Article

Carlos Ramírez Castañeda

Investigative Perspective on Cyberterrorism from a Contextual Analysis

Abstract

Cyberterrorism is a phenomenon that must be addressed from different angles. Although it originates in the digital environment, this does not mean that its scope and impact are restricted solely to this context, as the repercussions are direct and palpable in the physical world. We will analyze cyberterrorism from an impact perspective, profiling and contextualizing everything that cyberterrorists encompass, some of their modus operandi and historical cases of impact, as well as the visions and nuances left in each action. Having a broader overview and emphasizing the constant evolution of this phenomenon, as well as the importance of a multidisciplinary approach based on cybersecurity, giving due importance to international cooperation in legislation and digital education to mitigate its effects and strengthen human and digital resilience in the face of various emerging threats, which are advancing by leaps and bounds, therefore, the analysis of the context and adaptation of cyberterrorists is essential, without losing the historical heritage that deserves a point of comparison to achieve a better and greater understanding.

Keywords: Cyberterrorism, Profiling, Analysis, Context, Mexico

Carlos Ramírez Castañeda, Lecturer and Researcher, Attorney General's Office of the State of Michoacán.

Received
11/07/2025
Accepted
03/09/2025

To cite this article: Ramírez, C. (2025), Investigative Perspective on Cyberterrorism from a Contextual Analysis, Revista Internacional de Estudios sobre Terrorismo, issue 15:31-43.

1. Introduction

It suffices to turn to the internet to find a universe of information in which it is sometimes difficult to differentiate between legitimate contents and things that seem taken from a science fiction novel. The internet arrived disruptively as a technology that achieved positioning as a tool for immediate and expeditious communication, reigning far and wide across the world, allowing contact between people regardless of borders or geographical barriers, ideologies, genders, thoughts. Today, the internet is the key point in the functioning at different social scales.

From the aforementioned premise, we can proceed to various analyses of cybercriminal behaviors, from legal and technical-informatics perspectives, which are addressed abundantly. However, a bifurcation that branches into social and psycho-criminological perspectives on the topic relating to this quadrant of characteristics related to cyberterrorism is overlooked.

In this article, we will analyze what could be the background or context in cyberterrorism, based on a criminological profiling, as well as its comparison with other branches related to cybersecurity and cybercriminality.

Among the multiple advantages of internet use are from scientific advances to the exploitation that terrorist groups around the world manage to have to achieve positioning in their cause. In this sense, the needs faced by security forces, citizenship, companies, and users in general require an approach to analysis on the context to achieve a better and greater understanding in favor of prevention.

It is worth highlighting that terrorism in its different modalities is present in all countries, in some cases more marked and visible than in others, and for that, it suffices to make a catharsis of the historical facts in regions around the world, which are clear examples of how technology and the internet become the main points of convergence for social control. From here is where we need to glimpse the contextual considerations directly related to cyberterrorism and thus leave a precedent.

2. Understanding Cyberterrorism

Cyberterrorism corresponds to a complex that implies the use of information and communication technologies (ICT) to carry out attacks under a technological premise, intended to cause, instill fear, panic, and derived damages on a worldwide level, since the internet knows no borders. However, many times it is achieved within a demarcation or geographical region nuanced by prevailing political and social situations. The contrasts in cyberterrorism are notable in terms of motivations, ideology, methods, impact, and direct consequences, as well as collateral ones. Below, we will mention some historical cases and more recent examples to illustrate these contrasts:

- Attacks on Estonia in 2007: A series of cyberattacks paralyzed Estonia's governmental, financial, and media services. These attacks were attributed to Russia and are believed to have been related to a political dispute over a monument in Tallinn. The attacks highlighted the vulnerability of the country's digital infrastructures and the way in which geopolitical conflicts

could escalate in the digital realm as well.

- Operation Aurora in 2009: This cyberattack was attributed to China and targeted numerous technology companies and national security defense firms. It is believed that the purpose behind this attack was cyber espionage, theft of intellectual property, and thereby the revelation of trade secrets, which highlighted how states could use cyberterrorism for economic, strategic, and positioning purposes.

- Stuxnet in 2010: The Stuxnet malware was discovered in 2010 and is believed to have been developed by governments of Western countries to sabotage an Iranian nuclear plant. This case demonstrated how states could use cyberterrorism as a tool to halt the development of nuclear weapons in other countries, opening a debate on the ethical and legal implications of the use of digital tools (Buxton, 2022).

- Attacks on the power grid in Ukraine: In 2015 and 2016, Ukraine suffered a series of cyberattacks that left entire regions without electricity for hours[1]. These attacks were considered a clear example of how cyberterrorism could have a direct impact on a country's critical infrastructure, causing massive interruptions in public services (CCDCOE, s.f.).

On the other hand, more recently, we can list some of the attacks in which the use of digital tools is nuanced through terror and social control:

- Use of ransomware[2]: In the last decade, ransomware attacks have increased significantly. Criminal groups use malware[3] to encrypt their victims' systems and demand a ransom in exchange for the decryption key. Notable examples include the attack on the Colonial Pipeline company in the United States in 2021, which affected fuel supply in several regions of the country. These attacks highlight how non-state actors can cause large-scale havoc with primarily financial motivations (Easterly, 2023).

- Operations between nations and disinformation: Some countries engage in cyber operations to influence public opinion and destabilize other governments. The case of the alleged Russian interference in the United States presidential elections in 2016 and 2020 is a prominent example of how cyberterrorism can be used to undermine confidence in democratic systems and undermine political stability.

- Advanced Persistent Threats (APT) from China: China has been accused of conducting sustained and highly sophisticated cyberattacks against government, military, and corporate

1 This event was also known as the "Blackout".

2 "Ransomware is a type of malware that holds a victim's sensitive data or device hostage, threatening to keep it locked, or worse, unless the victim pays a ransom to the attacker" (Kosinski, s.f., para. 1).

3 "Malware is a term that encompasses any type of malicious software designed to harm or exploit any programmable device, service, or network. Cybercriminals typically use it to extract data that they can use as blackmail against victims for financial gain. Such data can range from financial information to medical records, personal emails, and passwords. The variety of information that can be compromised has become limitless" (McAfee, s.f., para. 1).

targets worldwide. These attacks are usually aimed at obtaining strategic and technological information for the benefit of the state. Examples include the theft of information related to the development of stealth fighters and advanced military technology (America's Cyber Defense Agency, s.f.).

- Emerging AI threats: As artificial intelligence advances, concerns arise about how it could be used in cyberattacks. From the development of more intelligent malware to the automation of targeted attacks, the integration of AI in cyberterrorism could significantly increase the scope and effectiveness of attacks.

The technological partnership that we must understand first is the one achieved between technology and psychosocial impact factors, at the time of bringing to reality, subsequent to the digital plane, all those palpable affections that leave a mark.

Technological evolution is not an isolated fact; it is a point exploited by terrorism to magnify its impacts and simplify its efforts.

3. Human Factor

Within cyberterrorism, we must recognize that not everything is purely digital when involving tools developed to achieve a purpose, since behind it there is a human or group of humans in charge of handling the technology. Some examples of this type of actions are the following:

- Activism and hacktivism: Hacktivist groups, such as Anonymous or Guacamaya, have carried out cyberattacks to promote social and political causes. These groups often attack websites and online platforms to spread messages and expose sensitive information. While their motivations may be driven by ideals, their methods can cause collateral damage and generate debates about the limits of digital protest.

- Extremist groups: Some terrorist groups years ago began to use cyberspace as a tool for recruitment, propaganda, and coordination. The Islamic State, for example, has used social networks and online platforms to recruit followers and spread its ideology. Although these groups may not have the technical capacity to carry out sophisticated cyberattacks, their online presence remains a major concern in terms of radicalization and destabilization[4].

- Cyber warfare: Tensions between states can manifest in the form of cyber espionage and high-level cyberattacks. With the above, we can see bodies of cyber soldiers prepared for cyber warfare, something that has been reflected in the Russia-Ukraine war conflict, where a large number of digital operations of scale and impact have been deployed with real damages in the nations from 2022 to date, still with latent consequences.

4 Other groups that can be mentioned in this regard are war groups such as the FARC in South America and drug trafficking groups in Mexico.

Ultimately, cyberterrorism continues to evolve and present a wide range of challenges in terms of security and cybersecurity, allied to other issues such as diplomacy, ethics, and legislation. The international community must collaborate to develop effective prevention and response strategies to address this constantly changing threat, not only from digital issues but toward a human factor that allows knowing the context in favor of prevention.

Cyberterrorism is present with nuances of diverse and varied impact, with that we can mention some clear examples for the understanding of the degree of damage that could be reflected in the material world. Under the aforementioned premise, it is worth emphasizing awareness for users by allowing them to know that although something is gestated in cyberspace or through technologies and at first is not tangible, it can have irreversible consequences in the real world, in the tangible world. Therefore, below, the impacts on different scales are described in more detail:

Social impact. One of the main factors that cyberterrorism relies on, which is related to its name, is fear and panic. Many cyberattacks, technically or digital attacks using platforms, can generate sensations of fear in the population, since the interruption of essential services or the exposure of sensitive data can undermine confidence in the institutions and systems we depend on for our daily lives.

In recent years, we even see a new factor, control through fear, since it is not necessary to resort to sophisticated tools, perhaps a publication that seems real or is real (depending on the context) can generate entire populations fearing to leave their homes. This is how it happens with the case of drug trafficking in Mexico, where through social media platforms messages with photographs taken from public squares are disseminated so that the population feels fear (Contreras, 2023).

Attacks gestated through cyberterrorism on a large scale can erode confidence in the government, companies, institutions. The perceived lack of security in cyberspace can have lasting effects on public confidence, attracting distrust that deteriorates the social fabric. The above can even be used as tools to influence political processes and undermine government stability[5]. The dissemination of false information, election manipulation, and the exposure of compromising information can have a direct impact on internal politics and international relations.

Digital impact. Attacks targeted at critical infrastructures, such as power grids, water systems, nuclear, telecommunications, and health services, can cause significant damages. The interruption of these essential services can have devastating effects on people's lives and a country's economy. Some collateral damages can result in the loss of personal, financial, and business data. This can lead to financial exploitation, identity usurpation or impersonation, and the exposure of industrial secrets, which can have long-term consequences for the affected individuals and organizations.

Attacks diversify into significant economic losses for nations and companies in particular. Likewise, the interruption of commercial operations, the degradation of a company's reputation, and recovery costs can have a negative impact on the economy in general. For cyber espionage tasks, it is usual for cyberterrorists to focus on sensitive and at the same time strategic information.

5 As previously mentioned, the latest elections in the United States are an example of this.

Global scale impact. Cyberterrorism with its direct and collateral consequences contributes directly to global destabilization, with attacks that can exacerbate international tensions and lead to diplomatic or even military conflicts. Viewed from another perspective, when the actors are countries, cyberterrorism can be used as a tool to influence international relations. Cyberattacks between nations can generate tensions and alter geopolitical dynamics, leading to armed conflicts.

Cyberterrorism highlights the importance of international cooperation in cybersecurity matters. The global community must establish norms and agreements to address the unique challenges presented by it and promote a safer cyberspace. Although the latter seems like a utopia, efforts are required to achieve a first firm step between nations.

As we have said, there are various nuances and approaches to impact, from the social and political to the economic or the digital aspect. These impacts can be profound and lasting, affecting both individuals and entire nations. The prevention and mitigation of cyberterrorism require a coordinated global response and a multidisciplinary approach.

4. Digital Terror

When speaking of fear or terror, we must mention cyberterrorism, its present and existing context behind it, to thus proceed to a post-analysis understanding.

Digital terror is a strategy used in cyberterrorism to manipulate and spread fear, disinformation, and propaganda through digital media with the objective of achieving various goals, such as radicalization, mobilization of followers, and social destabilization. This tactic has become increasingly effective due to the omnipresence of technology and global interconnection through the Internet and social networks. Below, we will mention some of the strategies used as points of impact.

4.1. Media Manipulation

Cyberterrorist groups can use digital media to spread false information and disinformation with the purpose of sowing chaos, undermining confidence in institutions, and disseminating their extremist ideology. They can leverage social media platforms, fake websites, and online forums to spread their narrative and thus incentivize some to join their cause and others not to take action out of fear. Narratives are often constructed that exploit sensitive and controversial topics, such as religion, politics, and discrimination. These narratives are used to attract vulnerable individuals and manipulate their emotions, which can lead to radicalization and that tendency to nuance it in an act that impacts the material world (Waldmann, 2010).

In a radicalization process, the creation of an identity is sought, and for that, social networks and other digital media can be used to create that online belonging that converges with individuals seeking to belong to something bigger than themselves. This can lead to greater participation with more radical entities. In this sense, we arrive at an aspect of analysis for the construction of the cyberterrorist context: the sum of people to a cause makes that same one remain present and current.

Here lies the importance for which cyberterrorist groups continually seek people or digital media and tools on which to rely, such as the following.

Social media platforms. They offer an effective platform for cyberterrorists to recruit new members. They can use anonymous or fake profiles to contact and radicalize individuals online, offering distorted information and creating a sense of community (Cyber Zaintza, s.f.).

Multimedia content. The use of impactful multimedia content, such as propaganda videos, graphic images, and extremist speeches, can have a powerful effect in attracting new adherents. These materials can be designed to appeal to emotions and foster adherence to the terrorist cause.

Social engineering techniques. Cyberterrorists can use social engineering techniques to psychologically manipulate people and make them perform actions they would normally not do. This can include persuasion to join extremist groups, participate in illegal activities, or carry out attacks.

Video games. The use of video games as a medium to recruit adherents for cyberterrorism is a concerning phenomenon that has gained attention in recent years. Although not all video games are associated with cyberterrorism, some extremist groups have leveraged these interactive platforms to attract young and vulnerable individuals toward their agendas. Within video games, cyberterrorists can introduce propaganda, either through in-game messages, images, or even videos. This propaganda can promote extremist ideologies, glorify acts of violence, or present distorted narratives.

4.2. Destabilization and Social Chaos

From the terror effect we arrive at the chaos effect, in the mere style of philosophical narrative in which devastation becomes present, playing a key role in destabilization, which is the sum of the aforementioned factors.

By spreading messages of hate, polarization, and discrimination, cyberterrorists can contribute to social and ethnic division. These messages can provoke internal conflicts and weaken social cohesion. We have seen throughout history uprisings in favor of social causes to overthrow regimes (Khader, 2012) and other cases where they manage to destabilize societies.

For this latter assumption, online platforms can be used to coordinate physical or digital attacks. This can include the planning of terrorist attacks, cyberattacks, or the fomenting of riots and violent protests.

Terror as part of digital in cyberterrorism is a multifaceted strategy that seeks to influence public opinion, radicalize individuals, and destabilize society using digital media and social networks. The speed and breadth of online communication make this tactic powerful and challenging to counter, and it underscores the importance of digital education and cybersecurity.

5. Analysis and Context

Context analysis is fundamental in understanding and preventing cyberterrorism. To address this topic, it is necessary to consider both the units or elements involved in the analysis as well as the profiling techniques and methods used to identify potential threats, with the aim of having a prevention parameter before it nuances into an irreversible material result.

For the above, a multidisciplinary approach is needed, as we mentioned at the beginning, to be able to identify and discern, among others, cyber threats, motivations, techniques and tools, or vulnerabilities. All of them we will discuss below.

When we speak of cyber threats we refer to the activities and actors that represent a threat to cybersecurity. This includes individuals, groups, organizations, and states that seek to carry out cyberattacks with malicious purposes, in this case cyberterrorists. As for motivations, understanding those existing behind cyberattacks is crucial to identify the actors and their objectives. Their ends can be political, economic, ideological, or simply malicious. On the other hand, analyzing the techniques and tools used in cyberattacks can provide information on the sophistication of the actors and their level of technical knowledge. Finally, identifying vulnerabilities in systems and networks is essential to prevent cyberattacks. This implies understanding the potential weaknesses that could be exploited by malicious actors, this on a somewhat more technical scale but applicable to the context.

6. Profiling in Cyberterrorism

Profiling[6] in cyberterrorism implies the creation of profiles of the actors involved and their characteristics. This is done with the objective of identifying patterns, behaviors, and motivations that can help prevent or mitigate attacks. In this sense, in 2019 the researchers Macdonald, Jarvis, and Lavis. In their study: "Cyberterrorism Today? Findings from a follow-on survey of researchers", reinforce the relevance of analyzing the ideological and behavioral components within cyberterrorism. Based on a survey conducted with specialists in 2017, the authors show a growing consensus around certain essential traits of this phenomenon: political or ideological motivation, the use of digital media as an instrument or target, and the generation of fear in society as the main effect. Likewise, the researchers foresee that the threat of cyberterrorism is perceived as increasing and that different actors (including States and terrorist organizations) may be involved. In response, they highlight the need for preventive measures, such as strengthening infrastructures, international cooperation, and cybersecurity education, rather than resorting to exceptional or drastic responses (Macdonald, Jarvis & Lavis, 2019).

Likewise, we find this terminology in similar digital sections (AT Internet, s.f.). Some key aspects of profiling for the cyberterrorist are:

6 "Vicente Garrido defines criminal or criminological profiling as the discipline of forensic science that deals with analyzing behavioral traces at a crime scene to provide useful information to the police for the capture of an unknown offender" (Garrido, 2012, p. 11).

Demographic characteristics. This includes factors such as the age, nationality, education, and gender of the individuals involved. These aspects can provide clues about their possible motivations and social environment.

Technical skills. Evaluating the technical skills of the actors is crucial to understanding their level of experience and the type of threats they may pose.

History of activities. Analyzing the online activity history can reveal behavioral patterns and preferences. This can help identify if an individual is involved in suspicious or extremist activities.

Communications and contacts. Examining online communications and contacts can provide information on the networks and groups in which an individual is involved. This is fundamental for tracking possible collaborations and associations.

Language analysis. The evaluation of the language used in online publications can provide clues about the individuals' ideological beliefs and intentions. This includes the use of extremist terms, hate speech, and violent rhetoric.

Connection patterns. Identifying patterns of connections between individuals and groups online can reveal networks and alliances in cyberspace. This is essential for tracking the spread of ideas and collaboration in extremist activities.

Multimedia content analysis. Examining images and videos shared online can reveal extremist symbology, glorification of violence, or evidence of illicit activities.

Reconnaissance techniques. Cyberterrorists can carry out online reconnaissance techniques to identify potential targets. This can include gathering information on critical infrastructures or key individuals.

Group behavior analysis. Observing how groups interact online can help understand how extremist ideologies are spread, how members are mobilized, and how activities are planned.

Within all the methodology to be implemented during and after the construction of a profiling for the cyberterrorist, we can mention some techniques to consider within the context analysis process, among which we find:

Dark web monitoring. Many extremist and cyberterrorist activities occur in the "dark web"[7]. Monitoring these spaces can provide valuable information on the planning and execution of attacks.

Cyber intelligence. Involves the collection and analysis of data related to cyber threats. This can include monitoring online forums, social networks, and encrypted communications.

7 The "Dark Web" is a part of the Internet that is not indexed by traditional search engines and requires specialized browsers, such as Tor, to access it. It is characterized by the anonymity of its users, making it a space where both legitimate and illegal activities can take place.

Behavior analysis. Observing online behavior patterns can help identify suspicious or unusual activities that could be related to cyberterrorism.

Trend analysis. Identifying emerging trends in cyberterrorism, such as new types of attacks or techniques, is crucial to be prepared and develop prevention strategies.

Threat analysis. Involves evaluating the severity and probability of specific cyber threats. This helps prioritize resources and security measures.

Geopolitical context. Understanding the geopolitical context is essential, as international tensions and conflicts can have an impact on the motivations and activities of cyber actors.

Open and closed intelligence. Open intelligence involves the use of public sources, such as social networks and websites, to collect information. Closed intelligence is based on classified or exclusive information from government or corporate sources.

Advanced Persistent Threat (APT) Analysis. APTs are high-level and persistent attacks. APT analysis involves tracking attack patterns over time and understanding the techniques, tactics, and procedures used by the actors to identify their objectives and motivations.

Social network analysis. Social network analysis involves monitoring online platforms to identify the spread of extremist content, interaction between individuals, and the formation of communities in digital environments.

Likewise, contributions such as that of Jiménez Serrano (2012) in the Practical Manual of Criminological Profiling or Miranda Díaz (2017) "Introduction to Criminal Profiling. Criminological Criminalistic Vision", are useful to transfer the line of profiling analysis to the digital realm. The authors explain that the criminological profile is built from the identification of stable characteristics and repetitive behavioral patterns, considering elements such as modus operandi, the offender's signature, criminal geography, and victimology, which allow inferring motivations, behaviors, and probable future scenarios.

Although mainly the manual by Jiménez Serrano focuses on the traditional forensic and police realm, its methodology can be applied to cyberterrorism, where the "crime scene" translates as the digital environment; the modus operandi into attack techniques (such as those already mentioned as examples like malware, ransomware, APT, among others) or dissemination of propaganda; the geography into the virtual location of forums and networks; and finally the victimology into the selection of strategic targets (individuals, states, organizations, databases, to mention some). Thus, just as in the physical realm, digital profiling allows orienting investigations toward a more preventive than reactive approach, anticipating risks and recognizing ideological and behavioral patterns of extremist actors in digital environments. In summary, context analysis becomes a critical tool for understanding and preventing cyberterrorism. Profiling and analysis methods allow identifying patterns and behaviors that may be indicative of potential threats. This is essential for taking proactive

measures and protecting security at different scales, at the individual, business, and national level.

Collaboration between security agencies, international organizations, companies, and civil society is crucial to combat cyberterrorism. Prevention is based on sharing information, developing robust security policies, educating about online risks, and promoting a safe digital environment.

7. Conclusions

In summary, context analysis in cyberterrorism is based on the collection and analysis of information to understand cyber threats and the motivations behind them. Profiling and analysis methods help identify patterns, behaviors, and activities that could indicate the presence of malicious actors. Cooperation and prevention are essential to address this constantly evolving threat.

A critical need is to educate and raise awareness in society about digital threats and cyberterrorism. People must understand how to recognize signs of online radicalization, how to protect their information, and how to report suspicious activities. For their part, government agencies, companies, academic institutions, and international organizations must collaborate to share information and resources. Cooperation between sectors can help prevent cyberattacks and counter cyberterrorism.

As cyberterrorism tactics evolve, constantly innovative cybersecurity solutions are needed. This includes the development of advanced detection and prevention technologies, as well as the promotion of good practices in the design of secure systems. In this sense, governments must establish clear legal and policy frameworks to address cyberterrorism and punish the guilty. This implies the precise definition of cybercrimes and international collaboration in the prosecution of cybercriminals.

Balancing online privacy and security is a challenge. Considerations on data collection, surveillance, and access to personal information must be handled carefully to avoid abuses and vulnerabilities. The internet and cyberspace have brought both advantages and challenges, including cyberterrorism. The evolution of technology has allowed malicious actors to use cyberspace to spread fear, disinformation, and violence.

Cyberterrorism is a complex phenomenon that encompasses a wide range of actors, motivations, and techniques. The contrasts in terms of methods and objectives have created a diverse and constantly evolving landscape. Likewise, media manipulation and digital terror are tactics used by cyberterrorists to radicalize, recruit, and destabilize through digital media. Social networks and video games have become channels to spread extremist ideologies.

Ultimately, cyberterrorism presents a global challenge that requires a coordinated response at the international level. Cybersecurity, legislation, and education become essential pillars to maintain the balance between online freedom and protection against cyber threats.

8. References

America's Cyber Defense Agency (s.f), People's Republic of China Threat Overview and Advisories. AT Internet. (s.f.). Elaboración de perfiles

Basque Cibersecurity Centre. (s.f.). Ciberterrorismo.https://www.ciberseguridad.eus/ciberglosario/ciberterrorismoBuxton, O. (14 julio 2022), Stuxnet: ¿Qué es y cómo funciona?, Avast Academy,

CCDCOE. (2015). *Power grid cyberattack in Ukraine*

CISA. (s.f.). *China cyber threat overview and advisories.*

Cyber Zaintza (s.f.), *Glosario de términos de ciberseguridad.*

Contreras, L. (10 agosto 2023), *CJNG anunció presunto toque de queda en Tepotzotlán con narcomensaje*, Infobae.

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. Studies in Conflict & Terrorism, 40(1), 77–98.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. En J. Arquilla & D. Ronfeldt (Eds.), Networks and netwars (pp. 239–288). RAND Corporation.

Díaz, D. N. M. (2017). Introducción a la perfilación criminal [PDF]. Revista CLEU.

Easterly, J. (7 mayo 2023), *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years, America's Cyber Defense Agency.*

Gómez Sevilla, J. (2024). Ciberespacio y ciberterrorismo: Una aproximación a los nuevos campos de batalla inmateriales. Revista Internacional de Estudios sobre Terrorismo.

IBM. (s. f.). Ransomware. IBM Think.

Infobae. (2023, agosto 10). CJNG anunció presunto toque de queda en Tepotzotlán con narcomensaje.

Jarque, J. M. (2005). El País frente a los atentados del 11–S norteamericano: "acriticismo" y alineamiento discursivo con la postura estadounidense.

Jiménez Serrano, J. (2012). *Manual práctico del perfil criminológico (2.ª ed.)*. Lex Nova.

Khader, B. (2012). *La primavera árabe: el día después*, Papeles.

Martineau, M., Spiridon, E., & Aiken, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. Forensic Sciences, 3(3), 452–477.

McAfee. (s. f.). ¿Qué es el malware?

Macdonald, S., Jarvis, L., & Lavis, S. (2019). Cyberterrorism today? Findings from a follow-on survey of researchers. Studies in Conflict & Terrorism, 42(1–2), 17–45.

Oficina de las Naciones Unidas contra la Droga y el Delito. (s. f.). Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio. Serie de Módulos Universitarios: Delitos Cibernéticos.

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Tshimuila, J. M., Nkashama, D. K., Muabila, J. T., et al. (2024). Psychological profiling in cybersecurity: A look at LLMs and psycholinguistic features [Preprint]. arXiv.

Universidad del Rosario. (s. f.). Repositorio institucional: Documento académico

Waldmann, P. (26 abril 2010), Radicalización en la diáspora: por qué musulmanes en Occidente atentan contra sus países de acogida, Real Instituto Elcano.