EGE AKADEMİK BAKIŞ / *EGE ACADEMIC REVIEW*

Cilt 23 • Sayı 2 • Nisan 2023
SS. 163/184
Doi: 10.21121/eab. eab.1083229
Başvuru Tarihi: 4.3.2022 • Kabul Tarihi: 29.9.2022

Article Type: *Research Article*

Relativity Approach to the Strategic Cyber Conflict Management In Businesses

Fahri ÖZSUNGUR[1]

ABSTRACT

The study aims to form a theoretical basis for the development of strategies needed by businesses and establish strategic principles. The starting point of this research is that cyber conflict is an operational, managerial, relational, and strategic problem of businesses rather than a cross-country administrative problem. This research was carried out by adopting grounded theory, known as theorizing-based theory. The study was carried out with 593 limited liability and joint-stock companies operating in Turkey. The research results revealed a new theory named "relativity of strategic cyber conflict management". According to the research findings, the five orbital forces (negotiation, managerial, infrastructure, defense, competition) were determined in cyber conflict management. Four principles were determined as a business within the system (location in space), the business within cyber cosmos (relativity of time), warping spacetime due to cyber conflict (Curvature of strategy), and illusions due to cyber conflict (Gravitational lenses).This study introduces a new theory of the cyber conflict management with the inspiration of the principles of relativity theory.

Keywords: Cyber conflict, management, strategy, relativity theory, grounded theory.

JEL Classification Codes: M10, M15, M16, M19

Referencing Style: APA 7

INTRODUCTION

Internationalization and cyber developments continue to increase their influence on organizations, country economies, and societies (Barrinha & Renard, 2017). The positive contributions of digital innovations to business life support the strategic developments of the manufacturing and service sectors (Barrett et al., 2015). Innovations such as automation, nanotechnology, 3D printing, robotic applications, industrial internet of things (IIoT), cloud computing, big data, augmented reality, 5G, artificial intelligence, cybersecurity, and smart factory technologies have created a revolution in production and planning (Campbell & Ivanova, 2013; Zollo et al., 2007; Carmigniani et al., 2011). This revolution has brought technologies such as autonomous vehicles, real-time supply chain visibility, verified carbon standard technology, blockchain, artificial and augmented intelligence, digital twins, advanced analytics to businesses in the field of logistics (Kato et al., 2015; Caridi et al., 2014; Sharma et al., 2012; Li et al., 2020).

Technological, digital, and cyber innovations emerging in the manufacturing sector have revealed important developments in the service sector. Smartphones, the internet of things (IoT), virtual reality, quantum computing, AI-boosted and predictive cyber protection, runtime application self-protection, biometric verification, identity-as-a-service, distributed artificial intelligence, edge computing, 5G cellular such innovations facilitate the functions of businesses (Emig et al., 2007; Li et al., 2017). The multidimensional positive effects of cyber developments on businesses such as productivity, performance, profitability, customer satisfaction, functional speed, ease of access, virtual access have brought risks and threats (Monostori, 2014; Lee et al., 2015).

The rapid development of cyber innovations has revealed security risks (Andrijcic, & Horowitz, 2006; Alhayani et al., 2021). Hidden competition between countries and organizations has triggered the malicious use of cyber innovations. Cyberwarfare serves this purpose (Dipert, 2010). Cyber attacks aimed at attacking the political, military, economic, and cultural values of countries often target international companies and organizations (Li et

[1] Mersin University, Faculty of Economics and Administrative Sciences Department of Labor Economics and Industrial Relations, fahriozsungur@mersin.edu.tr

al., 2012). This situation reveals cyber conflicts (Danyk, Maliarchuk, & Briggs, 2017). Businesses that are important actors in realizing economic goals, contributing to the global economy, opening the way for the implementation of entrepreneurial ideas, and creating new angel investors are under the threat of cyber conflicts.

Cyber conflicts damage the relationships of businesses with their stakeholders, environment, and employees (Gandhi et al., 2011). Conflicts can negatively affect many processes related to company mergers, negotiations, intra-organizational relations, operations, production and planning, and business (Shackelford, 2014). Businesses need a strategy that they can implement against these conflicts. Studies on cyber conflict deal with limited issues such as cyber-attacks and cyber warfare (Junio, 2013; Karatzogianni, 2008; Shi et al., 2007; Heckman et al., 2013; Denning, 2014; Xu, Lu, & Li, 2015). In conflict management, it is necessary to develop a new theory and strategy principles on issues such as the relations of businesses with their stakeholders, the perceptions of employees, the relativity of the changing conditions and experiences over time, and the fight against the obstacles that arise in the elimination of cyber conflicts. Elimination of this important deficiency can strengthen businesses in the context of struggling with cyber conflicts.

In the context of cyber conflict management, structuring the theoretical basis for the development of strategies needed by businesses and establishing strategic principles are the objectives of this study. It is among the other aims of the study to provide practical and theoretical inferences to practitioners, policymakers, and academics, based on the issue that cyber conflict is an operational, managerial, relational, and strategic problem of businesses rather than a cross-country administrative problem.

THEORETICAL FRAMEWORK

General View of Cyber Conflict Management

The virtual movement that emerged with the internet and digital developments has increased the freedom of action of organizations, countries, and individuals in cyberspace. Cyber and digital developments that started at the end of the 20th century and continued at a dizzying pace at the beginning of the 21st century have highlighted the issue of managing the conflicts caused by cyber elements (Radanliev et al., 2018; Broadhurst, 2006; Lin, 2012). Cyber conflict management has provided taking important steps in the prevention of cyberattacks, cybersecurity against malware, elimination of conflicts arising from the virtual environment in international negotiations, protection of intellectual property and trade secrets, hate speech and discrimination in social media, and information security (Taillat, 2019).

Initially, the basic principles of conflict theory were based on cyber conflict, taking into account the rivalries and inequalities between different groups in society (Brief et al., 2005). The conflicts that started with class conflicts and power struggles have expanded to many areas such as social, economic, psychological, military, political, and cyber (Gayer et al., 2009). The critical theory, which deals with the conflicts arising from the competitive relationship created by power structures, gained a different dimension with the feminism approach focusing on the conflicts created by gender inequality (Rush, 2004). The queer movement, which involves the thought of elimination of heterosexual prejudice, was replaced by world-systems theory based on the transnational division of labor (Rand, 2013). Thus, an important step was taken regarding the management of the wide-ranging conflicts caused by internationalization and globalization.

Globalization, digitalization, and media conflicts have brought a new dimension to the conflict by revealing the cyberwarfare movement (Gompert & Libicki, 2014). Cyber conflict, which continues to increase in international relations, politics, propaganda, racism, and discrimination, continues to be reflected in all areas of life (Bobo, 1983). Cyber conflict, spreading like a virus, damages the relations with every institution, business, person, and organization that businesses are in contact with. This type of conflict, which negatively affects business life, has turned into a crisis, especially during the pandemic period.

Relativity Theory

The theory of relativity includes the idea of predicting spacetime as a four-dimensional manifold. Three-dimensional space consists of length, width, and depth. Relativity theory adds the time dimension to these dimensions. Three dimensions provide revealing of coordinates and determination of their location in determining a point in space. According to this theory, simultaneity is relative. If the observing individuals are in relative motion, two simultaneous events may not be perceived simultaneously.

One of the notable principles of the theory is the time-gravity relationship. As gravity increases, time slows down. Another feature is that there is no difference between constant acceleration in space and gravity. This principle reveals an energy-derived property of mass.

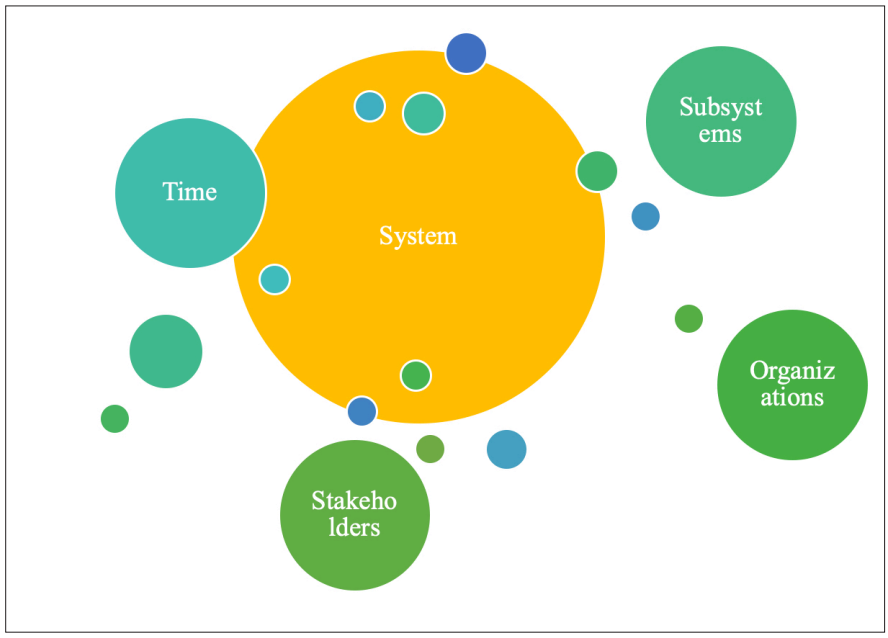

Figure 1. Relativity of the infinite system

The energy and mass of an accelerating object increase, creating a twist in space. Because mass is an indicator of resistance to acceleration. However, the photons that makeup light have no mass. Therefore, photons do not have the ability to resist acceleration. However, light is bent by the mass's warping of space. This situation is called the gravitational lens according to the theory. Thus, it has been shown that the path followed by the light moving between the shortest line is not a straight line. With its shortest definition, the curvature is a whole, consisting of space, time, and dimensions.

The fact that time is different for different parts of the world shows that different times are experienced in different regions in terms of the time concept of space. In other words, time dilation and the twin paradox are the two main determinants of this approach. The warping of the light with mass orientation causes visual and temporal misconceptions. The theory is important in that it reveals that time varies relative to the observer, not position in space.

Relativity Theory in Organizations

Planets rotating in elliptical orbits around the sun demonstrate the gravitational force between objects and cause the light warpings revealed by rotations. The theory of general relativity reveals these warpings, and special relativity does how spacetime warping slows time.

Einstein argued that the basis of the universe consists of the space-time dilemma. From this point of view, how does this theory relate to organizations, businesses, and social sciences in the context of cyber conflict? The theory emphasizes the importance of the fourth dimension, time, in determining a location in space. On the other hand, relativity reveals that time differs according to space's three-dimensional location. In the light of these explanations, the issue of the position of organizations emerges in the context of relativity and the fourth dimension.

Organizations are entities created for people's purposes. These entities are a whole in which the aims, goals, knowledge, creativity, leadership qualities, and managerial skills of the founder are organized. Businesses are organizations in which commercial operations are carried out. A business or organization established within the legal system survives in the infinite system. Systems based on many needs such as law, cyber, virtual, politics, economy, international, cultural, scientific, etc. are emerging. The infinity of these systems shows that they can be determined relatively and depending on time. Organizations emerge through three basic dimensions, human, purpose, and action. The theory of relativity is related to the idea that organizations and the systems they are in surviving depending on the time dimension. However, this relationship requires the existence of an endless cycle between past, present, and future. Sub-systems, organizations, time, and stakeholders create a trajectory around the system under the gravitational effect of the central system (Figure 1).

The trace left by an organization after its interaction and communication with its environment in the period between its establishment and its termination may

Table 1. Fundamentals of relativity approach

Basic features	Descriptions
Location in space (three dimensions)	Width, length, and depth are the main determinants of location in space.
Key position factor (time) in space	The time differs according to points in different locations in space.
Curvature of spacetime	Mass in space creates a gravitational effect with the energy released, causing space and time to warp.
Warping spacetime	The warping caused by mass and energy reveals the energy-momentum and pressure-stress cycle.
Gravitational lens	The warping of light from a source in space as it reaches the observer's observation area.

affect future organizations. Thus, the organization can adopt a strategic management approach by obtaining information about the past, present, and future. The warping space-time put forward by the relativity theory is similar to the temporary trace that appears after seating on the seat. Organizations leave some traces to their environment and systems throughout their existence. These traces provide strategically important managerial functionality considering the time dimension.

Organizational purpose and system are like time-space. According to the theory of relativity, these two complementary elements provide important information about the actual positions of the observed elements. The traces left by organizations in their relations with their environment may cause misperceptions about observation, depending on time and light warpings. This gravitational mirage can deviate the strategies of the organization, causing unsuccess. The factors that form the basis of these deviations are presented in table 1.

METHODOLOGY

The grounded theory, a qualitative research method, was adopted in this research. The principles of the grounded theory (theorizing-based theory) were applied to the realization of the research and to collect the data. This approach is a research method that enables a theory to be constructed after analyzing qualitative data (Bryant, 2017). This method allows a theory to be revealed by inductive inferences. This research method includes the stages of collecting qualitative data, analyzing the collected data based on coding, and constructing theory (Nelson, 2020). To construct an inductive theory, the data obtained are interpreted and reported. The grounded theory process followed in the study is shown in figure 2.

In grounded theory, research questions are determined at the preparation and collecting data stage, ethical

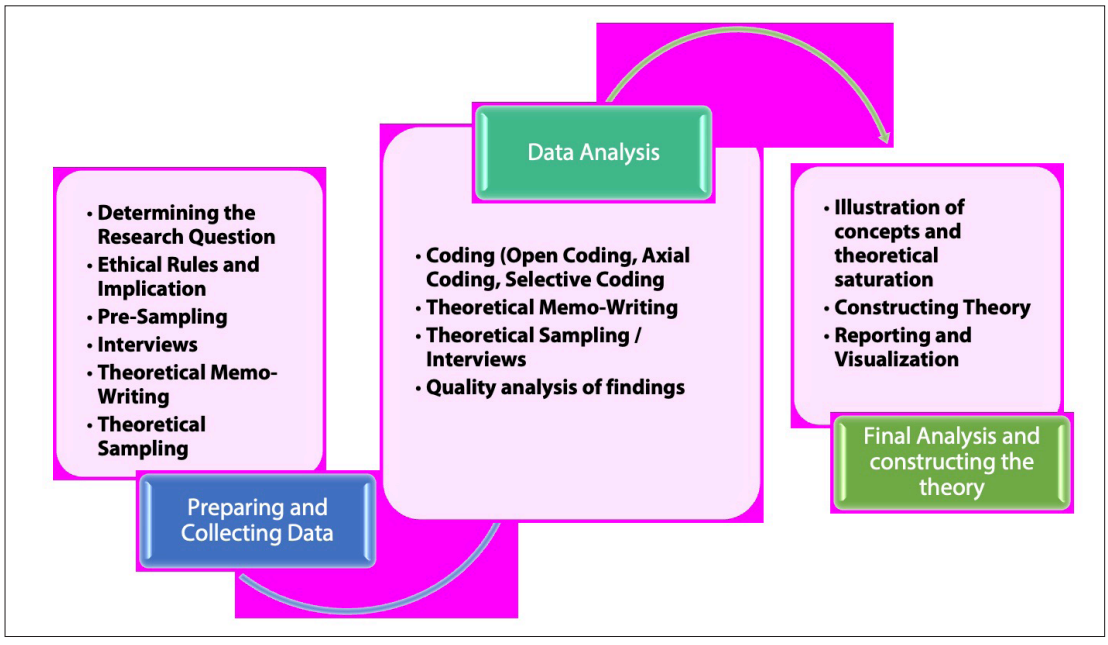

Figure 2. Grounded theory process

principles are applied for the data to be analyzed, interviews are conducted with the participants using the pre-sampling method, notes are taken about the data obtained from these interviews (theoretical memo-writing) and, if necessary, new participants are included in the sample with the theoretical sampling method (Charmaz, 2014).

The data analysis stage includes the coding of the data obtained through the interview, the inclusion of new participants in the sample with the theoretical sampling method when necessary, quality analysis in the context of the contribution of data to the new theoretical structure and results (Charmaz, 2014). In the last stage, the new theoretical structure is constructed through the illustration of concepts, theoretical saturation, and visualization. The successful execution of these processes ensures the reliability of the constructed theory (Charmaz, 2017).

Determining the Research Question

The grounded theory focuses on the causes and consequences of social events (Charmaz, 2017). This theory provides to reveal the theoretical reflections of knowledge based on experiences, thoughts, and observation in life (Strauss & Corbin, 1997). Grounded theory, which is a socio-psychological approach, plays an important role in revealing exploratory, explanatory, and interpretative information about individual-individual, individual-society, individual-environment communication, and interaction (Charmaz, 2014). The lack of cause and effect information about interactions and communications requires the determination of the research question. Unknown truths or known mistakes are tried to be determined through the research question (Charmaz, 2017).

Cyber conflict management is inspired by the concepts of crime, attack, danger, risk, espionage, information leakage, execution of the concept of cyber. Internet and digital developments have pushed businesses to adapt to these developments on the one hand and to adopt defense strategies on the other hand. Technological developments in production have created a revolution in human-based resource dependence in the workforce by enabling the use of automation and robotics. While social media, virtual reality, virtual applications support the production and service functions of businesses, they have become an important conflict factor on the other hand.

Businesses that are pioneers in the realization of economic goals and entrepreneurship and establishing international economic ties are in cyber conflicts in today's world. These conflicts are increasing with the pandemic. The current management strategies of businesses are far from meeting many needs in managing cyber conflicts. The complexity and the lack of studies in the definition of cyber conflicts in the literature raise the following questions: What are the factors that cause cyber conflicts in businesses? What should be the strategic principles that can be adopted in managing these conflicts? What is the theoretical basis for the strategic cyber conflict management of businesses?

After the determination of the research questions, the interview questions to be performed with the participants were determined (appendix). While determining the Interview questions, research questions were taken as the basis. These questions were asked during an approximately one-hour meeting/interview with the participants. In order to fill the theoretical gaps, different questions were also asked in cases where theoretical sampling was required and according to the information obtained through memo-writing.

Ethical Rules and Implication

The study was approved by the ethics committee of the [blinded for review] University. Participants were informed that participating in the interview was voluntary, that they could end the interview at any stage of the research, and that their information would be kept confidential. All information about the research was explained to the participants clearly and without any doubt before the interview. In addition, all necessary measures were taken during the coding and memo-writing phase to keep the information of the participants confidential and personal information was anonymized.

Pre-Sampling

The sampling method recommended in the implementation of the grounded theory is purposive sampling (Palinkas et al., 2015; Robinson, 2014). In this method, the sample size suitable for the purpose of the study is determined (Draucker et al., 2007). Senior and IT managers of businesses have information in determining the cyber conflict management strategy. In order to reach this sample population, joint-stock and limited companies operating in Turkey and registered to the chambers of commerce and industry were included in the sample. Among these businesses, those who use virtual merchandising, automation in production,

and robotic technology and have cyberinfrastructure in the service sector were selected. Since qualitative research causes an important constraint in the context of time, Adana, Muğla, Ankara, İstanbul, İzmir, İzmit, and Antalya provinces with the highest number of joint-stock and limited companies were preferred in sample selection. The communication and sectoral information of the companies were obtained from the trade registry directorates in accordance with the Law on Protection of Personal Data in force in Turkey. An invitation was sent to the participants via phone, Whats App, LinkedIn, e-mail, google form, and Skype about the interviews to be held with the sample.

The number of companies targeted and accessed for pre-sampling, together with their sectoral information is presented in Table 2.

Table 2. Pre-sampling findings

Provinces	**N^{tc}**	**N^{ac}**	**Sector**	
			Service	**Manufacturing**
Adana	90	72	32	40
Muğla	50	43	19	24
Ankara	150	91	36	55
İstanbul	200	89	32	57
İzmir	130	75	37	38
İzmit	270	112	46	66
Antalya	190	92	39	53
	1080	574	241	333

N^{tc}: Number of targeted companies; Nac: Number of accessed companies

Two employees from each company were selected in the sample selection to be included in the interview. Two basic executive profiles were identified (IT department manager, company senior manager) who had information about strategic cyber conflict management. 43 companies that did not meet these two criteria were excluded from the study. Among the participants included in the interview, senior managers consisted of the businesses' CEO, chairman of the board, and general managers had detailed information about the cyber conflict management and strategies of the company they were affiliated with. Both employees were included in the interview together and at the same time (in the same session, separately).

In order to minimize the time constraint of the grounded theory and the distribution error in the representation of data from each unit in the sample, the number of participants to be interviewed in each company was limited. The generalizability and reliability of the data depend on increasing the sample size and the fact that the statistical contribution of each unit included in the sample is equal with the other units.

Interviews

The research was carried out in 2021. The data collection, theoretical sampling, and analysis of the research took approximately 3.5 months. Interviews were conducted with an average of 8-9 (169 per month) businesses every day during the week (1st month: 174; 2nd month: 181; 3rd and the last month: 219+19). At the end of the second month of the research, 19 more businesses were included in the study in accordance with the theoretical sampling and memo-writing. Data were recorded and coded after each interview.

Research data were collected through semi-structured questions. Interviews were carried out with the IT department manager of the businesses and the senior manager of the company. The data obtained through the research were recorded through digital applications and tools. Interviews were carried out in accordance with COVID-19 measures. Zoom, Google meet, Skype, Whats App, Microsoft Teams applications were used for data collection and interviews. Participants were informed that the interviews were recorded in accordance with the Law on Protection of Personal Data. Participants were informed that they could refuse to record these interviews. The participants were informed about the links, ID, and password about the interview at least five days before the interview. After the interviews, the researcher took notes and processed the data related to the recorded interviews in the digital environment.

DATA ANALYTICS

Data analysis consists of the analysis steps performed until the illustration of concepts and constructing theory stage. This process requires coding (open, axial, and selective coding), theoretical memo-writing, quality analysis of findings, analysis and interpretation stages (Birks & Mills, 2015).

Coding

Open Coding

Open coding includes the process of extracting the raw data required in the construction of the theory, uncovering and categorizing the phenomena (Vollstedt & Rezat, 2019). The obtained raw data are analyzed in the context of similarity and difference. Data is extracted, labeled, encoded, and categorized. The extraction of raw data is performed by determining the central categories that attract them like a magnet. It is important to determine the phenomenon in the extraction. For this reason, sentences have been reduced to words, words to labels, labels to concepts, concepts to phenomena, and phenomena to categories. Thus, the first stage of coding was performed (Walker & Myrick, 2006).

The open coding process was carried out in three stages. Findings of the first open coding stage are presented in table 3.

Table 3. The findings of the first stage of open coding

Raw data	Data extraction	Phenomena	SC
Identifying cyber conflict.	Differences of opinion on issues such as agreement, data management, negotiation, operation, sales, marketing, production, service.	Cyber conflict is the disagreement, a clash of opposing needs or feelings, incompatibility situations that arise through elements such as negotiation, communication, competition, interaction, attack.	Determining cyber conflict within the system and in cyberspace
The types of cyber conflict that the business face.	Competition, institutionalism, operational, functional, strategic, infrastructure, negotiation	Businesses may conflict with the stakeholders, consumers, malicious attackers, and the system that they interact with.	Identifying and managing cyber conflict within the system
Solution recommendations for the cyber conflicts faced by the business.	Protecting, updating, and improvement of digital infrastructure, training, improvement of negotiations, strategy development, employment of qualified employees to fight against cybersecurity threats.	Businesses can resolve conflicts arising in social media, virtual communication, online negotiations and meetings, operational processes and production with training, infrastructure improvement, and effective human resources management.	Ensuring cybersecurity, education, improvement, and updating.
How the cyber conflicts being determined.	Employee, project reports, feedbacks, robotic automation, cobots (collaborative robots), email, virtual applications, web site	Cyber conflicts can be detected by companies' internal reporting, automation, cyberinfrastructure, and feedback.	System and cyber tools management

SC: Sub Categories (Grouping as a result of tagging)

The findings of the second open coding stage are presented in table 4.

Table 4. The findings of the second stage of open coding

Raw data (Q1)	Data extraction	Phenomena	SC
Criteria that enable the identification of cyber conflicts.	Results contrary to the goals and objectives adopted in negotiations and agreements, negative statements, negative outputs, deviations from the set target, failure.	Cyber conflicts are situations that result in failure and negative outputs in the context of negotiation, agreement, relationship, and operation in businesses.	Perceptual and detection-based criteria in cyber conflict management.
Key factors leading to the emergence of cyber conflict.	Digital and cyberinfrastructure weaknesses (software, transformation, IoT, and IIoT errors), information security risks, information deficiencies, perceptual errors, administrative and user errors, interpersonal negotiation tactic errors, cultural differences, social media.	Information, communication, culture, psychology, social media, and the organizational climate of the business are key factors in the emergence of cyber conflict.	Perceptual and detection-based criteria in cyber conflict management.
Difficulties in identifying key factors that led to the emergence of cyber conflict.	Ending the negotiation by the other party, psychological factors, legal factors, being a weak party in the agreement, perceptual difficulties, lack of education, weakness in digital transformation, depersonalization.	Ending the negotiations or internal and external factors that drive actors into conflict makes it difficult to identify key factors that lead to the emergence of cyber conflict.	Difficulty/struggling management in conflict resolution
Strategies and methods adopted to manage cyber conflict	Continuation of negotiations, rewarding those who detect cyber vulnerabilities and conflicts, sustainable education, developing and adopting corporate principles regarding information privacy, strengthening cyberinfrastructure, cooperation with cyber stakeholders, sustainability, mergers, and consortium	Negotiation, cyber threats, information privacy, cyberinfrastructure, cooperation-oriented corporate strategies are adopted in businesses.	Sustainability + empowerment + collaboration

SC: Sub Categories (Grouping as a result of tagging)

The findings of the final stage of open coding are shown in Table 5.

Axial Coding

Axial coding is a transition process in coding where main categories are associated with subcategories. This coding enables the determination of the central categories that determine the contribution of the cause and effect of the phenomenon to the theoretical structure through the paradigm model (Vollstedt & Rezat, 2019). Central categories are associated due to their practical contribution to the theoretical structure. Attracting (center) categories and sub-categories obtained after this stage play an important and mediating role in revealing selective coding (Kendall, 1999). The findings of axial coding are shown in table 6.

Selective Coding

Selective coding is an important coding process in constructing the theory. This type of coding involves linking categories, creating orbit categories, and associating the central category with these categories (Vollstedt & Rezat, 2019). The findings obtained from

Table 5. The third stage of open coding findings

Raw data (Q1)	Data extraction	Phenomena	SC
Importance and effects of methods adopted in cyber conflict management; experiences and deviations.	The methods of cyber conflict management are effective in the stakeholder-business-leader triangle. Sustainability, cybersecurity vulnerabilities are not always predictable. When financial, legal, social, cultural, identity, entrepreneurship interests conflict, deviations are encountered.	In the management of cyber conflicts, deviations may occur due to the factors required by the interests of the business.	Managerial deviations and management of illusions.
Flexibility in methods and strategies.	Crisis management, reactive behaviors, updating cyberinfrastructure, leadership qualities, human resources management.	Strategy and managerial deviations require flexibility.	Strategic flexibility + crisis management
Problems arising in cyber conflict management.	Conflicts of interest may arise between the employee-leader, employee-customer, employee-business, customer-business, stakeholder-business, parties of the negotiation. Financial and reputational losses due to operational time losses. Human resource issues.	Cyber conflicts can cause conflicts of interest and some losses in the business.	Conflict of interest management + time dilation management

SC: Sub Categories (Grouping as a result of tagging)

Table 6. Axial Coding findings

AC	Negotiation Conflict	Managerial Conflict	Infrastructure Conflict	Defense Conflict	Competition Conflict
Sub (Orbit) Categories	Inter-team conflicts	Project management	Technological infrastructure	Cyberattacks	Malicious attacks
	Business-stakeholder conflicts	Conflicts between departments	Digital infrastructure	Cybercrime	Operational Security
	Business-customer conflicts	Leader-employee conflicts	Cyber transformation conflict	Cyberterrorism	Cybersecurity Threats
	Employee-customer conflicts	Institutionalism	Virtual applications	Data and Information Security	Virtual entrepreneurship and cyber innovation
	Depersonalization / derealization	Human Resources Management	Human Resources Management	Application and Software Security	Virtual market entry conflict
		Organizational virtual climate	Technology transfer	Network and Communication Security	Company mergers and consortium

AC: Attracting (Center) Categories

the open and axial coding analysis of the phenomenon representing the research questions enabled a central and general framework about the theory to be depicted through selective coding. Relativity theory was taken as the basis in the creation of this picture. Findings of selective coding are presented in table 7.

Orbit categories were created by associating the findings of the codification of the obtained data with the relativity theory principles. Strategic categories and orbit categories in the cyber conflict were put forward after this association process. Location in space, the relativity of time, warping spacetime, gravitational lens reflect the principles of the relativity theory.

Table 7. Final Results of Selective Coding

(Orbit) Categories	Central Category	Definition
Business within the system (location in space)	Relativity of Strategic Cyber Conflict Management (SCCM)	Businesses are organizations that encounter cyber conflict in legal, economic, social, virtual, sectoral systems. Determining the position of businesses in systems is important and necessary in resolving and managing conflicts.
Business within the cyber cosmos (relativity of time)		Businesses are constantly evolving in the cyber world. Digital innovations, cybersecurity risks, cyber transformation are the relative key factors in establishing strategies and developing cyberinfrastructure.
Warping spacetime due to cyber conflict (Curvature of strategy).		When the strategies and methods determined in cyber conflict encounter an obstacle, they warp by changing direction (deviation from strategy). After this warping, cyber conflict management should be directed to its former position with an emergency action plan.
Illusions due to cyber conflict (Gravitational lens)		Perception is important in achieving the goal in cyber conflict management. Deviations and obstacles from strategy cause perceptual illusions of the business observer.

The cyber cosmos stated in the relativity of time symbolizes the Japanese word "Yūgen". "Yūgen", a Japanese aesthetic concept, represents a mysterious, dim, and deep sense of the beauty of the universe. According to this opinion, the suffering of people has beautiful aspects. In the cyber cosmos, the negative situations that occur after the cyber-attacks are faced by the businesses strengthen the businesses in a strategic context. Relativity symbolizes the sustainability of this power and the ability to cope with possible obstacles.

Theoretical Memo-Writing

The data obtained in the codification process, which is the most important step in constructing a theory with the principles of grounded theory, is interpreted through theoretical memo-writing. During or after the interview, the meanings, contradictions, questions, uncertainties, and interesting issues attributed to the raw data by the researchers and participants are noted and recorded. During the analysis process, the adequacy of the coding and sample is revealed by memo-writing. This method reveals the saturation status of the researcher regarding the analysis and sample. Coding, association, category, and classification are performed reliably through theoretical memo-writing.

The theoretical memo-writing provides observational evidence during the interview. The emotional states of the participants, body movements, emphasis on words, avoidance of answering reveal the reactions of the participants regarding the researched phenomenon. These reactions and situations are recorded by this method.

During the memo-writing phase, it was determined that the participants used expressions reflecting relativity in their statements regarding the determination and implementation of the cyber conflict strategy. In addition, illusions in conflicts, strategic deviations, and infinity of strategy were recurring issues. This situation played an important role in relating to the principles of relativity theory. In addition, the conditions required by theoretical sampling to achieve saturation in the formation of the theory were determined by theoretical memo-writing (table 8).

Theoretical Sampling

The theoretical sampling method was applied in the study. In this sampling method, data collection continues throughout the analysis until theoretical saturation (Conlon, et al., 2020). Intentional, systematic, and random sampling techniques were applied in a mixed manner, as suggested by Strauss and Corbin (1997). The

Table 8. Sample of theoretical memo-writing analysis.

Raw Data	Memo-Writing analysis / Notes
Cloud computing vulnerability attacks are causing great financial damage to the business. We often experience theft of intellectual property and cryptography problems. This situation affects our legal and economic position.	Emphasis is placed on the position of the business within the systems. System perception should be investigated in business management.
Employees' psychology is manipulated by means of ransomware or phishing. Hackers demand payment for the release of infected data. However, often our competitors do this. This causes us to deviate from the target strategically.	This is an expression regarding illusions and deviations in cyber conflicts. More evidence is needed.
The most common problem in automation is the denial-of-service attack. The security of cyber applications causes conflicts in the operational and production processes we carry out through mobile computing. We use virtual reality applications to reduce and end conflicts. We also benefit from virtual applications in bilateral agreements…. The British have an idiom: If you do not want to flog a dead horse, you must reduce or eliminate the conflict immediately….	Emphasis is placed on the impact of virtual reality on reducing conflicts. It is also emphasized that the conflict should not be prolonged in terms of time.
The business' internet, digital and virtual network provides information about the causes of the conflict. The most common problems in conflict arise due to errors in the Wi-Fi network, industrial internet of things. Manufacturing-as-a-Service can eliminate the margin of error and errors in these conflicts.	Illusions related to cyber conflict are mentioned. The relativity and solution recommendations of this situation should be investigated.
Social media accounts and e-blogs are the most important places where conflicts arise with customers, stakeholders, and malicious cyber attackers. Cybercrime cases such as hate speech and hacking create critical conflicts. Statements that do not belong to the business create a perception of conflict in third parties. Moreover, this differs from time to time.	Conflict perception that changes with time. Perception varies according to the actors. This issue should be investigated in different samples.
We are experiencing conflicts in our export relationship with many countries due to fear of cyber terrorism. Cultural, legal, digital, and social changes cause changes and mistakes in our strategies.	It is mentioned about deviations and obstacles in cyber conflict management. More information needs to be gathered on this subject (Theoretical sampling).

Table 9. Theoretical sampling variables

Provinces	**N^{ac}**	**Sector**	
		Service	**Manufacturing**
Adana	1	0	1
Muğla	1	0	1
Ankara	4	1	3
İstanbul	4	1	3
İzmir	5	1	4
İzmit	3	0	3
Antalya	1	0	1
TS^t	19	3	16
$PreS^t$	574	241	333
Total	593	244	349

N^{ac}: Number of accessed companies; TS^t: Total theoretical sampling

$PreS^t$: Total Pre-sampling

intentional sampling technique is performed to reach sampling related to the categories to be determined. The systematic sampling technique enables the detection of similarities and differences between concepts and categories. The random sampling technique enables the inclusion of probabilistic coincidences to the theory in determining the sub and central categories of the theory to be revealed (Butler, Copnell, & Hall, 2018).

Elimination of contradictions that arise in coding and theoretical memo-writing stages, analyzing new phenomena, clarifying the relationships between categories, elimination of classification errors, confirming the relations between sub-central categories, elimination of uncertainties (filling the gaps) that arise in the formation of a new theoretical structure are accomplished through theoretical sampling (Braun & Clarke, 2021). Due to the theoretical sampling requirement that emerged after pre-sampling, 19 more businesses were interviewed (Table 9). Theoretical sampling was applied to obtain more detailed information about the perception of conflict over time, perceptual differences of deviations in cyber conflict strategy, system perception in business management and to fill the coding gaps that emerged.

Quality Analysis of Findings

In qualitative research, the quality of the data obtained as a result of analysis and coding provides information about the reliability of the results. In order to ensure reliability in the results, personal information was kept separate from the data included in the analysis in the processing of data. Cybersecurity of data recorded in a digital environment was ensured. Theoretical memo-writing and raw data were recorded in a short time after the interview.

The anonymized data were delivered over to a team of seven experts for interpretation in order to ensure objectivity in the interpretation and coding of the data, association, and formation of the theoretical structure. The interview duration was limited to an average of one hour in order to avoid any deviation in the interpretation of the obtained data. Participants were advised to take a short break during the interview. Thus, it was tried to eliminate the negative stimulation of the participants about the research subject psychologically.

Analysis and Interpretation

Analysis and interpretation is the evaluation of data obtained from codification, association, categorization, theoretical memo-writing, theoretical sampling stages (Birks & Mills, 2015). At this stage, small pictures are combined to create the picture that reveals the whole puzzle. The theoretical structure is constructed by interpreting this picture and the small pictures that make up the picture together (Bryant, 2017).

Illustration of Concepts and Constructing Theory

The construction of the theory depends on reaching saturation of the data emerging during the analysis process. Saturation depends on the integrity of the picture that emerges in taking the steps in the analysis and the level of representation of the parts that make up the integrity (Bryant & Charmaz, 2007). The codes obtained in the analysis phase consist of the pixels of the big picture, and the categories consist of modules. The theory reflects the big picture made up of these small parts. Different pictures and models obtained in coding, theoretical memo-writing, and theoretical sampling stages are transformed into a single picture via illustration of concepts and constructing theory (Charmaz, 2014).

In order to construct a substantive theory, the researcher needs to reach saturation about the research subject/phenomenon, new theory, associations, and interpretations. When the data obtained from the participants are repeated and the theoretical gaps are completed, steps are taken regarding the stages of customizing the code system, category building, illustration of concepts, and constructing theory (Strauss & Corbin, 1997). In the analysis process, theoretical sampling should not be performed at a level that exceeds the objective of the research. The sampling that exceeds the objective may negatively affect the deviations in theoretical saturation and the reliability of the results (Walker & Myrick, 2006). For this reason, steps in accordance with these rules were taken during the research and analysis process.

The consistency of the data obtained as a result of the analysis during the theory constructing phase was re-analyzed. At this stage, the notes obtained through theoretical memo-writing were compared with the final analysis findings, and the quality of the analysis results was analyzed. Consistency was detected and theoretical saturation was provided. The results revealed the relativity theory of strategic cyber conflict management.

Five Orbital Forces of Cyber Conflict

The findings of the research showed that the five orbital forces were attracted to cyber conflict. These orbital forces (negotiation, managerial, infrastructure, defense, competition) create significant accelerations in the context of strategic management in the cyber conflicts of businesses (figure 3).

Figure 3. Five Orbital Forces of Cyber Conflict

Creating a strategy in cyber conflict management (CCM) depends on sustainability, investigation of the cause-effect relationships of the conflict, defining the system in which the business is involved (located), and taking measures to reduce or end the conflict.

Negotiation Conflict

The research results demonstrated that negotiation is a factor in the strategic CCM that could end, mitigate, or cause new conflicts. This conflict includes conflicts that may arise between teams. There may be differences of opinion between people in teamwork in businesses. Employees may experience conflicts for many reasons such as competition, career development, award, and prestige.

Businesses are in contact with suppliers, company partners, shareholders, social responsibility actors, and project stakeholders. These stakeholders may experience conflicts according to the benefit-loss, contribution-loss balance of the businesses. Participants stated that many actors from stakeholders and beyond were experiencing problems due to the damage businesses cause to the environment. It was stated by the participants that reducing these conflicts depends on cooperation with stakeholders and projects should be developed in this context.

Customers are at the forefront of the conflict strategy in the context of profitability and sustainability of businesses. The results of the research revealed that employee conflicts are often experienced in product diversification strategies. Customers' expectations, the rate of return of complaints, after-sales services, negotiation problems in the digital environment, the sharing of personal data recorded in the company's digital database with third parties, and security weaknesses that emerged after cyberattacks were stated as the major causes of cyber conflict.

Depersonalization/derealization occurs when negotiation requires an intense effort or when the fighting power of the individual is weak. Participants reported that deliberative cyber conflicts arise especially among women and people with executive or leader status. The reason for this was stated as those women were constantly subjected to digital assault and violence. On the other hand, it was stated that the busy pace of work, the belief that negotiations would not yield results, and having a low level of commitment to the workplace desensitized the employees against conflicts. In addition, stress, unfair practices in the workplace, lack of cyberinfrastructure were reported by the participants as other causes of depersonalization/derealization.

Managerial Conflict

Research findings showed that the cyber aspect of the managerial conflict was related to project management, interdepartmental conflicts, leader-employee conflicts, institutionalism, human resource management, and organizational virtual climate. Project management can be carried out with the virtual network of the business. In zoom, google meet, skype, and other similar virtual meeting applications, reasons such as connection breaks, low connection quality, infrastructure deficiencies, participation from home environment cause conflicts in project management.

Another type of managerial conflict is interdepartmental conflict. Departments are units in which functions such as operations, logistics, law, human resources, sales, after-sales services, marketing, procurement-purchasing are carried out. E-mail errors between these units, e-mails causing cyber attacks, and informal addressing between parties style cause cyber conflicts.

According to the participants, the leader-employee conflicts, e-mail correspondence, informal addressing, ignoring the subordinate-superior relationship, using the video-call function of the smartphone applications against the purpose cause cyber conflicts. On the other hand, the institutional structure of the businesses was specified as a managerial cause of cyber conflict. Participants directly associated institutionalism with human resources and training in the context of cyber conflict. It was emphasized that employees in human resources management should be trained for the elimination or reduction of cyber conflicts, and awareness-raising about cyber-attacks should be made.

Organizational climate is related to the perception of the employee in the organization, mood, workplace environment, management practices, and working conditions. The findings confirmed the existence of a virtual climate within the organization. The participants emphasized that the virtual application and cyberinfrastructure should be suitable for the mood of the employees, and applications that would keep them away from boredom and negative effects should be preferred. On the other hand, in virtual meetings and negotiations, it was stated by the participants that the factors that cause perceiving false of the employee or the stakeholders of the business in the context of virtual management should be eliminated. For instance, it was suggested by the participants not to send persistent emails bearing the traces of mobbing, to give equal right to speak to all employees in the teleconferencing method, to protect the digital devices of the employees and the business against cyber and malicious attacks, and to ensure compliance with digital transformation in cyberinfrastructure.

Infrastructure Conflict

Business infrastructure fulfills important functions in managing resources and channeling them to relevant units. The findings of the study showed that infrastructure issues in the cyber conflict were related to technology, digital, cyber transformation, virtual applications, human resource management, and technology transfer. Participants stated that deficiencies in technological, digital, and cyberinfrastructure triggered conflict in cyber negotiation, communication, and interaction.

Virtual meetings with stakeholders, general assembly discussions, meetings with employees, live broadcasting on social media, broadcasting of advertisements in a digital environment, the functional infrastructure of the website, accessibility to social media accounts, technical problems in robotics, and automation can cause conflicts. According to the participants, cyber problems experienced in automation and robot applications in production can cause serious complaints and customer losses in product delivery.

Participants associated human resources management with both managerial and infrastructure conflicts. This is because human resources are both a solution and a node point in cyber conflicts. The findings showed that determining certain principles regarding the cyber conflict in human resources management would prevent possible conflicts and eliminate existing conflicts. It was stated that in many companies where training on cyber conflict in human resources management was provided, there was a decrease in conflicts.

Technological infrastructure is one of the most basic requirements of a business. Especially businesses operating in the manufacturing sector apply to technology transfer for product diversification, prototype, design, and to provide innovation to the business. Participants stated that technology transfer supported and improved the cyberinfrastructure of the business and was effective in reducing cyber conflict. Website and product design, innovative product, and service design were reported by participants as factors that reduce conflicts in the context of customers and stakeholders.

Defense Conflict

Research findings revealed that businesses were exposed to attacks such as cyberattacks, cybercrime, and cyberterrorism. Participants reported that such attacks posed a serious threat and risk to businesses and caused major conflicts in their relationships with customers and stakeholders. For this reason, data and information security are important in preventing cyber conflicts in businesses. On the other hand, it was stated by the participants that the security of digital elements in the website, automation, robot applications, and business infrastructure should be protected in the context of application and software.

The exposure of businesses to cyber-attacks and cybersecurity risks causes them to take a defensive position in their relations with customers and stakeholders. Participants believed that cyberattacks could be eliminated with defense strategies for the business, stakeholders, business infrastructure, and employees. Another factor that causes defense in cyber conflict is the network and communication security risk. Automation and communication in the manufacturing sector, communication, and marketing functions in the service sector are significantly affected by this factor. Participants stated that this defense factor created conflict with the customers and stakeholders with whom the business was in contact in the procurement, production, distribution, and marketing of products. The emergence of these conflicts causes businesses to fight for prestige against actors inside and outside the organization. Therefore, businesses take a defensive position for profitability, efficiency, performance, sustainability, and cybersecurity.

Competitive Conflict

Businesses are in active competition for the realization of economic goals. Research findings revealed that this competitive situation was caused by malicious attacks in cyber conflicts, operational security, cybersecurity threats, virtual entrepreneurship and innovation, virtual market entry conflict, company mergers, and consortium. Participants stated that malicious attacks were carried out by competing businesses to weaken the business's competitiveness, damaged its commercial reputation, and ensured that it withdrew from the market, and in this case, it caused conflicts between the victim business and the attacker business.

Operational Security is a form of risk management that aims to protect business operations by protecting business managers from competing businesses and malicious cyber attackers. Applications and networks with high-security risks such as projects, customers, production planning, cyberinfrastructure must be procedurally protected. This risk management is also important for cybersecurity threats.

Research findings showed that cyber innovation and entrepreneurship cause competitive conflict in businesses selling through cyber virtual stores. This conflict also causes disputes with rival businesses in entering the virtual market, which is under the influence of social media.

It is common for businesses to apply for mergers and consortia in resource dependency. Participants highlighted the conflict of cyber roles among businesses regarding this situation. Cyber roles were specified by the participants as managerial problems in the use of cyber and digital tools such as social media, virtual networks, virtual applications specified in the partnership or merger agreements of the businesses. The most experienced cyber conflicts were stated as social media posts, virtual advertisements, and virtual promotion activities.

Relativity of Strategic Cyber Conflict Management

The findings obtained as a result of the coding enabled the relativity approach in management and strategy to be constructed theoretically. While constructing the theoretical structure, the principles of relativity theory in different branches of science were taken into consideration. The similarity of the data obtained as a result of our research to the relativity theory inspired the name given to the theory. Although the five orbital forces of cyber conflict reveal important principles in strategy formulation, it was found as a result of our research that these principles were strategically under the theoretical structure.

The structure that emerges as a result of coding qualitative data reveals relativity. In the light of these findings, businesses are organizations in the cyber cosmos and systems such as economy, law, social, culture, sector. Cyber cosmos is an unlimited area of the digital world that provides speed of operation and access for businesses and individuals such as innovation, communication networks, virtual applications, virtual reality, robotics. This area eliminates physical, functional, interactional, and communicative distances in businesses. For this reason, businesses are cyber, legal, organizational, purposeful entities within the systems and cyber cosmos (figure 4).

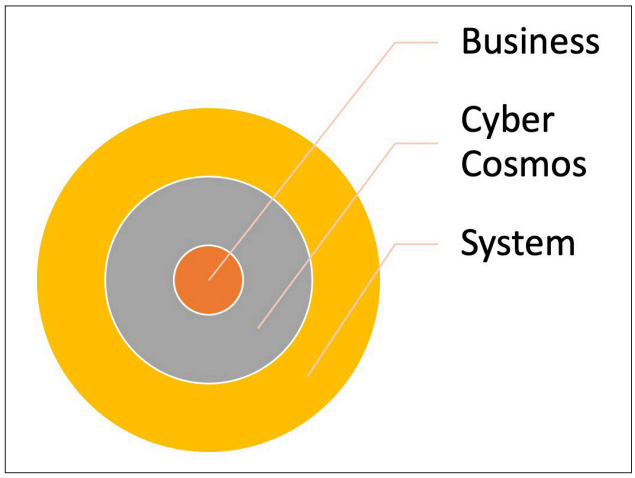

Figure 4. Cyber business within the system

Businesses in the cyber cosmos should develop strategic management principles in cyber conflicts that arise. The research results revealed that these principles were four basic principles that should be applied depending on the five orbital forces of cyber conflict (figure 5). These principles are business within the system (location in space), the business within the cyber cosmos (relativity of time), warping spacetime due to cyber conflict (curvature of strategy), and illusions due to cyber conflict (gravitational lens).

Business within the System (Location in Space)

Location in space, which is the first principle of the created theoretical structure, is related to the determination of the position of the business in the systems. Businesses can constitute subclasses of many classes such as law, culture, industry, economy, social media. In terms of determining the actors, possible attackers, and solutions, in conflict management, which of these systems businesses are included is important. Businesses pull (attract) or push businesses around them. This situation was associated with the proximity of suppliers, customers, and stakeholders to businesses in the research findings. Thus, the rules of the system in which the business is located, the strength of the conflict, and the high level of competition play a leading role in determining the strategy.

Business within the Cyber Cosmos (Relativity of Time)

The results of the research revealed that the adaptation of businesses to the changing and developing world conditions was important in achieving the strategies and targets. This ability to adapt is important in the context of dealing with conflict risks arising in the cyber cosmos. Time relativity requires businesses to keep history charts in cyber conflicts. Employees, managers, business with their institutional features, stakeholders, customers, and consumers change their views on the business-adaptation balance over time. This change should be recorded in the determined strategies, and the emerging differences and business-related developments should be kept on the agenda. Participants explained these differences, which change over time, with the expectations of customers about virtual reality and applications.

Warping Spacetime Due to Cyber Conflict (Curvature of Strategy)

When faced with an obstacle, the strategies determined by businesses regarding cyber conflicts change direction, they do disappear. Participants stated that the strategies of businesses in this direction would not end even if the business was closed, and could be a source of inspiration for other businesses. Therefore, the strategy creates an infinite light effect within the cyber cosmos and system (infinity of strategy). The results of the research revealed that the obstacles that emerged were malware, changes

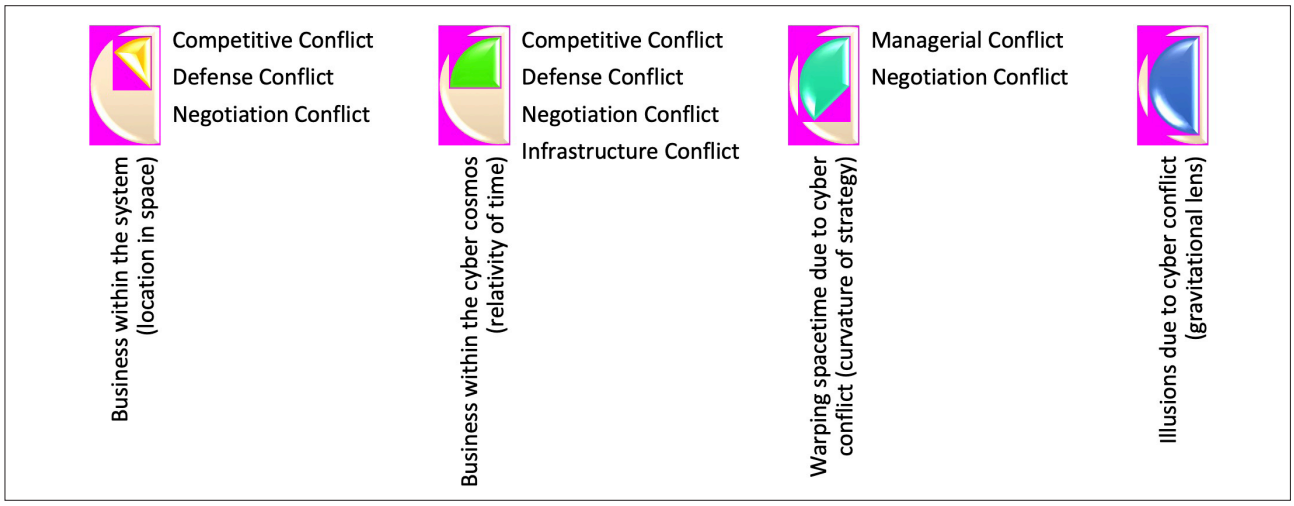

Figure 5. Relativity of Strategic Cyber Conflict Management

in cyber attacks, loss of cyber adaptability of the business, and unwillingness to negotiate with the conflict parties.

In CCM, deviation from the strategy can be improved by using an emergency action plan or using alternative routes. Participants gave examples regarding this situation, such as problems in encryption and software engineering, infrastructural problems arising in negotiations, communication problems caused by managers, and virtual interaction problems with stakeholders.

Illusions Due to Cyber Conflict (Gravitational Lens)

Perception is an important factor in CCM. Managers may be perceptually mistaken about the direction and resolution of the deviation in strategy. Misperception is linked to the obstacle, event, means of conflict, actors. Despite the implementation of negotiation methods, the termination of negotiations by the other party and misunderstanding of virtual correspondence due to cultural differences can cause perception errors. Participants stated that connection problems, emojis, and informal writing forms caused errors in communication during the interviews conducted via virtual applications. In addition, it was stated that the sensitivity to the words and sentences used in the compensatory negotiations and meetings for the elimination of conflicts was higher than the previous interviews.

The level of error (misunderstanding/misperception) in negotiation depends on whether the negotiation is synchronous or asynchronous. Since the interaction is instantaneous in synchronous negotiation, perceptual errors can be turned into solutions in the later stages of the negotiation. However, in asynchronous negotiation, the maintenance of the interaction is not synchronous, so action cannot be provided to resolve the error most of the time.

The perception of the unsuccessful methods used in reducing and ending cyber conflicts as successful by the managers puts the conflicts in an impasse. According to the data obtained from the participants, managers often acted on the basis of their past experiences. Many managers fall victim to their traits. Individuals with poor empathy skills, overly sensitive, emotional, and aggressive characteristics may be mistaken about conflict. This situation can negatively affect the success of the applied strategy.

DISCUSSION

Cyber conflict is reflected in the literature as a type of conflict that threatens the economies of the country and is related to security vulnerabilities and cyber attacks. According to this approach, cyber conflict is carried out on states, online organizations, hackers, and malicious software. Hate speech, discrimination, cyber attacks, cyberwar, law, and ethical issues are prominent types of conflict that this approach puts forward.

Studies on CCMs of businesses are related to cyber espionage, cyber warfare, and law (Akoto, 2021). These studies revealed that financial and telecommunication companies were targeted with cyber-attacks and aimed to harm the country's economy (Junio, 2013; Karatzogianni, 2008). Valeriano & Maness (2014) demonstrated the competitive dimension of this conflict in the context of cyber warfare between states. This approach was followed by cyber defense strategies (Shi et al., 2007; Heckman et al., 2013; Denning, 2014; Xu, Lu, & Li, 2015; Lu, Xu, & Yi, 2013). These studies focus on general issues such as law, government, cyber warfare.

Studies that reduce traditional conflict management approach to private are limited. Cebula & Young (2010) contributed to the reduction to private of the traditional cyber conflict approach and revealed that operational cybersecurity risks consist of technology failures, individual actions, systems, external events. Another study that highlighted individual actions was carried out by Ishii (2010). This study revealed that the cooperative-based cyber management approach was preferred among students in the event of cyber conflict.

Applegate & Stavrou (2013), which handled conflict management as individuals, systems, and events, proposed cyber conflict taxonomy. Taxonomy included forms of classification that defined the events, actors, and subjects of the taxonomy that gave rise to the conflict. Although taxonomy added a new dimension to cyber conflict, it could not provide empirical evidence and go beyond conceptual explanations. This classification form, which is beneficial in understanding complex relationships and categorizing the systemic structure, cannot offer a strategic perspective in cyber conflict.

The cyber conflict has become increasingly complex in the context of organizations, businesses, individuals, states, classes, and society. Studies on CCM cannot go beyond concepts such as inter-state war, espionage, cyber attack, malicious / ransomware, and cybersecurity. Putting forward the function and role of businesses as

an economic organization in cyber conflict, developing a strategy and theory, will provide competitive power for businesses in today's complex cyber cosmos.

This study revealed the relativity approach that enables businesses to develop strategies in cyber conflicts. A strategic management approach was revealed with the research findings beyond an attack and vulnerability approach to CCM. The relativity approach, strategic management, and the handling of cyber conflict in the context of businesses reveal three theoretical foundations. Lack of theory development in the literature on CCM, in the context of implementation and strategy development, poses risks related to the cybersecurity of businesses.

CONCLUSION

The research results reveal a new theory in the field of cyber conflict management. This theory is the "relativity of strategic cyber conflict management". This theory was constructed so that businesses can develop a strategy that suits the needs of the cyber world. The negative effects of cyber attacks and threats on the relations of businesses with stakeholders and their environment and serious damage to the business infrastructure make it necessary to develop a strategy in this direction.

According to the results of the research, five orbital forces (negotiation, managerial, infrastructure, defense, competition) were determined in the CCM. These orbital forces also constitute types of conflict in businesses. Businesses enter into cyber conflicts through these orbital forces within the system and cyber cosmos. This result provides important insights into the causes and consequences of possible cyber conflicts internally and externally. For this reason, it is necessary to pay attention to the five orbital forces when developing strategies in cyber conflicts of businesses.

The theoretical foundation revealed by the research findings proves the four basic principles of CCM. The relativity approach determines the principles of this theory. Four principles were determined as a business within the system (location in space), the business within cyber cosmos (relativity of time), warping spacetime due to cyber conflict (Curvature of strategy), and illusions due to cyber conflict (Gravitational lenses). These principles are important in determining, implementing, and sustaining the strategic CCM of the business. Managers should pay attention to the deviations and obstacles experienced in cyber conflicts that arise in the business. It should be noted that cyber conflict is not just about the management of infrastructure and resources. The relativity according to time and perception, emergency action plans, the idea that strategy is an infinite light should be adopted by businesses. In addition, time-based perceptions and experiences should be recorded by establishing a history regarding cyber conflicts.

The results of the research show that the strategic CCM based on five orbital forces can achieve the competitive power of the business, promoting in the market, rapid adaptation to cyber developments, and success in negotiations. For this reason, it is suggested that the strategic management and human resources management of the businesses should be developed according to the strategic CCM. These practical contributions will help to determine the position of the business in the system and cyber cosmos.

For a successful CCM, attention should be paid to relativity in the issues of cyber communications, cyber and online negotiations, online conflicts, depersonalization, psychological, social, cultural, and institutional factors, technological and digital infrastructure, operations, human resources management, conflict in online meetings and negotiations, management strategy. In addition, since the interaction is not synchronous in asynchronous negotiation, communication with the parties should be maintained and feedback should be obtained in order to resolve the misperceptions.

In the context of human resources management, it is important to train employees on employment, orientation, organizational culture, and conflict in organizational climate. On the other hand, awareness should be created with continuous training, as procurement, logistics control, production-planning, legal procedures, after-sales services, marketing, promotion are business functions where cyber conflicts can occur frequently.

Despite the theoretical and practical contributions of the study, empirical studies in this direction should be increased. It is recommended to conduct studies according to the theory established on subjects such as performance, competitiveness, productivity, organizational climate, employee-leader interaction, social responsibility, organizational behavior, and workplace. In addition to introducing the relativity approach to the strategic CCM into the literature theoretically, it is suggested that future studies should be carried out empirically in different types of organizations (eg public sector, associations, foundations, voluntary organizations, etc.). Investigating symbiotic sharing

in this context can make important contributions in a practical context.

LIMITATIONS

The analysis stages of the grounded theory, which is the method adopted in the research, caused a significant amount of effort and time. Data collection, theoretical sampling, and coding steps were carried out equally, requiring a great deal of effort and time. For this reason, problems can often be experienced in the abstraction of data. Communication, internet, and network problems made it difficult to encode data in video conference calls with some participants. In addition, supporting the study with more empirical evidence would benefit the development of the theory.

REFERENCES

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. Journal of Peace Research. https://doi.org/10.1177/0022343320964549

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings.

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. Risk analysis, 26(4), 907-923.

Applegate, S. D., & Stavrou, A. (2013). Towards a cyber conflict taxonomy. In 2013 5th International Conference on Cyber Conflict (CYCON 2013) (pp. 1-18). IEEE.

Barrett, M., Davidson, E., Prabhu, J., & Vargo, S. L. (2015). Service innovation in the digital age. MIS quarterly, 39(1), 135-154.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 3(4-5), 353-364.

Bobo, L. (1983). Whites' opposition to busing: Symbolic racism or realistic group conflict?. journal of personality and social psychology, 45(6), 1196.

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. Qualitative research in sport, exercise and health, 13(2), 201-216.

Brief, A. P., Umphress, E. E., Dietz, J., Burrows, J. W., Butz, R. M., & Scholten, L. (2005). Community matters: Realistic group conflict theory and the impact of diversity. Academy of Management Journal, 48(5), 830-844.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal, 29(3), 408-433. https://doi.org/10.1108/13639510610684674

Bryant, A. (2017). Grounded theory and grounded theorizing: Pragmatism in research practice. Oxford University Press.

Bryant, A., & Charmaz, K. (Eds.). (2007). The Sage handbook of grounded theory. Sage.

Butler, A. E., Copnell, B., & Hall, H. (2018). The development of theoretical sampling in practice. Collegian, 25(5), 561-566.

Campbell, T. A., & Ivanova, O. S. (2013). 3D printing of multifunctional nanocomposites. Nano Today, 8(2), 119-120.

Caridi, M., Moretto, A., Perego, A., & Tumino, A. (2014). The benefits of supply chain visibility: A value assessment model. International Journal of Production Economics, 151, 1-19.

Carmigniani, J., Furht, B., Anisetti, M., Ceravolo, P., Damiani, E., & Ivkovic, M. (2011). Augmented reality technologies, systems and applications. Multimedia tools and applications, 51(1), 341-377.

Charmaz, K. (2014). Constructing grounded theory. Sage.

Charmaz, K. (2017). Special invited paper: Continuities, contradictions, and critical inquiry in grounded theory. International Journal of Qualitative Methods, 16(1), 1-8.

Conlon, C., Timonen, V., Elliott-O'Dare, C., O'Keeffe, S., & Foley, G. (2020). Confused about theoretical sampling? Engaging theoretical sampling in diverse grounded theory studies. Qualitative Health Research, 30(6), 947-959.

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. Connections, 16(2), 5-24.

Denning, D. E. (2014). Framework and principles for active cyber defense. Computers & Security, 40, 108-113.

Dipert, R. R. (2010). The ethics of cyberwarfare. Journal of Military Ethics, 9(4), 384-410.

Draucker, C. B., Martsolf, D. S., Ross, R., & Rusk, T. B. (2007). Theoretical sampling and category development in grounded theory. Qualitative health research, 17(8), 1137-1148.

Emig, C., Brandt, F., Kreuzer, S., & Abeck, S. (2007). Identity as a service–towards a service-oriented identity management architecture. In Meeting of the

European Network of Universities and Companies in Information and Communication Engineering (pp. 1-8). Springer, Berlin, Heidelberg.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1), 28-38.

Gayer, C. C., Landman, S., Halperin, E., & Bar-Tal, D. (2009). Overcoming psychological barriers to peaceful conflict resolution: The role of arguments about losses. Journal of Conflict Resolution, 53(6), 951-975.

Gompert, D. C., & Libicki, M. (2014). Cyber warfare and Sino-American crisis instability. Survival, 56(4), 7-22.

Heckman, K. E., Walsh, M. J., Stech, F. J., O'boyle, T. A., DiCato, S. R., & Herber, A. F. (2013). Active cyber defense with denial and deception: A cyber-wargame experiment. computers & security, 37, 72-77.

Ishii, K. (2010). Conflict management in online relationships. Cyberpsychology, Behavior, and Social Networking, 13(4), 365-370.

Junio, T. J. (2013). How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. Journal of Strategic Studies, 36(1), 125-133.

Karatzogianni, A. (2008). Cyber-conflict and global politics. Routledge.

Kato, S., Takeuchi, E., Ishiguro, Y., Ninomiya, Y., Takeda, K., & Hamada, T. (2015). An open approach to autonomous vehicles. IEEE Micro, 35(6), 60-68.

Kendall, J. (1999). Axial coding and the grounded theory controversy. Western journal of nursing research, 21(6), 743-757.

Lee, J., Ardakani, H. D., Yang, S., & Bagheri, B. (2015). Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. Procedia cirp, 38, 3-7.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853.

Li, X., Liang, X., Lu, R., Shen, X., Lin, X., & Zhu, H. (2012). Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Communications Magazine, 50(8), 38-45.

Li, R., Zhao, Z., Zhou, X., Ding, G., Chen, Y., Wang, Z., & Zhang, H. (2017). Intelligent 5G: When cellular networks meet artificial intelligence. IEEE Wireless communications, 24(5), 175-183.

Lin, H. (2012). Escalation dynamics and conflict termination in cyberspace. Strategic Studies Quarterly, 6(3), 46-70.

Lu, W., Xu, S., & Yi, X. (2013). Optimizing active cyber defense. In International Conference on Decision and Game Theory for Security (pp. 206-225). Springer, Cham.

Monostori, L. (2014). Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia Cirp, 17, 9-13.

Nelson, L. K. (2020). Computational grounded theory: A methodological framework. Sociological Methods & Research, 49(1), 3-42.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Administration and policy in mental health, 42(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. Computers in industry, 102, 14-22.

Rand, E. J. (2013). Queer critical rhetoric bites back. Western Journal of Communication, 77(5), 533-537.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. Qualitative research in psychology, 11(1), 25-41.

Rush, F. (2004). Critical Theory. Cambridge: Cambridge UP.

Shackelford, S. J. (2014). Managing cyber attacks in international law, business, and relations: In search of cyber peace. Cambridge University Press.

Sharma, S. K., Telfer, M., Phua, S. T., & Chandler, H. (2012). A pragmatic method for estimating greenhouse gas emissions from leakage for Improved Forest Management projects under the Verified Carbon Standard. Greenhouse Gas Measurement and Management, 2(1), 22-32.

Shi, L., Jia, C., Lü, S., & Liu, Z. (2007). Port and address hopping for active cyber-defense. In Pacific-Asia Workshop on Intelligence and Security Informatics (pp. 295-300). Springer, Berlin, Heidelberg.

Strauss, A., & Corbin, J. M. (1997). Grounded theory in practice. Sage.

Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. Contemporary Security Policy, 40(3), 368-381.

Walker, D., & Myrick, F. (2006). Grounded theory: An exploration of process and procedure. Qualitative health research, 16(4), 547-559.

Xu, S., Lu, W., & Li, H. (2015). A stochastic model of active cyber defense dynamics. Internet Mathematics, 11(1), 23-61.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. Journal of Peace Research, 51(3), 347–360. https://doi.org/10.1177/0022343313518940

Vollstedt, M., & Rezat, S. (2019). An introduction to grounded theory with a special focus on axial coding and the coding paradigm. Compendium for early career researchers in mathematics education, 13, 81-100.

Zollo, L., Roccella, S., Guglielmelli, E., Carrozza, M. C., & Dario, P. (2007). Biomechatronic design and control of an anthropomorphic artificial hand for prosthetic and robotic applications. IEEE/ASME Transactions On Mechatronics, 12(4), 418-429.

Appendix

Interview questions

S1. How would you define cyber conflict in your business?

S2. What are the cyber conflicts your business face? What are your suggestions for resolving these cyber conflicts?

S3. How do you identify the cyber conflicts your business face? What are the criteria that enable these cyber conflicts to be identified?

S4. What are the key factors leading to the emergence of cyber conflict? What difficulties do you have in determining these factors?

S5. What are the strategies and methods you adopt to manage cyber conflict?

S6. What is the importance and impact of the methods you apply in preventing cyber conflict? Have you ever experienced events where you needed to be flexible in methods and strategies?

S7. Could you share your experiences regarding the methods you adopted, in the context of achieving your goals? Have you encountered events/conditions that caused you to deviate from your goals?

S8. What are the problems that arise in cyber conflict management when you consider your business, the environment of your business, departments, employees, stakeholders, customers, suppliers, and all other elements together?