Asia Pacific Academy of Science Pte. Ltd.

Smart Tourism 2024, 5(1), 2495.
https://doi.org/10.54517/st.v5i1.2495

Article

Methodology to analyse cybersecurity in tourism

Tanya Arenas[1,2,3,*], Julián Patiño[1], Miguel Ángel Martínez[1], Humberto Dorantes[4], Mauricio Chávez[4]

[1] Instituto Politécnico Nacional IPN, Mexico City Gustavo A. Madero 07738, Mexico
[2] Universidad Rosario Castellanos URC, Mexico City Gustavo A. Madero 07969, Mexico
[3] Centro de Ciencias de la Complejidad C3 UNAM, Mexico City Coyoacán 04510, Mexico
[4] Tecnológico de Estudios Superiores del Oriente del Estado de México Tesoem, Mexico State La Paz 56400, Mexico
*** Corresponding author:** Tanya Arenas, tanya.arenas@c3.unam.mx

CITATION

Arenas T, Patiño J, Martínez MA, et al. Methodology to analyse cybersecurity in tourism. Smart Tourism. 2024; 5(1): 2495. https://doi.org/10.54517/st.v5i1.2495

ARTICLE INFO

Received: 17 January 2024
Accepted: 18 February 2024
Available online: 20 March 2024

Abstract: Nowadays, hyperconnectivity provides an opportunity for the tourism industry to benefit from big data analytics as a determining factor for decision-making, product design, and assertive marketing strategies for target segments, but at the same time, having financial, organizational, and personal information stored in cyberspace and available to many users makes it vulnerable to security risks like phishing and hacking, both common cybercrimes that affect the tourism sector. This paper introduces the representation and model design stages of our own methodology based on a self-organization approach that we propose to reinforce cybersecurity in tourism as part of a research project founded by a National Council for Science and Technology postdoctoral scholarship for Mexico.

Keywords: tourism; complexity; phishing; hacking; cybercrime; cybersecurity

1. Introduction

Before the pandemic, the tourism industry accounted for 1.7 trillion U.S. dollars in exports, or 7% of the world's total, 29% of service exports, and 10% of the world's GDP [1]. In Mexico, the tourism industry contributed 8.7% of GDP [2]; in the National Survey of Occupation and Employment (ENOE, from its Spanish initials), the employed population in the tourism sector for the first trimester of 2019 reached 4 million, 246 thousand direct jobs, meaning 8.7% of total employment nationwide, which confirms the tourism industry is one of the driving forces of the national economy [2]. According to UNWTO [1], Mexico ranked in 16th place with 22.5 billion dollars in tourism receipts and in 7th place with 41.4 million tourist arrivals in 2019. These data are representative of the economic relevance of the tourism sector. With the internet revolution, the digital footprint behind the Mexican tourism industry stores tourist providers and customers valuable information as well as their financial transactions in cyberspace, making them vulnerable to security risks like phishing and hacking, both common cybercrimes that affect the tourism sector [3]. In order to diminish such vulnerability, we introduce a model to reinforce cybersecurity in tourism based on Heylighen's [4] and Hutchin's [5] self-adaptation approach.

2. Purpose

To design a model useful to:
Understand tourism data vulnerability in cyberspace.
Provide solutions to diminish tourism data vulnerability in cyberspace.

3. Implications and expected outcomes

Nowadays, after human capital, the greatest value of industries and economies relies on data and information. That's why, in this paper, we highlight the importance of reinforcing cybersecurity in the Mexican tourism industry. And our expected outcomes are aligned to contribute to a transdisciplinary methodology to represent and support an integral cybersecurity proposal.

4. Research design

We propose a cybersecurity ecosystem to reinforce tourism in Mexico, based on the Gershenson [6] self-organization approach to build a system that will be able to cope with complex problem domains.

The design of our research is systemic, transdisciplinar, and dynamic in order to avoid approaches that simplify and isolate effects. Our systemic design considers the relationships and interactions to support a comprehensive understanding of tourism cybersecurity. In that way, in **Table 1**, we summarize recent approaches dealing with cybersecurity to compare and position our proposed solution to existing ones, indicating congruity and differences.

Table 1. Existing approaches dealing with cybersecurity.

Author	Year	Approach	Comparison
Fragniere and Yagci [7]	2021	Cybersafety	Congruity based on complexity conceptual framework, they refer Cyber resilience and our study considers cybersecurity as an emergent behavior
Djebbar and Nordstrom [8]	2023	Analysis of cybersecurity Standards	Congruity considering Control hierarchy
Che Mat et al. [9]	2024	Literature review on persistent Threat behaviors	Congruity considering multi stage correlations, in our case modules
Abelson et al. [10]	2024	Scanning and Artificial intelligence methods	Difference on content scanning design principles as isolated strategy
Naqvi et al. [11]	2023	Literature review on phising mitigation strategies	Difference focusing on software based Techniques instead complex model representation

5. Conceptual framework

Because of transdisciplinary nature in this research, we propose the next conceptual-theoretical supports:

5.1. Complexity and Mexican tourism digital infrastructure system

The tourism digital infrastructure system in Mexico integrates large sets of real-world data, and that information quantity stands today as a preeminent challenge for modern science [10,12]. That is the reason why this frontier science project is focused on the data and fingerprints of tourism activity in cyberspace.

As digital data is an important part of new technology analytics, the theoretical framework for this research is based on complexity, since there is no more pertinent framework than transdisciplinarity for this applied research aligned to the new knowledge of frontier science in Mexico.

Our project represents the tourism digital infrastructure system in Mexico as a complex system with emergencies, conjunctures, combinations of circumstances, and the appearance of collective properties.

We consider that the complex system behavior of tourism digital infrastructure in Mexico is the result of the mixed effects of many parameters, variables, and agents that influence and enhance each other.

Our project approaches the complexity of the tourism digital infrastructure in Mexico in terms of functional redundancy, where diverse functions and activities are carried out in the same cyberspace.

Given the growth and constant diversification of the tourism sector in cyberspace [13,14] where travel agencies, tour operators, search engines for accommodation reservations, transportation tickets, etc. work with the personal data of tourists and depend on the digital infrastructure of the web and the internet.

With 71% of travelers carrying out searches from their smartphones, tourism currently ranks 3rd in the most affected industries by cyber security crimes, with the theft of tourists private financial data for use in fraudulent activities being the most frequent digital crime in tourism.

In that way, the digital infrastructure system with large volumes of personal and financial information from both tourists and tourism service providers—extremely valuable data—is exposed to the vulnerability of the digital world. When hacked or victimized by cybercrime, it affects the ability of tourism companies to provide their services, negatively affects the experience of travelers, and damages the Mexican tourism system, losing the confidence of travelers and harming the reputation of brands and tourist destinations with significant economic losses.

This is how in our project we represent the complexity of the digital tourism infrastructure in Mexico in congruence with functional redundancy, which corresponds to the multiplicity of digital tourism transactions executed in the same cyberspace. Functional redundancy characterizes “complexity” which leads us to our next complementary theoretical support.

5.2. Law of requisite variety

In our project, we refer to the concept of variety as a measure of complexity, based on William Ross Ashby’s law of requisite variety: “With an increase in complexity, problem domains become non-stationary, requiring dynamic solutions that will be able to adapt to the changes in the problem domain [15].

We analyze the multiplicity of digital fraudulent operations executed in cyberspace, such as phishing and hacking, to generate the vulnerability of the digital world and how we should respond to this situation. We propose integral cybersecurity as an essential element to protect and strengthen the tourism digital infrastructure system in Mexico.

We suggest a cybersecurity ecosystem because we believe that fragmented approaches and partial and unilateral solutions are not enough to face the vulnerability of the digital world and that when information is hacked or victimized by cybercrime [16], it affects the ability of tourism companies to provide their services. It negatively affects the experience of travelers and damages the Mexican tourism system,

generating a loss of confidence among travelers and damaging the reputation of brands and tourist destinations with significant economic losses.

The law of requisite variety establishes that "only variety absorbs variety" [15]. That is, the disturbances that a system represents to another system (variety) can only be reduced or eliminated through the same or greater variety. Beer [17] defines variety as the number of possible states of a system, which would be considered the measure of complexity in a system.

The principle of requisite variety functions as a support to model how the results of fraudulent operations generate an imbalance in the cyberspace organizational system and how governments, companies, and tourists should respond to this situation. In that way, congruent to cybernetics of second order, we propose:

- Attenuators and amplifiers That regulates the variety of the Mexican tourism digital infrastructure system against cybercrime perturbations, leading the system to a certain region of viable cybersecurity, according to Wiener [18].
- Feedback loops

Both as indispensable tools for an integral cybersecurity to protect and reinforce the Mexican tourism digital infrastructure system.

5.3. Data of Mexican tourist activity in cyberspace as self-organizing system

We consider the self-organizing systems principle because different authors have employed it to solve complex problems, like Ashby [19]; Beer [17]; Bonabeau et al. [20]; Di Marzo Serugendo et al. [21]; Zambonelli and Rana [22]. Also, domains like software engineering and collaborative support have proposed self-organization in particular methodologies (Wooddridge et al. [23], Zambonelli et al. [24], Jones et al. [25].

We approach the data on Mexican tourist activity in cyberspace as a self-organizing complex system, mainly because of the behavior that it presents given its derivated emergencies, conjunctures, combination of circumstances, and appearance of collective properties.

But we also approach it in this sense based on Gershenson [6] reasoning that there is no sharp boundary to distinguish this kind of system, but definitely they are partially determined by the observer describing the system and its purpose. Any dynamical system can be said to be self-organizing or not, depending partly on the observer (Gershenson and Heylighen [26]; Ashby [27]), and because of our frontier science research intention, we consider it the most pertinent option.

In that way, our model design aligns with Gershenson [6] description of a self-organizing system as one in which elements interact to achieve dynamically a global function or behavior; in this case, cybersecurity is not imposed by one single or a few elements nor determined hierarchically (Naqvi et al. [11], but instead achieved autonomously as the elements interact with one another, and these interactions produce feedback that regulates the system.

5.4. Cybersecurity as emergent behavior in Mexican tourism cyberspace

Emergence, or appearance, in complex social systems is understood as a functional association of complementary and interconnected heterogeneous elements. This research steers the system into negative phishing and hacking friction reduction, synergy promotion, and the desired integral cybersecurity in tourism ecosystem performance.

6. Methodology

In this research, we propose our own methodology inspired by Gershenson [6] to design and control self-organizing systems. We took it as a reference because it is specialized to solve complex problems within the premise that reducing the "friction" of the interactions between the elements of a system will result in greater "satisfaction" of the system, that is, better performance [6]. Based on that, our research contributes:

- representation of how cybersecurity can reinforce tourism in Mexico,
- to increase our understanding of cybersecurity in tourism,
- introducing an integral cybersecurity ecosystem that considers amplifiers and attenuators to reinforce the Mexican tourism sector.

Our proposed methodology is a guideline to find and develop efficient cybersecurity amplifiers and attenuators to reinforce tourism in Mexico. In general, our research provides a conceptual framework and model representation to support the solution of an integral cybersecurity ecosystem to reinforce tourism in Mexico.

As we took inspiration from Gershenson's general methodology to design and control a complex system that includes five steps allowing backtracking, we decided to sequence our own methodology into four inter-emergent stages:

Definition of inter-emergent stages. The flexibility condition between methodology stages allows backtracking with each other.

- The first and second inter-emergent stages are: representation and model design. Dedicated to the abstraction and description of the complex system under research.
- The third and fourth inter-emergent stages are simulation and feedback. Dedicated to understanding the behavior of the system and making evaluations and feedback recommendations for its functioning within the limits imposed by certain criteria or drivers.

This research paper only includes the representation and model design stages. Reaching the objective of providing representation to support the solution of integral cybersecurity for tourism in Mexico. In future research papers, we will introduce simulation and feedback stages.

6.1. First stage: Representation

Carlos Gershenson, author of the methodology that inspires ours [6], recommends using metaphors to speak about the system. In that way, for our system under study, we use the next metaphor:

We consider the Mexican tourism digital infrastructure system to be a self-organized system that has legitimate and organic communication derived from the interactions and transactions related to tourism generated in cyberspace. And we

intend that the attenuators and amplifiers proposed in our model preserve organic communication as social help forums do, where information on certain topics is shared between users, in order to provide other users with elements for better informed decision-making. In our interest case, those elements are related to cybersecurity conflicts in tourism: information shared between consumers, tourist providers, authorities, and diverse implicated agents to prevent and avoid other consumers and tourist providers from being victims of cybercrime. Considering organic social communication will contribute to identifying cybersecurity conflicts in tourism in order to diminish them.

And at the same time, the representation we make of the complex system under study is guided by the modularity principle, which says each subsystem in a complex system is generally made of modules, whose interconnections allow the global functionality of the subsystem [28]. And we managed to represent our complex system with not overly constrained modularity to allow adaptiveness, as recommended by Francois [28] for the study of social systems and Gershenson [6] to increase robustness and adaptability because of the integration and solutions for each module.

As we are introducing our own methodology and knowing from Gershenson [6] that there is still no general framework for constructing self-organizing systems, the modularity principle guided our research for that construction, so we did a checklist about the actors of our complex system. If the actor covers some characteristics, then he is an agent of a certain module or subsystem.

We classified agents or elements by the tasks or functions expected from them, and those functions have to do with the satisfaction of the module, subsystem, and system that is being designed. If the functions are fulfilled, then it can be said that the system is "satisfied" or that the goal has been achieved, implicating in the design stage of our model the engineering of elements that will strive to reach system satisfaction (**Table 2**).

Table 2. Agents and elements in tourist cyberspace.

Internet module	**Goal**
Internet search engine	The general goal of internet module is to allow the free exchange of information among all its users. For this research purpose, our interest is focused on tourist information exchange and e-tourist commerce.
Web pages	
Fake web pages	
Websites with malicious code	
Malicious apps	
Booking websites	
Tourist apps	
Internet Protocol IP	
User Datagram Protocol UDP	
Transmission Control Protocol TCP	
Transactional Transmission Control Protocol T/TCP	
AES standard	

Table 2. (*Continued*).

Internet module	**Goal**
Bancanet platforms	
PayPal	
Mercado pago	
Google	
Facebook	
Instagram	
Twiter	
Individual profiles	
Group profiles	
Fake profiles	
Passwords	
Biometric data	
Government module	**Goal**
National Council of Public Safety	The general goal of government module is to create, apply, and enforce laws. Mediate in conflicts, develop policies regarding economy and social systems. For this research purpose, our interest is regarding tourist socioeconomic implications.
31 Public security bureaus	
Cyberpolice units	
General attorney	
Federal attorneys	
Federal consumer attorney	
Tourism Bureau	
Enterprises module	**Goal**
Stakeholders investors, employees and suppliers of tourist enterprises	The general goal of enterprises module is to satisfy the needs of customers and all groups involved in the organization; utility creation, for shareholders, and workers.
Tourism providers	
Travel agencies	
Tour operators	
Hotels	
Banks and financial enterprises	
Cibercriminal organizations	
Users module	**Goal**
Travelers	The general goal of users module is communication, information exchange and service-products consumption.
Tourists	
Cardholders	
Cyber criminals	
Feedback/Control instruments	**Goal**
Cyber incident catalog	The goal of feedback/control instruments is having resources to help overcome cyber crimes.
Cybersecurity guide	
National tourist registry	
National registry of cyber incidents	
Technological control devices	
Security domain standards	

Also, for this first-stage classification, we have considered the specification of levels, granularity, variables, and interactions that need to be taken into account. And we also followed Gershenson's [6] idea that the identification of goals is useful to measure the satisfaction of elements in the system (**Table 2**).

6.2. Second stage: Modeling design

Continuing with our inter-emergent stages, the second one corresponds to modeling. For this research, we designed our model with the following characteristics:

- Suitability to changing adaptative environments like cyberspace
- Pertinence to cope with threats in complex environments
- Providing attenuators and amplifiers to manage unexpected negative frictions between elements that diminish system satisfaction
- Increasing understanding of cybersecurity will reinforce tourism in Mexico.
- Identifying cybercrimes that affect tourism
- Increasing element satisfaction to obtain integral system satisfaction

Those characteristics congruent with the self-organization of our model are given:

- Our complex system and environment are very dynamic and unpredictable.
- We want the system to solve the cybersecurity problem, but the "solution" is not known beforehand and is changing constantly; it is dynamically striven for by the elements of the system.
- The observer cannot a priori conceive of all possible configurations, purposes, or problems that the system may be confronted with. The suitability that Heylighen and Gershenson [26] emphasize for complex software systems such as the Internet is where cybersecurity tourism issues take place.

Following another Gershenson [6] piece of advice for model design, we have divided the system into semi-independent modules with internal goals, dynamics, and interactions. Our division obeys the next classification:

6.2.1. Dynamic organization of the model by modules

Our model design considers modules that integrate digital data and fingerprints of mexican tourist activity in cyberspace (**Table 3**).

Table 3. Interactions by module.

Interactions within the internet module	
Positive	**Negative**
• Hotel rooms reservations • Traveler records on booking websites • Traffic on tourist websites • Buy/sell of tourist services and products • Encryption of encryption algorithms	• Traffic on fake tourist websites • Hacking financial information with malicious code websites or apps • Phishing tourist providers websites • Frauds

Table 3. (*Continued*).

Interactions within the government module	
Positive	**Negative**
• National tourist registry • National registry of cyber incidents • Cyberpolice units operations • Federal consumer attorney reports/complaints	• Restriction to access national registry of cyber incidents • National tourist registry is not updated
Interactions within the government dule	
Positive	**Negative**
• Biometric payment authentication • Tourist services and products management • Tourist services and products offers	• Cibercriminal organizations • Fake tourist excessive offers
Interactions within the users module	
Positive	**Negative**
• Profiles registration on tourist websites • Tourists social media posts • Tourists reviews • Cardholders registers update	• Cybercriminals communication with potential victims

Based on complexity approach our model dynamic self-organization characteristics (**Table 4**), provide insights to answer below research questions.

Table 4. Dynamic and self-organization characteristics of our model.

Characteristic	**Explanation**
Multiple friction interactions	Non linear, non static
Flexibility and adaptability	Possible to fit changed circumstances
Modules or modularity principle	Representation by modules allows to analyze self-organization of a complex system
Variety balances	Dynamic representation
Information exchange	Represents organic legitime communication

6.2.2. How can we design integral cybersecurity ecosystem to reinforce tourism in Mexico? and How elements in the model will co-evolve influencing each other's development?

The integral cybersecurity proposal, from a systemic perspective, tends to offer solutions to balance cybersecurity complexity and to explain how elements in the model will co-evolve, influencing each other's development, based on the principle of the requirement variety law from William Ross Ashby [19]. In **Figure 1**, we explain in a diagram this principle law.

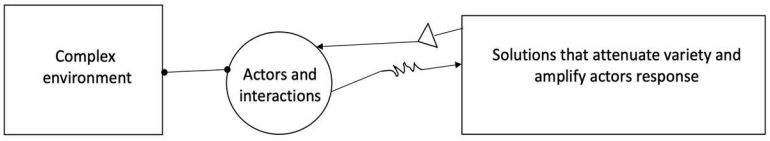

Figure 1. Diagram explanation of requisite variety law.

Following the requisite variety logic, to survive in the complex environment of cyberspace, the booking websites, the travel agent web pages, and the tour operator web pages must be complex enough to fit into the cyberspace environment and its

threats like phishing and hacking cybercrimes. If the web pages of the tourist providers fail to correspond to the complexity of the environment, it means that these organizations have failed to achieve what is expected of them, which basically consists of providing a safe and quality service to the consumer or tourist in cyberspace.

All booking websites, web pages that sell tour packages, and travel agent web pages face the challenge of fitting into the environmental complexity of cyberspace. The problem is that the complexity of cyberspace is theoretically infinite, so there must be selectivity as to which aspects of the environment are of most concern. In this research case, we consider the two types of crimes that most affect the tourist sector:

- Phishing tour operators and travel agency websites to gain consumers trust to make them pay for a fictitious package or trip.
- Hacking with the purpose of stealing private financial data from travelers or tourists to use this data later in fraudulent activities.

Our representation of an integral cybersecurity ecosystem to reinforce tourism in Mexico seeks to reconcile the imbalances caused by phishing and hacking. The balance can only be achieved by amplifying the response of travelers, tourists, booking websites, and web pages that sell tour packages; this response will attenuate the variety and threats of cyberspace. In that way,

Two important elements of our model are attenuators and amplifiers that are represented with electric symbols.

The attenuators (AT on **Figure 2**) that we propose are:

- Identify booking or tour-selling websites that operate through hacking and phishing.
- Classify booking or tour-selling websites that operate hacking and phishing.
- Make public or inform which booking or tour-selling websites operate hacking and phishing.

The amplifiers (AM on **Figure 2**) that we propose are:

- Awareness campaigns for tourists to inform them how to book and buy package tours on secure internet sites
- Encryption of encryption algorithms for information security using the AES standard
- Multilayer with biometric data for more secure financial transactions

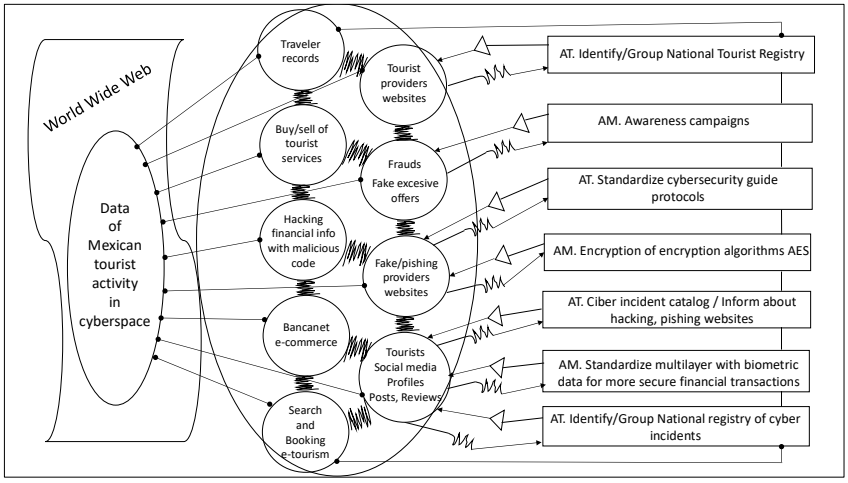

Figure 2. Cybersecurity ecosystem to reinforce tourism in Mexico.

Basically, understanding the level of complexity in cyberspace that must be absorbed gives us a reference to achieve an integral cybersecurity ecosystem model that considers self-organization dynamic by modules and goals.

6.2.3. How the Mexican tourism system self-organizes in cyberspace?

The main general goal that we identified for the Mexican tourism system in cyberspace is tourist information exchange, marketing, business networks, booking, purchase, and sale of tourism services and products.

We can refer to all those activities in complex system terms as interrelations in cyberspace. But not all activities contribute to optimum behavior for the whole tourism system; for example, we consider for this research purpose phishing and hacking cybercrimes as interactions or behaviors from certain actors that create negative frictions and change the optimum dynamic in the whole tourism cyber system. We made this analogy based on Kauffman's [29] idea that in some cases, the behavior of the institutions or actors in our research case changes the optimum behavior of the whole system.

Our self-organization approach for the Mexican tourism system is precise: it is able to adapt Holland [30] to changing situations and respond to the changing demands of its environment, in this case cybercrimes like phishing and hacking.

In that way, the responses of the Mexican tourism cyber system prove some new learnings in environment phishing and hacking negative frictions. Che Mat et al. [9] and are indeed self-organization evidence of the need to be adaptive, extensible, and open in the interactions. Responses or moves, learning how to interact and communicate, with whom to cooperate, and how to delegate and coordinate tasks. To evolve collectively capable of reaching cybersecurity in some degree (**Figure 3**).

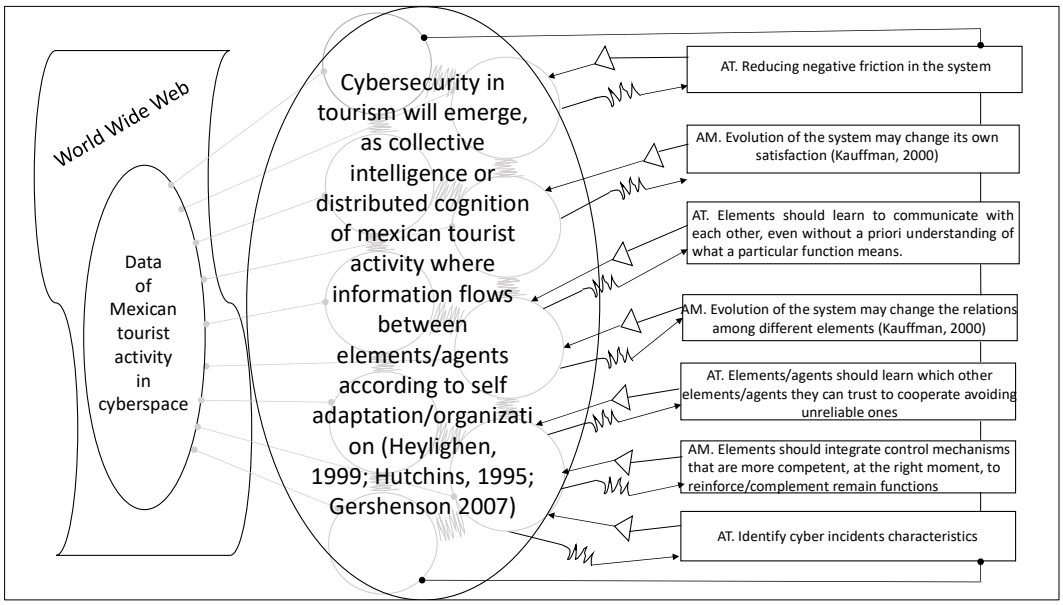

Figure 3. Cybersecurity ecosystem self-organization to reinforce tourism in Mexico.

So we have designed our model according to Shalizi [31] trying to keep it robust and simple to anticipate as much as possible. Considering attenuators, amplifiers, and feedback to ensure the system is balanced, satisfying goals, doing what it is required

to do, and adapting or reacting quickly to unforeseen cybercrime emergencies. Moreover, promoting positive interactions (synergy) and constraints to prevent negative interactions between elements (friction) means keeping variables within certain boundaries in the Ashby [27] sense.

In that way, proper interaction should produce the desired performance of cybersecurity to reinforce Mexican tourism. For this reason, the dynamic organization of our model preserves self-organization, dividing the problem for better understanding and integrating modules to reduce friction and promote synergy. Luo and Choi, 2022 [32]. According to Wiener [18], the steering system should be in a certain region appropriate for design and control.

On **Figure 4**, we present an example showing the application of representation and modeling with the data of the PROFECO Mexican federal consumer attorney from December 2018 to February 2022 SSP [33].

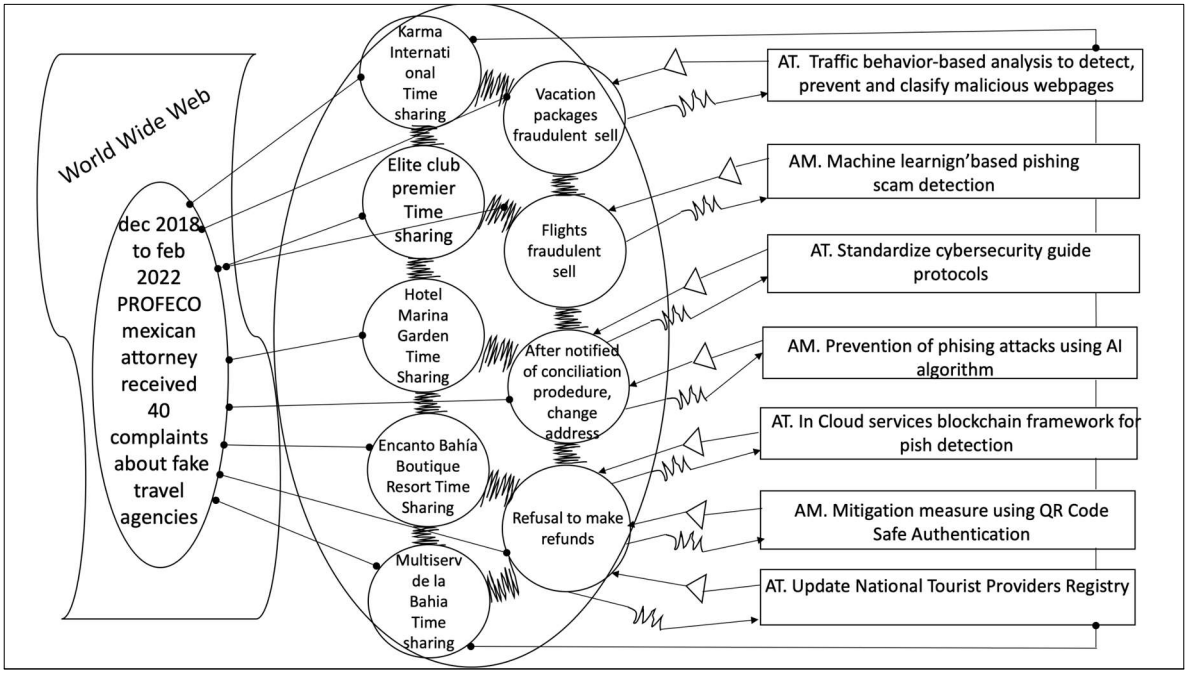

Figure 4. Example showing application of representation and modeling.

6.2.4. Significance regarding the sustainability of the proposed model

The proposed model is aligned with Sustainable Development Goal 9, which seeks to build resilient infrastructure and foster innovation. Our cybersecurity proposal is directly related to economic growth, social development, and technological progress, considering that by 2022, 95% of the world's population will be within reach of a mobile broadband network. Investment, tourist providers service competitiveness, employment, and tourist income generators, as well as tourist consumers, need to be safe on the world wide web protected from cyberattacks. In that way, our model is congruent with the sustainability perspective for 2030 [34].

6.2.5. Cybersecurity ethical considerations

Regarding technology and tourist economic activity in cyberspace, ethical considerations in cybersecurity Boustead [35] range from having access to financial

and confidential sensitive data to user privacy and business proprietary information, and the critical challenge of reaching a balance between optimal data management and business interests prioritizing defense against cyberattacks and preserving human rights.

7. Discussion

Our research contributes theoretically and conceptually to increasing understanding of the complexity of re-enforcing Mexican tourism with cybersecurity. The practical implications of contributing to that understanding are that nowadays Mexican companies and governments must invest funds and efforts to reinforce cybersecurity. Given the continuing growth of vulnerability derived from hacking and phishing, cybercrimes represent a major challenge that affects the reputation of brands and destinations, and it can even cost significant losses in the operation of the tourism business economy. Besides, how we can respond and design a cybersecurity ecosystem to reinforce the Mexican tourism sector is still not understood very well.

In that way, we proposed a cybersecurity ecosystem model to improve the reliability of the Mexican tourism sector. How we manage our response to cybercrimes will have a huge impact on Mexican tourist competitive indicators over the long term.

Indeed, the cybersecurity ecosystem approach as emergent collective intelligence or distributed cognition to reinforce tourism puts us closer to answering questions such as: What causes vulnerability in cyberspace? Can we suggest integral solutions for tourist organization needs in cyberspace based on complexity? Is it necessary to promote attenuators and amplifiers for the Mexican tourism system to ensure its continued competitive functioning, or is it an unnecessary burden? This paper suggests some insights into those ways for a Mexican tourism system to perform its tasks and achieve its goals in the cybersecurity ecosystem.

8. Limitations and future work

This research paper limits itself to the representation and model design stages. Further research will include simulation and feedback, including hacking and phishing cybercrime datasets, to track the evolution and accumulation of this kind of incident and study its detailed dynamics.

9. Conclusion

Our proposal is useful to design and manage Mexican tourism cybersecurity complexity based on scientific and engineering understanding of the world wide web space to provide inferences and possible solutions. Not surprisingly, much research effort worldwide is now devoted to understanding the drivers and dynamics of complex challenges in cyberspace.

At this point of our study, we have developed our own methodology based on complexity principles, resulting in a flexible model that is already a technological development in frontier science that can be replicated and scalable into different economic sectors that also have presence in cyberspace and that, at the same time, are

vulnerable to cybercrime. It is helpful for further cybersecurity developments, suggestions, and concepts from distinct application scopes.

We found cybersecurity in tourism is a major challenge that must be tackled from a complex organizational perspective that considers an integral cybersecurity ecosystem aimed at reinforcing Mexican tourism in a multi-faceted, variable, and competitive environment and induced optimal interactions that reduce vulnerability and negative frictions. Variety attenuators (AT) and amplifiers (AM) are necessary and essential across Mexican tourist activity in cyberspace.

The model we have proposed and its self-organization intend to reflect distinct features of interactions between elements. It is our contribution to approach the underlying structure of Mexican tourist activity in cyberspace, which is notoriously complex, representing both significant challenges and opportunities. Given that tourism plays a key role in economic growth and development, it must be reinforced with cybersecurity as a high priority in this digital era.

Our model is replicable because it can be successfully reproduced on different scales and in different economic sectors that have activity in cyberspace.

We have identified and represented linkages between elements—clusters that are connected to each other—that exhibit consistent objectives in cyberspace.

We have also provided a little frontier science example applying complexity concepts and principles to analyze cybersecurity in tourism. We therefore conclude that our suggested methodology can be useful for social complexity issues.

Author contributions: Conceptualization and methodology, TA; formal analysis and supervision, JP; investigation, MAM and HD; review and editing, MC. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. UNWTO. Tourism highlights, 2019th edtion. World Tourism Organization; 2019.
2. First work report of the ministry of tourism 2018-2019. Available online: https://www.gob.mx/sectur/articulos/primer-informe-de-labores-de-la-secretaria-de-turismo-2018-2019-218765?idiom=es (accessed on 9 January 2024).
3. Alcántara-Pilar JM, del Barrio-García S, Crespo-Almendros E, et al. Toward an understanding of online information processing in e-tourism: does national culture matter? Journal of Travel & Tourism Marketing. 2017; 1-15. doi: 10.1080/10548408.2017.1326363
4. Heylighen F. Collective intelligence and its implementation on the web. Computational and Mathematical Theory of Organizations. 1999, 5(3): 253–280. doi: 10.1023/A:1009690407292
5. Hutchins E. Cognition in the Wild. MIT Press. 1995.
6. Gershenson C. Design and control of self-organizing systems. Copit Arxives. 2007.
7. Fragniere E, Yagci K. Chapter: Network & Cyber Security in Hospitality and Tourism. Hospitality & Tourism Information Technology. University of South Florida M3 Publishing. 2021.
8. Djebbar F, Nordström K. A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access. 2023; 11: 85315-85332. doi: 10.1109/access.2023.3303205
9. Che Mat NI, Jamil N, Yusoff Y, et al. A systematic literature review on advanced persistent threat behaviors and its detection strategy. Journal of Cybersecurity. 2024; 10(1). doi: 10.1093/cybsec/tyad023
10. Abelson H, Anderson R, Bellovin SM, et al. Bugs in our pockets: the risks of client-side scanning. Journal of Cybersecurity. 2024; 10(1). doi: 10.1093/cybsec/tyad020

11. Ardito L, Cerchione R, Del Vecchio P, et al. Big data in smart tourism: challenges, issues and opportunities. Current Issues in Tourism. 2019; 22(15): 1805-1809. doi: 10.1080/13683500.2019.1612860
12. Naqvi B, Perova K, Farooq A, et al. Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security. 2023; 132: 103387. doi: 10.1016/j.cose.2023.103387
13. Paraskevas A. Cybersecurity in Travel and Tourism: A Risk-based Approach. In: Handbook of e-Tourism. Xiang Z, Fuchs M, Gretzel U, et al. (editors). Cham: Springer Nature Switzerland AG; 2020. doi: https://doi.org/10.1007/978-3-030-05324-6
14. Xiang Z, Fuchs M, Gretzel U, et al. Handbook of E-Tourism. Springer International Publishing; 2020. doi: 10.1007/978-3-030-05324-6
15. Ashby WR. The nervous system as physical machine: With special reference to the origin of adaptive behavior. Mind. 1947; 56(221): 44–59. doi: 10.1093/mind/lvi.221.44
16. Florido-Benítez L. The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users' Private Data in Smart Cities. Smart Cities. 2024; 7(1): 475-495. doi: 10.3390/smartcities7010019
17. Beer S. Decision and control: The meaning of operational research and management cybernetics. John Wiley and Sons. 1966.
18. Wiener N. Cybernetics or Control and Communication in the Animal and the Machine. Wiley and Sons. 1948.
19. Ashby WR. An Introduction to Cybernetics. Chapman & Hall. 1956.
20. Bonabeau E, Dorigo M, Theraulaz G. Swarm intelligence: From natural to artificial systems. Santa Fe Institute studies in the sciences of complexity. Oxford University Press. 1999.
21. Di Marzo Serugendo G, Karageorgos A, Rana OF, Zambonelli F. Engineering self-organising systems, nature-inspired approaches to software engineering. Lecture Notes in Computer Science. Springer; 2004.
22. Zambonelli F, Rana OF. Self-Organization in Distributed Systems Engineering: Introduction to the Special Issue. IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans. 2005; 35(3): 313-315. doi: 10.1109/tsmca.2006.846372
23. Wooldridge M, Jennings NR, Kinny D. The Gaia methodology for agent-oriented analysis and design. Journal of Autonomous Agents and Multi-Agent Systems. 2000; 3(3): 285–312. doi: 10.1023/A:1010071910869
24. Zambonelli F, Jennings NR, Wooldridge M. Developing multiagent systems. ACM Transactions on Software Engineering and Methodology. 2003; 12(3): 317-370. doi: 10.1145/958961.958963
25. Jones PM, Contractor N, O'Keefe B, Lu SC. Competence models and self-organizing systems: Towards intelligent, evolvable, collaborative support. In: 1994 IEEE International Conference. pp. 367–372.
26. Gershenson C, Heylighen F. When can we call a system selforganizing? In: Advances in Artificial Life, 7th European Conference, ECAL 2003 LNAI 2801. Springer; 2003. pp. 606–614.
27. Ashby WR. Principles of the self-organizing system. Principles of self-organization. In: Foerster HV, Zopf, Jr., GW (editors). Pergamon, Oxford; 1962. pp. 255–278.
28. François C. International Encyclopedia of Systems and Cybernetics. Published online December 31, 2004. doi: 10.1515/9783110968019
29. Kauffman SA. Investigations. Oxford University Press; 2000.
30. Holland JH. Adaptation in natural and artificial systems. The University of Michigan Press; 1975.
31. Shalizi CR. Causal architecture, complexity and self-organization in time series and cellular automata [PhD thesis]. University of Wisconsin at Madison. 2001.
32. Luo S, Choi TM. E-commerce supply chains with considerations of cyber-security: Should governments play a role? Prod. Oper. Manag. 2022; 31, 2107–2126. doi: 10.1111/poms.13666
33. Fraud in the tourism sector (Spanish). 33 Mesa de seguridad turística SSPC. Mexico. 2022.
34. UN DESA. The Sustainable Development Goals Report 2023: Special Edition. UN DESA; 2023.
35. Boustead AE, Kugler MB. Juror interpretations of metadata and content information: Implications for the going dark debate. Journal of Cybersecurity. 2023; 9(1). doi: 10.1093/cybsec/tyad002