Chaos in Order: Applying ML, NLP, and Chaos Theory in Open Source Intelligence for Counter-Terrorism

IOANNIS SYLLAIDOPOULOS
Open University of Cyprus,
Nicosia,
CYPRUS

Abstract: - The present research aims to investigate whether Chaos Theory can be combined with Machine Learning and Natural Language Processing to apply these techniques to Open Source Intelligence (OSINT) analysis. Describing the role of OSINT in different domains and highlighting chaos as a valuable resource for information gathering, the study highlights that the substantial volume, swift velocity, and extensive variety of open-source data pose significant challenges. To address these challenges it is proposed to apply elements of Chaos Theory and advanced computational methods to open-source data. Key concepts from Chaos Theory that will be explored are the 'Butterfly Effect', and 'Strange Attractors', attempting to demonstrate that chaotic aspects of data can be exploited and transformed into dynamic and powerful sources of information. To support the above, the research includes a case study that exploits and analyses data from Reddit posts and concludes that recognizing and exploiting the dynamic interaction between order and chaos places Chaos Theory not only complementary but as a foundational stone of the overall OSINT toolkit, in the hands of intelligence analysts.

Key-Words: - OSINT, Chaos Theory, Cybersecurity, Counter-terrorism, Intelligence Analysis, Complex Systems, Data Science.

Received: October 25, 2023. Revised: April 11, 2024. Accepted: May 26, 2024. Published: July 1, 2024.

1 Introduction

1.1 Overview of Open Source Intelligence (OSINT)

It is undeniable that open source intelligence (OSINT) resulting from the collection and analysis of publicly available data from various platforms and digital sources, such as social media, news agencies, traditional media, and academic publications, is increasingly becoming a prominent option for information collection in the 21st century. This fact, combined with the growing reliance on these techniques in areas such as national security, business intelligence [1] and cyber security, underlines their importance, [2]. However, one of the key challenges that those involved in information discovery and analysis have to overcome is managing the inherent disorder due to the volume, velocity, and variety of open source data, a complexity that often leads to ambiguity and preconceptions about these data sources.

1.2 The Challenge of Disorder in OSINT

As a branch of mathematics that focuses on the behavior of dynamical systems that are sensitive to initial conditions, chaos theory lends itself to the extraction of useful conclusions in various fields such as meteorology, biology, economics, and others [3]. Originally formulated in the field of physics to explain complex, non-linear phenomena, the importance of the theory has now found resonance in various aspects of life and scientific research as in modern life the prevalence of complex and dynamic systems has increased significantly.

Although the relationship between Chaos Theory and OSINT is seemingly indistinguishable, there is strong evidence that basic principles of Chaos Theory, such as sensitivity to initial conditions and emergent properties, can provide valuable insights into the OSINT methodology. Simply put, understanding the chaotic nature of open-source data and its apparent disorder can enhance the ability to navigate and draw important conclusions during the information cycle, since the management of open-source data can directly affect the quality, reliability, and usefulness of the information.

Therefore, the present research aims to

investigate through Chaos Theory to what extent the interaction between ataxia and OSINT can lead to new approaches to information collection and analysis, exploiting for this purpose the dynamic, non-linear characteristics of open-source data. A key objective is to create a coherent framework that exploits the basic principles of Chaos Theory to optimize the extraction and interpretation, from seemingly messy data, of information accessible through open sources.

1.3 The Potential of Chaos Theory in OSINT

In the following sections, the historical and philosophical origins of order and disorder will be sought. Then the basic principles of Chaos Theory will be analyzed with the main question of whether these principles can be applied in the context of OSINT. The central axis is the search for innovative methodologies that incorporate elements of Chaos Theory into OSINT practices.

It is argued that the principles of Chaos Theory can contribute to offering new strategies for understanding and exploiting the information arising from the disorder that characterizes information from open sources, and to improve the efficiency and effectiveness of information retrieval.

To support this hypothesis, a case study will both further explain these concepts and open up the discussion on the implications and possible future directions of this crossover of ideas, aiming, by presenting a practical example of the application of these theories, to elucidate the potential benefits and challenges of integrating these seemingly divergent concepts, in the hope of opening the way to a more comprehensive and innovative approach to open source intelligence.

2 Literature Review

2.1 OSINT in Various Research Areas

The previous reference, that OSINT is at the forefront of various research areas, applies to areas such as national security, where the role played by OSINT, both in processes and in the transformation of information, is of paramount importance. Today there are several references to the integral role of OSINT in the strategies pursued by law enforcement authorities in the fight against terrorism, national security, and defense policies, [4]. It is therefore perfectly understandable that the use of OSINT not only widens the range of options available but also opens the way for the use of innovative methodologies in the processing of the data collected.

For example, the analysis of publicly available data from social media platforms has helped to identify and prevent terrorist activities, [5]. In addition, several studies demonstrate the fact that many of the individuals, especially younger individuals, who have engaged in extremist activities have previously browsed and posted content on the web and social networking sites. Consequently, it is easy to see that online platforms have a significantly high ranking in terms of the means used by extremist and terrorist organizations to radicalize and recruit vulnerable individuals. With these tools now at their disposal, these organizations are increasingly using them to promote, incite, intimidate, and radicalize a significantly larger audience that was previously inaccessible, [6]. This creates a new context for intelligence analysis services, as it shifts the focus towards a more proactive rather than reactive attitude, a strategy that can be successfully achieved using OSINT methods and tools, ultimately providing a more robust basis for strategic decision-making.

It is no exaggeration to claim that one of the key steps in the process of data analysis is the appropriate handling of the disorder inherent in open-source data, especially if they are large in volume (Big Data). To better handle such data, computational intelligence methodologies such as Machine Learning are used. However, there is still a lack of research exploring unconventional, interdisciplinary approaches, such as the application of chaos theory to OSINT. The present study focuses on the hypothesis that this integration may offer a new perspective and enhance the capabilities of information analysts and law enforcement authorities.

2.2 Exploring Chaos Theory in Different Scientific Domains

The idea of applying Chaos Theory in different fields is not new. Various scientific disciplines, exploiting its potential, derived from basic principles of physics and mathematics, have successfully applied it to the elucidation of complex systems and phenomena, such as weather phenomena [7], biological systems [8], and economics [9]. Thus, the recognition of the inherent chaotic structures in these fields has facilitated a deeper understanding and prediction of seemingly irregular phenomena and situations.

It would be interesting to investigate to what extent the understanding of the basic principles of Chaos Theory can be applied to the field of computer science, in particular in data analysis, through understanding the inherent chaotic behavior of unstructured data, optimizing the performance and results of the analyzed information, [10]. Such a finding would lend credence to the potential utility of Chaos Theory, laying the foundation for its incorporation into the practices followed by practitioners in the field of OSINT.

3 Theoretical Foundations

3.1 Order and Disorder in Data Systems and OSINT

Order and disorder have deep philosophical roots and seem to have been of concern to mankind since antiquity as they are found in the ancient Greek words for "Cosmos" and "Chaos". Etymologically, 'Cosmos' refers to an organized universe, while ‘Chaos’ denotes the absence of order and the existence of disorder, [11]. If this duality is attempted to be paralleled and transferred to the current data systems, the order could be interpreted as the structured and predictable data, and correspondingly the ataxia would represent the unstructured and thus unpredictable data. If this dimension is taken into account, it is clear that the distinction between order and disorder is also applicable in the real world and affects how we interact and interpret data.

Therefore, understanding this distinction, in frameworks such as OSINT, is a critical stage for the effective analysis of information, as well as for the subsequent safe extraction of useful conclusions. Furthermore, if it is considered that the 'noisy', scattered, and unclassified data on the web cause the disorder and the structured and correctly indexed data contribute to the efforts of the information analysts, then it can easily be concluded that traditional methodology has difficulty in meeting this challenge. This is in contrast to the assumption that class can be seen as a complex system, but with its internal structures and patterns.

3.2 Understanding Chaos Theory

In the 1960s tried to understand why it was impossible to make long-term weather predictions, [12]. His work is considered the beginning of Chaos Theory and led him to the realization that small changes in initial conditions can drastically change the final result. This phenomenon, subsequently referred to as the "Butterfly Effect", [13], is characterized by high sensitivity to initial conditions and leads to a lack of predictability in long-term estimates.

Simply put, according to Chaos Theory, there is seemingly no order in a complex system. However, upon closer observation, patterns appear, often referred to as "Strange Attractors", [14], [15]. These patterns are not random but are determined by the complexity and nonlinearity that govern the behavior of any system, and is believed that these findings will contribute to the understanding of complex systems and the application in various domains such as mathematics, geology, microbiology, biology, computer science, economics, etc [16].

3.3 The Butterfly Effect: Sensitivity to Initial Conditions in OSINT

One of the basic tenets of Chaos Theory is that small changes in initial conditions can lead to significant differences in the subsequent state of a system, [17]. In the context of OSINT, the horseshoe effect, as this principle is called, can be equated with the significant effect of small, seemingly insignificant elements on the outcome of information analysis.

For example, a simple social media post could potentially reveal a critical piece of information about extremist activity, and it is for this reason that this research argues that sensitivity to initial conditions necessitates comprehensive data collection and rigorous analysis in OSINT. It also requires a proactive and adaptive intelligence analysis strategy that can identify and respond to these small changes in a timely and effective manner.

3.4 The Three Vs: Volume, Velocity, and Variety

It has been mentioned in previous sections that open source intelligence (OSINT) comprises a vast, interconnected landscape of publicly available information that is nevertheless characterized by an inherent disorder attributed mainly to the Vs: volume, velocity, and variety [18] and it is these elements that encapsulate the challenges and opportunities presented.

Volume refers to the huge amount of data that is constantly generated and disseminated through various platforms, such as social networks, and naturally creates significant difficulties in extracting, storing, and analyzing data. However, this huge volume presents a wealth of information that, if analyzed correctly, can provide important insights.

Velocity refers to the rate at which new data are produced and the fact that the high speed of information production and circulation can quickly render the information already collected obsolete, thus adding to the difficulties of relating it to current events. On the other hand, rapid updating of data can also serve to provide real-time information, which is vital in cases of rapidly evolving incidents, and early detection of emerging threats.

Finally, variety indicates the heterogeneous nature of OSINT, with data spanning different types of content (e.g. text, audio, and video), or different languages, and introduces complexities in data processing and interpretation, enhancing the disruption but at the same time offering, a comprehensive and multifaceted view of the situation at hand, enriching the information collected.

4 Chaos Theory and OSINT

4.1 Applying Chaos Theory to OSINT

The application of Chaos Theory principles to OSINT causes a change in perspective in that disorder is no longer seen as simple noise, but a complex system with intrinsic patterns waiting to be revealed. In this way, the unstructured nature of open-source data is transformed from an obstacle to an advantage, as unseen connections and patterns are discovered. From this perspective, the seemingly chaotic landscape of OSINT may not be as cluttered as it first appears, as important information may be revealed. This fact makes the transition from chaos to order, from noise to intelligence, an innovative context for immersion and understanding in open-source data analysis.

4.2 Navigating the Disorder of OSINT through Chaos Theory

Chaos Theory provides a new perspective for understanding and navigating the seemingly messy landscape of OSINT, as the parallels between the complex systems inferred in Chaos Theory and the complex, non-linear nature of OSINT are evident. In summary, it can be said that the two domains involve managing a high level of uncertainty and unpredictability, alongside the prospect of emerging order and meaning.

This may be because, in Chaos Theory, the behavior of a system is both unpredictable and deterministic, driven by patterns known as 'Strange Attractors'. This principle suggests that, although the sheer volume and diverse nature of data generated using OSINT methods makes them appear chaotic, they may nevertheless exhibit hidden patterns waiting to be discovered, [14]. By exploring potential 'Strange Attractors' within open-source data, recurring patterns, themes or associations can be revealed, potentially guiding the information analysis process and allowing the data to be considered as interconnected elements of a larger, meaningful structure. The emergent information arising from interactions within a context could not be predicted without knowledge of the individual components, [15] of a dataset, and this is why the application of these theories can significantly enhance the depth and relevance of information, providing a nuanced understanding of the situation or problem.

5 Case Study: OSINT in Counter Terrorism

5.1 Scenario Overview

The case study presented in this paper aims to describe the application of OSINT techniques, in a counter-terrorism context, by identifying potential threats through Reddit posts on the subreddit "worldnews". Using algorithms Machine Learning and Natural Language Processing techniques, an attempt is made to answer the question of whether by making small changes in the sentiment of selected posts, the effects of the 'Butterfly Effect' and 'Strange Attractors' on the conclusions and results of information analysis and processing can be demonstrated through observation.

5.2 Data Collection and Analysis

Data was collected through the Reddit API. It facilitated a preliminary process of cleaning and formatting the dataset, which involved a combination of machine learning and natural language processing techniques to ensure compatibility with subsequent stages of processing. It is worth emphasizing at this point both the complexity and the importance of this step since the extraction of results at subsequent stages relies to a large extent on the correctness of this process.

5.3 Applying Machine Learning and Natural Language Processing

The analysis began by using Machine Learning and Natural Language Processing techniques to examine the Reddit posts. The TfidfVectorizer library was used to convert the post titles into a numerical table representation and then sentiment analysis was performed on each post title using the TextBlob library to understand the sentiment associated with the posts. Finally, Non-negative Matrix

Factorization (NMF) was used to model themes and discover hidden themes in the dataset.

5.4 Identifying Potential Threats through Sentiment Analysis

To identify potential threats, specific keywords were used that are linked to violence, extremism, terrorism, and security and are present in the content of the posts. This technique allowed the filtering to be refined to extract, from the data set, only threat-related postings. As previously mentioned, this is a critical stage of processing and analysis that allows intelligence analysts to focus on data that has real value for national security.

The daily sentiment was mapped to reveal information from the analysis of the sentiment of threat-related postings. In this way, daily sentiment values were collected and visualized allowing for the identification of unusual spikes or patterns in sentiment, such as identifying sudden changes or trends in threat-related sentiment, which could indicate changes or potential escalations of incidents and conditions (Figure 1).

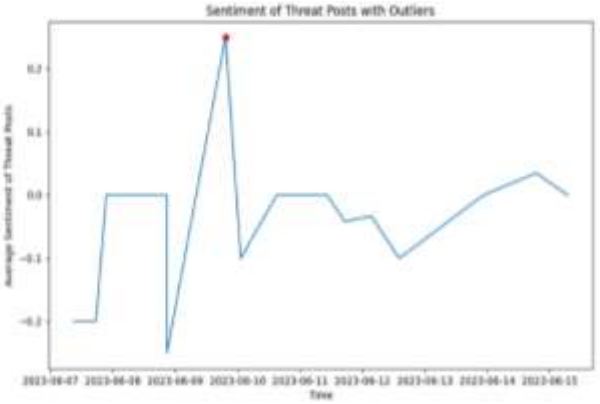


Fig. 1: The plot shows the sentiment of threat posts over time. The sentiment values are visualized as a line graph, with the x-axis representing time and the y-axis representing the average sentiment of the threat posts. There are some outliers in the data, which are highlighted in red as scattered points

5.5 The Butterfly Effect in Action

To clarify the meaning of the "Butterfly Effect", especially in the context of OSINT, the impact on the results of the analysis was recorded by changing the values of the emotion. Specifically, the sentiment values of the postings at the beginning, middle, and end of the period under study were modified and the changes were recorded and visualized.

The result of this process allowed through the comparative analysis of the distribution of emotion, before and after, to highlight the extreme values of emotion, and this part of the research provided valuable information about the dynamic and sensitive nature of OSINT, highlighting the importance of accuracy in data collection, analysis, and processing (Figure 2).

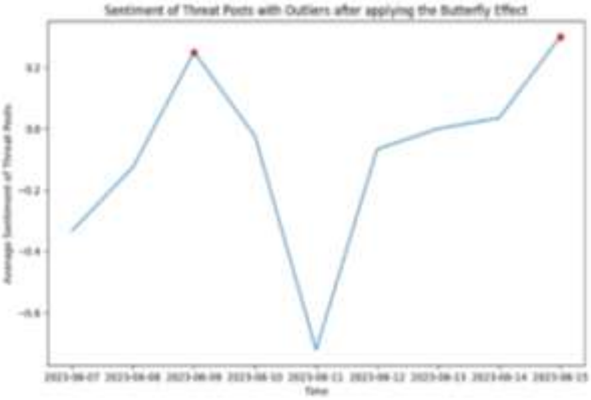


Fig. 2: The plot shows the sentiment of threat posts over time after applying the Butterfly Effect concept. The sentiment values have been modified for specific time points. The sentiment data is visualized as a line graph, with the x-axis representing time and the y-axis representing the average sentiment of the threat posts. There are outliers in the data, which are highlighted in red as scattered points.

5.6 'Strange Attractors' in OSINT

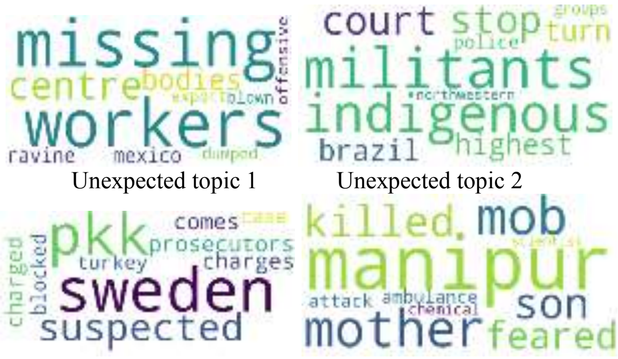
Another useful takeaway that emerged from the process is the unexpected themes that emerged from the content of the postings. In this way, the concept of "Strange Attractors" was also understood in an OSINT context, highlighting the potential benefits of incorporating chaos theory principles. Each topic was generated using Latent Dirichlet Allocation (LDA). What is unique in this case is that pre-defined threat keywords were removed and it was shown that information derived from seemingly insignificant or irrelevant data deserves further investigation as it can provide valuable insights into potential new areas of concern or emerging threats to national security (Figure 3).

5.7 Findings and Interpretation of the Case Study

The results obtained from the analysis of the case study showed that by analyzing content and postings from various social networking media, forums, blogs, etc., it is possible to detect early and effectively possible threats related to violence, extremism, and terrorism. This validates the hypothesis that the capabilities of OSINT combined with the use of Machine Learning and Natural Language Processing techniques greatly facilitate the extraction of critical information from data, thus enhancing the capabilities of conventional information analysis techniques.

At the same time, the practical application of the 'Butterfly Effect' has shown that even small changes in the initial stage of data processing can lead to significant variations in the final result. This reinforces the need for greater attention to detail in every phase of OSINT, from data collection to processing and analysis.

Finally, emerging areas of concern and potential new threats that extended beyond the predefined keywords for threats ("Strange Attractors"), highlighted the need for a more flexible and adaptive approach to OSINT that adequately recognizes and responds to the dynamically evolving nature of the data.



Unexpected topic 1 Unexpected topic 2

Unexpected topic 3 Unexpected topic 4

Fig. 3: The figure shows four sectioned word clouds representing the unexpected topics that emerge from the collected comments using Latent Dirichlet Allocation (LDA). The unexpected topics are identified by checking if any of the top words in each topic are present in a list of threat keywords. Each section of the word cloud represents a different unexpected topic. The size of each word within the word clouds indicates its importance in the corresponding topic.

6 Methodological, Technological and Ethical Implications

It is generally accepted that in today's digital age, the wealth of publicly available data can be exploited to draw conclusions that contribute to the detection and prevention of threats. Moreover, the methodology used for the needs of the present research indicates exactly that. The potential of OSINT techniques and data analysis in efforts to combat terrorism and broader threats to national security is untapped.

Furthermore, the use of modern techniques and tools such as the TfidfVectorizer, NMF, LDA, and other analysis libraries is a testament to the power and ability to extract valuable information from unstructured, high-volume data. It is therefore readily apparent that these tools enhance the capabilities of analysts and intelligence agencies in identifying potential threats in a timely, accurate, and effective manner. However, the successful use of these tools depends on their appropriate selection and application, the development of appropriate analyst skills, and the continuous monitoring of technological developments.

Furthermore, the case study has paved the way for several research questions in the field of OSINT. For example, while the case study mainly used machine learning and natural language processing techniques, future research could explore more sophisticated models, such as Deep Learning, to improve the accuracy of threat detection and sentiment analysis. At the same time, the application of Chaos Theory principles to the OSINT framework offers an innovative perspective for understanding its inherent complexity, and future research could deepen these principles by using them to uncover hidden patterns and predict early threats. It is therefore readily apparent that understanding, for example, the extent to which changes in emotion affect the wider information landscape is a critical process that, if properly exploited, can facilitate improved decision-making processes to combat extremism and terrorism.

Finally, reference should not be overlooked to the ethical considerations which, given the nature of open-source data research, remain of paramount importance. Strict standards of privacy should be observed at every stage of the data processing process, and it should be ensured that the authorities use the appropriate licenses to extract the data, as well as ensuring where necessary that the data and the users who produce it are anonymized.

7 Conclusions

This paper attempted to integrate the basic principles of Chaos Theory, in the context of Open Source Information (OSINT), using the tools of Machine Learning and Natural Language Processing. Initially, the theoretical framework was set out, with the realization that the main characteristics of OSINT methodologies being the sheer volume, high velocity, and variety of data cause a seemingly inherent chaos for those who are required to effectively handle OSINT techniques and tools.

However, the findings demonstrated that when these advanced techniques are combined with Chaos

Theory, which emphasizes complex, nonlinear data systems, they form a powerful framework for deciphering the apparent disorder within OSINT, allowing computer analysts to discover hidden patterns and "Strange Attractors."

Practical proof of the above hypothesis was provided by the results of the case study developed in the paper demonstrating how these techniques and principles can turn unstructured and chaotic data into meaningful interpretation. The critical role played by powerful algorithms in detecting early and emerging threats was also highlighted.

Future research could focus on the potential application of the intersection of Chaos Theory, machine learning, natural language processing, and OSINT in other areas such as crisis management, health policymaking, and business intelligence.

Finally, while this research focused on Reddit data, it is well known that the digital world offers a wealth of open-source information waiting to be exploited. Expanding the research to include data from various sources, such as other social media platforms, news articles, blogs, and digital archives, could provide new perspectives and reveal hidden information, thus enhancing the usefulness of OSINT and making it increasingly usable and valuable. As the volume, velocity, and variety of open-source data continue to increase, is hoped that this study will spark further exploration and lead to a deeper understanding of the hidden order within the chaos.

Abbreviations:

OSINT: Open Source Intelligence
ML: Machine Learning
NLP: Natural Language Processing
API: Application Programming Interface
NMF: Non-negative Matrix Factorization
LDA: Latent Dirichlet Allocation

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this research, the author utilized OpenAI's ChatGPT to enhance the readability and language of the manuscript, and Python scripts were employed for data analysis and figure production. These tools were used to streamline certain aspects of the research process. The author reviewed and edited all content to ensure its accuracy and coherence, taking full responsibility for the final publication.

References:

[1] Entrepreneur, *"Thinking Like a Spy: How Open Source Intelligence Can Give Your Business an Edge"*, [Online]. https://www.entrepreneur.com/growing-a-business/thinking-like-a-spy-how-open-source-intelligence-can-give/444634 (Accessed Date: May 27, 2023).

[2] European Union Open Data Portal, *"Open Source Intelligence"*, [Online]. https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence (Accessed Date: May 27, 2023).

[3] Charles Oestreicher, "A History of Chaos Theory," *Dialogues in Clinical Neuroscience* 9, no. 3 (2007): 279-289, accessed May 27, 2023, https://doi.org/10.31887/DCNS.2007.9.3/coestreicher.

[4] Chris Pallaris, "Open Source Intelligence: A Strategic Enabler of National Security," *CSS Analyses in Security Policy*, no. 32 (April 2008): 1-3, [Online]. https://www.files.ethz.ch/isn/50169/css_analysen_nr%2032-0408_E.pdf (Accessed Date: May 27, 2023).

[5] Sam Zeiger and Jack Gyte, "Prevention of Radicalization on Social Media and the Internet," in *Handbook of Terrorism Prevention and Preparedness*, ed. Alex P. Schmid (ICCT Press, 2021), 358. https://doi.org/10.19165/2020.6.01.

[6] Sara Zeiger and Joseph Gyte, "Prevention of Radicalization on Social Media and the Internet," in *Handbook of Terrorism Prevention and Preparedness*, edited by Alex P. Schmid. ICCT Press, 2021. https://doi.org/10.19165/2020.6.01.

[7] Mark A. Runco, "Conclusion: What Creativity is and What it is Not," in *Creativity* (Second Edition), ed. Mark A. Runco (Academic Press, 2014), 389-427. https://doi.org/10.1016/B978-0-12-410512-6.00013-8.

[8] Ranjan Vepa, "Nonlinear Filtering of Oscillatory Measurements in Cardiovascular Applications," *Mathematical Problems in Engineering*, (2010): 1-18, Article ID 808019. https://doi.org/10.1155/2010/808019. Accessed via EconPapers.

[9] William A. Brock, "Chaos Theory," in *International Encyclopedia of the Social & Behavioral Sciences*, ed. Neil J. Smelser and Paul B. Baltes (Pergamon, 2001), 1643-1646.

https://doi.org/10.1016/B0-08-043076-7/00578-7.

[10] Michele Sasdelli, Thalaiyasingam Ajanthan, Tat-Jun Chin, and Gustavo Carneiro, "A Chaos Theory Approach to Understand Neural Network Optimization," *Proceedings of the International Conference on Digital Image Computing: Techniques and Applications (DICTA) 2021*, pp. 1-10, IEEE, 2021, DOI: 10.1109/DICTA52665.2021.9647143.

[11] Encyclopedia Britannica, "Chaos," last modified July 28, 2019, [Online]. https://www.britannica.com/topic/Chaos-ancient-Greek-religion (Accessed Date: May 27, 2023).

[12] James Gleick, *Chaos: Making a New Science* (New York: Penguin Books, 1987).

[13] Edward N. Lorenz, *The Nature and Theory of the General Circulation of the Atmosphere* (World Meteorological Organization, 1967).

[14] Debra Straussfogel and Christopher von Schilling, "Systems Theory," in *International Encyclopedia of Human Geography*, ed. Rob Kitchin and Nigel Thrift (Elsevier, 2009), 151-158. https://doi.org/10.1016/B978-008044910-4.00754-9.

[15] Glenn D. Walters, "Criminal Justice Policy and the Criminal Lifestyle," in *Modelling the Criminal Lifestyle*, Palgrave's Frontiers in Criminology Theory (Palgrave Macmillan, 2017): 245-273. https://doi.org/10.1007/978-3-319-57771-5_9.

[16] Hena Rani Biswas, Md. Maruf Hasan, and Shujit Kumar Bala, "Chaos Theory and Its Applications in Our Real Life," *Barishal University Journal Part 1* 5, nos. 1&2 (2018): 123-140. ISSN 2411-247X.

[17] Edward N. Lorenz, *The Essence of Chaos* (UCL Press, 1993).

[18] Jelena Lukić, "The Impact of Information and Communication Technology on Decision-Making Process in the Big Data Era," *Megatrend revija* 11 (2014): 221-234. https://doi.org/10.5937/MegRev1402221L.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Ioannis Syllaidopoulos is the sole author. The author read and approved the final manuscript.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The author, Ioannis Syllaidopoulos, hereby declares that there are no financial, commercial, or other affiliations that could be construed as a potential conflict of interest in the research, authorship, and/or publication of this manuscript. The research was conducted in the absence of any commercial or financial relationships that could be interpreted as a potential conflict of interest.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)