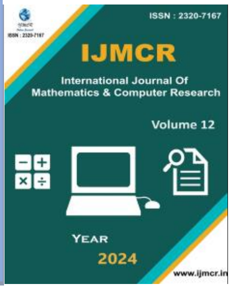
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 12 Issue 01 January 2024, Page no. 3966-3968

Index Copernicus ICV: 57.55, Impact Factor: 7.362

DOI: 10.47191/ijmcr/v12i1.06



Study and Analysis of Cyberterrorist Attacks from Hybrid Computer Systems under the Quantum Spectrum of Software Development and Data Processing; Colombia National Police

Vanesa Atencia Ramírez[1], Juan David Contreras Prada[2]

[1]Corpodesc & https://orcid.org/0009-0001-4011-4091

[2]Policía Nacional de Colombia & https://orcid.org/0009-0001-6800-6068

ARTICLE INFO

Published Online:
05 January 2024

Corresponding Author:
Vanesa Atencia Ramírez, Juan David Contreras Prada

ABSTRACT

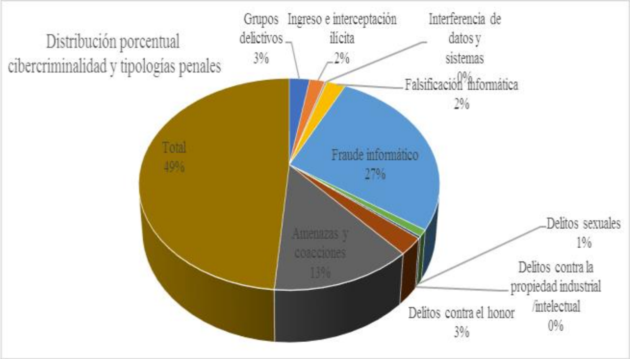
Today's technological society understands cybercrime as a growing phenomenon, because it implies a context where people are dependent on information and communication technologies (ICTs). Computer security reveals that 78% of IT security indicates that organizations do not have sufficient protection against cyber-attacks, therefore, more than 90% of organizations have reported a cybersecurity breach and 62.7% are a product of the pandemic crisis, 43% of cyberattacks affect small businesses along with the decoction of malware and ransomware observed between 2020 and 2021.The research is to analyze cyberterrorist attacks from hybrid computer systems under the quantum spectrum of software development and data processing. Methodology: qualitative approach under the interpretative-positivist paradigm in order to demonstrate knowledge through hypothesis predictions for better future understandings of reality. Discussions: Computer actors modify and access computer systems based on the different variations, because they are not always terrorist in nature, they can be actors knowledgeable about information systems, subjects who are skilled with network actions that dominate the network, that is, they are the mechanism for the achievement of objectives in the network. Conclusions: The phenomenon of cyberterrorism arises as a consequence of the development of technology and information sedimented from the cognitive, behavioral-behavioral and motivational triad, as well as the base tool for the perpetration of terrorist acts and with it the achievement of some political and ideological objective as mentioned before to cause fear in society.

KEYWORDS: Cyberattack, Cybersecurity, Cybercrime, Computer crimes, Digital threat

I. INTRODUCTION

The purpose of the research is to study and analyze cyberterrorist attacks from hybrid computer systems under the quantum spectrum of software development and data processing and compare them with conventional warfare, focusing the results obtained on the validation and hypotheses and obtain the new line of quantitative research and develop an institutional proposal at the convenience of the Colombian National Police to be a reference on cybersecurity and cyberterrorism. The research addresses the types of war and different methods of fighting and definition of the motivations to commit terrorist acts, based on an asymmetric explanation that is based on the documentary review for a comparison of descriptive data.Assuming in other words, cyberterrorism is the evolution of war between weapons, bombs and missiles by a computer and causing more damage to the civilian population because a terrorist is a person who causes panic and terror with the aim of weakening or discrediting governments and a society, in addition, this subject is strategic and is capable of capturing attention like the media, information together with social networks and has a target market segmentation; Their criminal profile is not the “white collar” type. This type of subject can be anyone who is qualified to be a computer terrorist or to design web pages, since all you need is a computer and learning in company, in addition to social resentment for them to The feeling of terrorism may arise, which influences the recruitment of people to manage computer media and the various uses of the network.

A. *Distribution of Cybercrime and Criminal Typologies*



II. METHODOLOGY

Paradigm and research approach

The research is framed in the qualitative approach under the interpretive-positivist paradigm in order to demonstrate knowledge through hypothesis predictions for better future understandings of reality (Hernández et al;2023).

Methodology

Qualitative methodology research, based on content analysis, according to Mayring (2019), this type of research allows the research to be oriented towards the prospective capacity and occurrence of the phenomenon.

Kind of investigation

Phenomenological research, given that, as stated by (Hernández et al;2023), phenomenology opens up the researcher to work directly with the units or statements of the participants or the study of categories of variables.

Research design

The main focus is on the refinement of categories in order to obtain pragmatic and non-ambivalent information. For this type of research, the research design is non-experimental because the coded data are analyzed at a single moment.

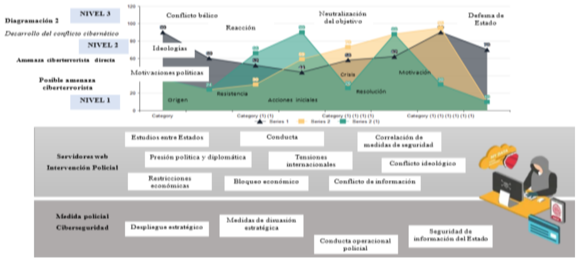
Research Scope

The research is based on the triangulation of the problem statement, naming of hypotheses and achievement of objectives. According to Hernández (2023), qualitative research is based on the achievement of specific deepening properties of the phenomenon**.**

III. RESULTS

Specific objective result 1: Demonstrate from the state of the art: cyber terrorist attacks from hybrid computer systems under the quantum spectrum of software development and data processing. What is described is contrasted with the study by Tapia and Teherán (2023) in the study of Terrorism And Its Transformation - terrorism and its transformation and with the typology of the degree of organization and planning of cyberterrorism along with the type of personality of the subject because Terrorist groups and individuals are part of a group of agents that determine commercial franchises, belonging to the global and systemic dynamism of the web. Cyberterrorism also uses computer hacking techniques to cause economic damage that alters national and transnational security between countries; The growing increase in cyberterrorism is related to strategic visions and ideological and psychological motivations of organizational leaders and their followers.

B. *Hybrid quantum model*



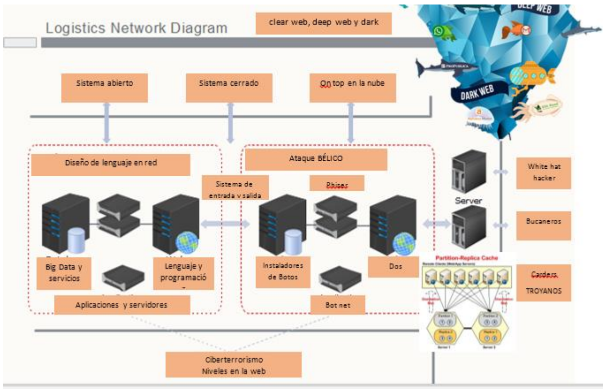
Specific objective outcome 2: Explain cyberterrorist attacks from hybrid computing systems under the quantum spectrum of software development and data processing.

The understanding of cyberterrorist attacks in ascending order of the capacity of terrorist groups to commit acts according to the type of organization, culture and structure; These levels are characterized by simple capacity: basic Hacks capacity against individual systems using the tools on a characteristic objective, exercising control and command over it together with learning capacity, then advanced capacity; characterized by conducting sophisticated attacks against systems on multiple networks with the ability to modify or create tools for complex computing domain and capability; It is the coordinated capacity that is the irruption against integrated and heterogeneous defenses to obtain information from security systems.

C. *Cyber conflict diagramming*

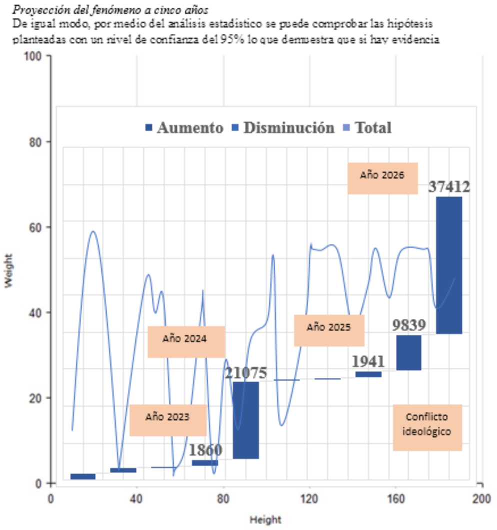
Specific objective result3: Synthesize the explanatory variables of cyber terrorist attacks from hybrid computer systems under the quantum spectrum of software development and data processing.

Through statistical analysis, the proposed hypotheses can be



verified with a confidence level of 95%, which demonstrates that there is scientific evidence to explain the cyberterrorism model from the hybrid spectrum, ideological objectives and assuming the threats and their types. This type of result means that the phenomenon of cyberterrorism increases due to the proportionality of the hybrid war that the world faces at levels in the system due to the source of artificial intelligence (AI), which strengthens terrorism at the web level. and level of social space as well, its financing capacity and collaborative agents to participate in the breadth of radical ideologies or war motivations.

D. Five-year projection of the phenomenon



IV. DISCUSSIONS

The correlation between terrorism and cyberspace, whose association is a favorable scenario to perpetrate terrorist acts and in the same way serve as a bridge for action by groups and individuals with terrorist purposes; however, terrorist acts are summarized by political motivations whose purpose is the achievement of the detriment of economic systems and human life.

V. CONCLUSIONS

The level of risk and its degrees that cyberterrorism represents can be identified as a sectorization process that is established for the development of war and is strengthened through ideologies and cyber resilience in the different social sectors. The contributions of cybersecurity strategies for a State allow the understanding of awareness processes about the risks of cyberspace and impact on national security, protection of computer and information systems and even the survival of the population.

REFERENCES

1. Hernández, R, Fernández, C y Baptista, P. (2023). Metodología de la Investigación. (6a Ed.). México, D. F., México: Editorial Mc Graw-Hill Education.
2. Mayring, P. (2019). Qualitative Content Analysis: Demarcation, Varieties, Developments. Forum Qualitative Sozialforschung, 20(3). https://www.qualitative-research.net/index.php/fqs/article/download/3343/4557?inline=1
3. Tapia, R. P. A., & Terán, L. S. M. (2023). EL TERRORISMO Y SU TRANSFORMACION. Revista de la Academia del Guerra del Ejército Ecuatoriano, 16(1), 13-13.