recibir-el-pago-rescate-n5757458
5. Barbería M. Ataque de hackers: una empresa vinculada a Rapipago que maneja información sensible sobre pagos online sufrió un secuestro virtual de datos. Infobae. 2022 Dec 13. https://www.infobae.com/economia/2022/12/13/ataque-de-hackers-una-empresa-vinculada-a-rapipago-que-maneja-informacion-sensible-sobre-pagos-online-sufrio-un-secuestro-virtual-de-datos/
6. BBVA. En la mente de un cibercriminal. https://www.bbva.com/es/innovacion/en-la-mente-de-un-cibercriminal/
7. Bertoia L. Los hackers publicaron finalmente la información robada a la Dirección Nacional de Migraciones. Página 12. 2020. https://www.pagina12.com.ar/291148-los-hackers-publicaron-finalmente-la-informacion-robada-a-la
8. Cárdenas MJ. Prevención y defensa ante el ciberterrorismo. Lisa News. 2023 Feb 23. https://www.lisanews.org/ciberseguridad/prevencion-y-defensa-del-ciberterrorismo/
9. Campus Ciberseguridad. Tipos de hackers. 2022. https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers
10. Cisco Umbrella. Top 10 Cybersecurity Tips. https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips
11. Code42. 6 Types of Insider Threats. https://www.code42.com/glossary/types-of-insider-threats/
12. Comisión Económica para América Latina y el Caribe (CEPAL). Medidas de ciberseguridad informática. https://biblioguias.cepal.org/c.php?g=495473&p=4398100
13. ComputerWord. Evolucionan las técnicas de evasión de la ciberseguridad. 2017. https://cso.computerworld.es/cibercrimen/evolucionan-las-tecnicas-de-evasion-de-la-ciberseguridad
14. Consejo de Europa. Convenio sobre la ciberdelincuencia, Budapest. 2001 Nov 23. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
15. Derechodelared.com. Hacktivismo: Ciberactivismo ético. https://www.derechodelared.com/hacktivismo-ciberactivismo-etico/
16. Diccionario de la lengua española. Real Academia Española. https://dle.rae.es/
17. Diez R. Ciberseguridad: así atacan los hackers y estos son los ataques más comunes. La Vanguardia. 2022 Dec 19. https://www.lavanguardia.com/tecnologia/20221219/8529724/asi-atacan-hackers-estos-son-ataques-mas-comunes.html
18. DuraLex Sed Lex. Espionaje industrial: qué es y cómo evitarlo? 2021 Dec 30. https://www.duralexsedlex.eu/espionaje-industrial-que-es-y-como-evitarlo/
19. EducacionIT. Ciberdelincuencia y tipos de ciberdelincuentes. https://www.educacionit.com/temario/ciberdelincuencia-y-tipos-de-ciberdelincuentes
20. El Cronista. Amenazas informáticas: por qué las empresas deben invertir más en ciberseguridad. 2022 Nov 18. https://www.cronista.com/negocios/Amenazas-informaticas-por-que-las-empresas-deben-invertir-mas-en-ciberseguridad-20221118-0002.html
21. El Economista. Evolución y consecuencias del cibercrimen. 2021 Dec 27. https://www.eleconomista.com.mx/sectorfinanciero/Evolucion-y-consecuencias-del-cibercrimen-20211227-0019.html
22. El Orden Mundial en el Siglo XXI. Qué es el ciberespionaje? 2019 Jul 24. https://elordenmundial.com/que-es-el-ciberespionaje/
23. El País. El ciberespionaje al servicio de la geopolítica. 2020 May 21. https://elpais.com/tecnologia/2020-05-21/el-ciberespionaje-al-servicio-de-la-geopolitica.html
24. El País. Ciberespionaje y 'hackeo' en el conflicto israelí-palestino: el arma silenciosa de las agencias de inteligencia. 2021 May 13. https://elpais.com/internacional/2021-05-13/ciberespionaje-y-hackeo-en-el-conflicto-israeli-palestino-el-arma-silenciosa-de-las-agencias-de-inteligencia.html
25. El País. Ciberataque al Registro Nacional de Trabajadores Rurales y Empleadores. 2022 Dec 29. https://elpais.com.ar/ciberataque-al-registro-nacional-de-trabajadores-rurales-y-empleadores-n1667638
26. El Poder de la Palabra (E.P.D.L.P.). Definición de "ciberespionaje". https://www.epdlp.com/definicion.php?pal=ciberespionaje
27. El Español. Ciberterrorismo: el arma de destrucción masiva que se activa con un clic. 2020 Jul 22. https://www.elespanol.com/omicrono/tecnologia/20200722/ciberterrorismo-arma-destruccion-masiva-activa-clic/507348746_0.html

28. Europol. EU Cybersecurity Challenge. https://www.europol.europa.eu/activities-services-main/activities/eu-cybersecurity-challenge
29. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2020. 2020. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2020
30. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021. 2021. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2021
31. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2022. 2022. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2022
32. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. 2023. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2023
33. Fernández M. Evolución del cibercrimen: desde los primeros virus hasta el ransomware. 2021 Aug 10. https://www.abc.es/tecnologia/informatica/soluciones/abci-evolucion-cibercrimen-primeros-virus-hasta-ransomware-202108100124_noticia.html
34. Ferré J. Auge y caída de los grupos de ciberactivistas. 2019 Aug 16. https://retina.elpais.com/retina/2019/08/16/tendencias/1565966729_585119.html
35. Fuentes I. Amenazas informáticas: un análisis de los riesgos más graves para la ciberseguridad. OpenAI. 2022 Jan 25. https://openai.com/research/amenazas-informaticas-riesgos-ciberseguridad
36. García F. Guerra cibernética: el nuevo campo de batalla. 2017 Sep 14. https://www.dw.com/es/guerra-ciber-n%C3%A9tica-el-nuevo-campo-de-batalla/a-40501843
37. García JA. Hacktivismo: el ciberactivismo en la red. 2022 Jan 18. https://www.muycomputer.com/2022/01/18/hacktivismo-ciberactivismo/
38. García JJ. Hacktivismo: una forma de activismo digital. 2022 May 23. https://www.huffingtonpost.es/jorge-jimenez-garcia/hacktivismo-una-forma-de-activismo-digital_b_19740188.html
39. Garriga L. La ciberseguridad en la empresa: una necesidad imprescindible. 2019 Jul 29. https://www.abc.es/espana/comunidad-valenciana/abci-ciberseguridad-empresa-necesidad-imprescindible-201907290217_noticia.html
40. Gestión. Los principales ciberataques que afectaron a empresas y gobiernos en 2022. 2022 Jun 9. https://gestion.pe/mundo/los-principales-ciberataques-que-afectaron-a-empresas-y-gobiernos-en-2022-noticia/
41. Global Guardian. Understanding the Differences Between Hacktivism and Cyberterrorism. 2022 Jan 21. https://www.globalguardian.com/blog/understanding-the-differences-between-hacktivism-and-cyberterrorism
42. Goiburu M. Ciberespionaje: cómo funcionan los ataques de espionaje a través de Internet. 2017 Jul 13. https://www.elconfidencial.com/tecnologia/2017-07-13/ciberespionaje-hackers-espionaje-internet_1417513/
43. González G. Qué es el hacktivismo: cómo influye en la sociedad. 2020 Oct 21. https://somoslibros.net/que-es-el-hacktivismo/
44. Gómez M. Ciberterrorismo: el nuevo peligro en el ciberespacio. 2022 Jan 21. https://okdiario.com/tecnologia/ciberterrorismo-nuevo-peligro-ciberespacio-11383616
45. Grupo de Delitos Telemáticos de la Guardia Civil. Cyber Terrorism. https://www.gdt.guardiacivil.es/webgdt/pinformatica/terrorismo_cibernetico/index.html
46. Hidalgo H. Ciberdelincuencia: qué es, tipos, consecuencias y prevención. 2019 Mar 6. https://concepto.de/ciberdelincuencia/
47. Inkrypt. Hacktivismo y la ciberseguridad. https://inkrypt.co/blog/hacktivismo-y-la-ciberseguridad/
48. Insight. Evolución del cibercrimen: desde los primeros virus hasta el ransomware. 2021 May 13. https://www.insight.com/es_ES/content-and-resources/2021/08/evolucion-del-cibercrimen.html
49. Insight. Tipos de ciberataques y cómo protegerse de ellos. 2022 Sep 28. https://www.insight.com/es_ES/content-and-resources/2022/09/tipos-de-ciberataques.html
50. Inteco-Cert. Tipos de ciberdelincuentes. https://www.incibe-cert.es/faqs/incibe-cert/tipos-ciberdelincuentes
51. Internet Society. Qué es el hacktivismo? https://www.internetsociety.org/issues/internet-censorship/hacktivism/
52. Internet Society. Understanding the Modern Hacktivist: Money, Mayhem, or Mischief? 2020 Nov 10. https://www.internetsociety.org/blog/2020/11/understanding-the-modern-hacktivist-money-mayhem-or-mischief/
53. Kaspersky. La historia de los ciberataques: desde los gusanos hasta el ransomware. https://www.kaspersky.com.mx/resource-center/threats/history-of-cyber-attacks
54. Kaspersky. Cibercrimen: concepto, historia, tipos y prevención. 2021 Dec 21. https://www.kaspersky.com.mx/resource-center/threats/what-is-cybercrime
55. Kaspersky. Hacktivismo: concepto, historia, ejemplos y riesgos. 2022 Sep 20. https://www.kaspersky.com.mx/resource-center/threats/what-is-hacktivism
56. La Tercera. Espionaje industrial, la amenaza que acecha a las empresas. 2018 May 30. https://www.latercera.com/pulso/noticia/espionaje-industrial-la-amenaza-que-acecha-a-las-empresas/171475/
57. Larsson L. Cyberspace, Hacktivism, and Civil Disobedience. Science and Engineering Ethics. 2017;23(3):781-797. https://link.springer.com/article/10.1007/s11948-015-9710-6
58. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, núm. 294. 2018 Dec 6. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
59. Mauri L. Ciberseguridad y ciberdelincuencia: retos y desafíos en la era digital. ESADEgeo. 2021 Nov 23. https://www.esadegeo.com/es/ciberseguridad-y-ciberdelincuencia-retos-y-desafios-en-la-era-digital
60. Mauri L. La lucha contra la ciberdelincuencia. ESADEgeo. 2022 Jan 6. https://www.esadegeo.com/es/la-lucha-contra-la-ciberdelincuencia

61. Merkow MS, Breithaupt J. Computer Security Assurance. Journal of Information Systems. 2006;20(2):85–101. https://doi.org/10.2308/jis.2006.20.2.85
62. Ministerio de Asuntos Económicos y Transformación Digital. ¿Qué es el ciberespionaje? https://www.mineco.gob.es/stfls/MICM/Menu/Areasdetrabajo/Ciberseguridad/Ciberespionaje.pdf
63. Molina C. La ciberseguridad en España: retos y amenazas. 2019 Nov 7. https://www.eleconomista.es/investigacion-eleconomista/noticias/10148209/11/19/La-ciberseguridad-en-Espana-retos-y-amenazas.html
64. Molina C. Ransomware: qué es, cómo actúa y cómo protegerse de él. 2020 May 6. https://www.eleconomista.es/tecnologia/noticias/10524413/05/20/Ransomware-que-es-como-actua-y-como-protegerse-de-el.html
65. Molina C. Phishing: qué es y cómo evitar caer en sus redes. 2021 Jun 7. https://www.eleconomista.es/tecnologia/noticias/11269536/06/21/Phishing-que-es-y-como-evitar-caer-en-sus-redes.html
66. Molina C. DDoS: el ataque que tumba los servicios digitales. 2022 Aug 23. https://www.eleconomista.es/tecnologia/noticias/11552270/08/22/DDoS-el-ataque-que-tumba-los-servicios-digitales.html
67. Molina C. Qué es el malware y cómo protegerse de él. 2022 Sep 28. https://www.eleconomista.es/tecnologia/noticias/11815666/09/22/Que-es-el-malware-y-como-protegerse-de-el.html
68. Molina C. Vulnerabilidades de seguridad: qué son y cómo protegerse de ellas. 2022 Oct 18. https://www.eleconomista.es/tecnologia/noticias/11916273/10/22/Vulnerabilidades-de-seguridad-que-son-y-como-protegerse-de-ellas.html
69. Myers MD. Qualitative research in business and management. Sage; 2013.
70. Naciones Unidas. Resolución 75/273 de la Asamblea General. 2021. https://undocs.org/A/RES/75/273
71. Nations Encyclopedia. Cybercrime. https://www.nationsencyclopedia.com/WorldStats/Crime-Statistics-Cybercrime.html
72. Núñez E. Qué es un hacker y cuántos tipos de hackers existen? 2020 Dec 21. https://www.muycomputer.com/2013/12/12/hacker/
73. OCDE. Informe sobre la ciberdelincuencia. 2020. https://www.oecd.org/internet/Informe-sobre-la-ciberdelincuencia.pdf
74. Paredes G. Ciberdelincuencia y ciberseguridad: diferencias y cómo prevenir ataques. 2022 Jan 5. https://www.genbeta.com/seguridad/ciberdelincuencia-ciberseguridad-diferencias-como-prevenir-ataques
75. PC Magazine. Qué es un ataque DDoS (Distributed Denial-of-Service)? https://www.pcmag.com/es/que-es/ataque-ddos-distributed-denial-of-service
76. Pew Research Center. The State of Privacy in America. 2017 Jan 26. https://www.pewresearch.org/internet/2017/01/26/the-state-of-privacy-in-america/
77. Pittaluga F. Ciberdelincuencia y ciberseguridad: diferencias y cómo prevenir ataques. 2022 Jan 5. https://www.genbeta.com/seguridad/ciberdelincuencia-ciberseguridad-diferencias-como-prevenir-ataques
78. Poza JJ. Qué es el ransomware, cómo funciona y cómo evitarlo? ABC. 2020 Jan 21. https://www.abc.es/tecnologia/informatica/soluciones/abci-ransomware-como-funciona-y-como-evitarlo-202001211226_noticia.html
79. Rex D. Cibercrimen y ciberdelincuencia: concepto, tipos y ejemplos. 2019 Dec 8. https://concepto.de/cibercrimen/
80. Rodríguez M. Ciberseguridad y ciberdelincuencia: retos y desafíos en la era digital. ESADEgeo. 2021 May 3. https://www.esadegeo.com/es/ciberseguridad-y-ciberdelincuencia-retos-y-desafios-en-la-era-digital
81. Sabadell B. Principales riesgos de seguridad informática para empresas y cómo prevenirlos. 2023. https://www.bancsabadell.com/cs/Satellite/SabAtl/Principales-riesgos-de-seguridad-informatica-para-empresas-y-como-prevenirlos/6000048086006/es/
82. Secretaría de Estado de Seguridad. Ciberterrorismo. https://www.interior.gob.es/web/servicios-al-ciudadano/ciberterrorismo
83. Security Art Work. Ciberterrorismo. 2019. https://www.securityartwork.es/2019/01/17/ciberterrorismo/
84. SegurInfo. Ciberseguridad. https://www.segurinfo.com/index.php/es/
85. Serrano A. Amenazas en la red: tipos de malware y cómo combatirlos. El País. 2018 Sep 13. https://elpais.com/tecnologia/2018/09/12/actualidad/1536772189_270775.html
86. Smith KW, Rogers MK. The Impact of Terrorism on the Global Economy: Statistical Evidence. Studies in Conflict & Terrorism. 2018;41(3):158–175. https://www.tandfonline.com/doi/full/10.1080/1057610X.2016.1264599
87. Solución Individual. Qué es la ciberdelincuencia y cómo protegerse de ella? https://www.solucionindividual.com/ciberdelincuencia/
88. Suárez-Tangil G, Egele M, Brumley D. Cc: identifying content-foraging malware. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2015. p. 226–246. https://link.springer.com/chapter/10.1007/978-3-319-20550-2_11
89. Tange A. Writing a doctoral thesis using LATEX: Tips, tricks and a template. Studies in Computational Intelligence. 2013;519:19–44. https://link.springer.com/chapter/10.1007/978-3-642-14058-7_2
90. Techopedia. Hacktivism. https://www.techopedia.com/definition/6522/hacktivism
91. Torres JA. Ciberespionaje: técnicas y tácticas utilizadas por los ciberespías. 2022 Aug 15. https://www.muyseguridad.net/2012/08/15/ciberespionaje-tecnicas-tacticas-utilizadas-ciberespia/
92. Unidad de Investigación Tecnológica. Ciberterrorismo. https://www.policia.es/ujit/ciberterrorismo.html
93. UNODC. Comprehensive Study on Cybercrime. 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
94. U.S. Department of Justice. National Strategy for Countering Domestic Terrorism. 2022. https://www.justice.gov/ag/page/file/1495171/download
95. U.S. Department of State. Country Reports on Terrorism 2018. 2019 Apr 25. https://www.state.gov/wp-content/uploads/2019/04/2018-Country-Reports-on-Terrorism-Full-Report.pdf

96. U.S. Department of State. Country Reports on Terrorism 2020. 2021 Apr 20. https://www.state.gov/wp-content/uploads/2021/04/Country-Reports-on-Terrorism-2020.pdf
97. U.S. Department of State. Country Reports on Terrorism 2021. 2022 Mar 31. https://www.state.gov/wp-content/uploads/2022/03/Country-Reports-on-Terrorism-2021-FINAL-2022.03.31.pdf
98. Valdés A. Ciberterrorismo: una amenaza en aumento. 2022 Jan 6. https://www.tekcrispy.com/2022/01/06/ciberterrorismo-amenaza-aumento/
99. Vila A. Qué es el ransomware? Claves, tipos y cómo protegerse. Xataka. 2019 Dec 16. https://www.xataka.com/basics/que-es-ransomware-claves-tipos-como-protegerse
100. Vila A. Phishing: cómo funciona, cómo protegerse y a quién recurrir si has sido víctima. Xataka. 2021 Jun 23. https://www.xataka.com/basics/phishing-como-funciona-como-protegerse-a-quien-recurrir-si-has-sido-victima
101. Vila A. Cibercrimen: qué es, cómo funciona y cómo protegerse. Xataka. 2022 Feb 16. https://www.xataka.com/basics/cibercrimen-que-es-como-funciona-como-protegerse
102. Vila A. DDoS: qué es un ataque de denegación de servicio y cómo protegerse. Xataka. 2022 Mar 28. https://www.xataka.com/basics/ddos-que-es-ataque-denegacion-servicio-como-protegerse
103. Vila A. Malware: qué es, cómo funciona y cómo protegerse de los distintos tipos. Xataka. 2022 May 16. https://www.xataka.com/basics/malware-que-es-como-funciona-como-protegerse-diferentes-tipos
104. Vila A. Vulnerabilidades: qué son, cómo se explotan y cómo protegerse. Xataka. 2022 Jun 29. https://www.xataka.com/basics/vulnerabilidades-que-son-como-se-explotan-como-protegerse
105. Walker G, Akdeniz Y. Cybercrime and the Law: Challenges, Issues, and Outcomes. In: Adimola MI, Ismaila O, Adekunle O, Oluwasegun T, editors. A Reader on Cybercrime and Information Security. African Books Collective; 2014. p. 1–36.
106. Wall DS. The Role of Policing in Cyberspace. Policing & Society. 2001;11(1):55–73. https://www.tandfonline.com/doi/full/10.1080/10439460120050192
107. Ward D. The State of Cybersecurity in the Wake of the SolarWinds Attack. OpenAI. 2021 Nov 24. https://openai.com/research/cybersecurity-solarwinds
108. Weimann G. Terrorist Migration to the Cloud. Studies in Conflict & Terrorism. 2016;39(4):347–356. https://www.tandfonline.com/doi/full/10.1080/1057610X.2015.1120099
109. Zerdoumi D, Kechadi MT, Crosbie M. An Empirical Study of the Classification of Malware Families. International Journal of Electronic Security and Digital Forensics. 2009;2(4):334–349. https://www.inderscienceonline.com/doi/abs/10.1504/IJESDF.2009.032716
110. Zheng Y, Zhuang W, Shao J. Comprehensive Model for Cyberterrorism Preparedness. Information Systems Frontiers. 2012;14(4):905–920. https://link.springer.com/article/10.1007/s10796-011-9335-0
111. Zhuang W, Zheng Y. A Framework for Cyberterrorism Preparedness. Information Systems Frontiers. 2011;13(4):483–496. https://link.springer.com/article/10.1007/s10796-011-9261-1
112. Zimmermann P, Haas S, Düring M. Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. Digital Investigation. 2014;11(1):S1–S10. https://www.sciencedirect.com/science/article/abs/pii/S1742287614000623
113. Zittrain J. Introduction: Exploring Anti-Circumvention. Berkeley Technology Law Journal. 2014;29(2):1229–1234. https://www.jstor.org/stable/24117960

FUNDING

The authors received no funding for the development of this research.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHORSHIP CONTRIBUTIONS

Conceptualization: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Data curation: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Formal analysis: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Writing – original draft: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Writing – review and editing: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.