A Study on the Concept of Cyber Cognitive Warfare and Case Study Methodology From a Psychological Perspective

Kim Kibeom
Korea University Graduate School of Information Security, Seoul, Republic of Korea

nobody5262@gmail.com

Abstract: Cyber cognitive warfare, which manipulates the opponent's cognition to change behavior in inter-state warfare, is emerging as an important element with the advancement of science and technology. Human behavior is based on psychology, and psychology provides scientific grounds for cyber cognitive warfare, but existing cyber cognitive warfare studies have only determined the cause of behavior as cognitive manipulation, and there is no research interpreting it from a psychological perspective. Therefore, this paper presents a methodology that can explain the characteristics of cyber cognitive warfare from a psychological perspective and the mechanism by which behavior is changed through cognitive manipulation using Skinner's operant conditioning theory, a behavioral psychology. Skinner's operant conditioning theory is a theory that intentionally changes and reinforces behavior, and as it is a theory that has been proven to change behavior through various experimental results, we applied it to cases of inter-state cyber cognitive warfare such as the Russia-Ukraine War and interpreted the mechanism by which behavior is changed. In addition, in the process of interpreting the behavior change mechanism, we presented a control variable management plan based on the research results that behavioral results can vary depending on the influence of control variables such as the intervention of a third country. In conclusion, this study is expected to serve as a foundation for scientifically identifying the causes of behavioral changes through a case study methodology of cyber cognitive warfare from a psychological perspective, as cyber cognitive warfare is inherently invisible, gradually permeates the target, and by the time the impact is recognized, it is often too late to respond.

Keywords: Cybercognitive warfare, Human vulnerabilities, Psychology, Methodological study, Psychology warfare

1. Introduction

The warfare we face is rapidly changing in the concept of war and the methods of conducting warfare according to the speed of scientific and technological development. Cognitive warfare has developed into cyber cognitive warfare, in which the operational area has expanded to cyberspace and the operational means have also changed to digital.

Looking back at past history, we can see that cognition was utilized in various deception operations based on deception and surprise attacks, such as the ancient Trojan horse, Napoleon's Battle of Austerlitz, and the Normandy landings, and cognitive warfare was also incorporated into military theories, such as Liddell Hart's Strategy of Inderect approach and Sun-Tzu's Art of War. Recently, with the development of the information environment such as cyberspace, cyber cognitive warfare is often discussed in wars between countries, and discussions on cyber cognitive warfare are underway in the United States, NATO, China, and Russia.

Although physical conflicts between nations have decreased significantly except for localized battles, large and small conflicts and clashes continue to occur in cyberspace. In particular, with the expansion of the Internet and digital platforms (such as SNS), even simple disinformation such as narratives and propaganda, which are aspects of cyber cognitive warfare, can become powerful weapons.

2. Theoretical Background

2.1 Cyber Cognitive Warfare Existing Discourse and Limitations

The United States' joint and field manuals JCOIE (Joint Operational Concept for Information Environment), ATP 2-01.3, and TC 3-22.69 specify the basic theories of cyber cognitive warfare, such as cognition, decision-making, and human characteristics, and are described as an operation that spreads disinformation to influence cognition.

NATO newly views the cognitive domain as the sixth domain and is emphasizing cognitive warfare(Lea Kristina Bjørgul, 2021). It aims to change the way people think and act, influence beliefs, and force policies to favor the attacking nation.

China emphasizes that the leader's psychology and psychological stimulation have an impact on winning a war, and is developing a strategy that sets cyber cognitive warfare as an operation equivalent to the three wars (psychological warfare, public opinion warfare, and legal warfare) and that it can win a war by securing an advantage in the cognitive domain(Kwon Tae-young and Kim Pureum, 2019).

Russia spreads large-scale disinformation through SNS to divide opposing countries, and is based on the concept of 'reflexive control' created by Lefebvre.

Each country is conducting research on cyber cognitive warfare from various perspectives, and the results of the research to date show that cyber cognitive warfare is the manipulation of perception and change in behavior by spreading disinformation in cyberspace. And most cyber cognitive warfare studies have concluded that the cause of behavioral change is cognitive manipulation, and there is no research on the mechanism of behavioral change. Just as past mentalistic psychology attributed all causes of human behavior to the mind, and thus research was not conducted further and was not adopted in many fields, cyber cognitive warfare may have limitations in its development if it concludes that the cause of behavior is cognitive manipulation.

2.2 Research Methods

This paper presents a research methodology on the behavioral change mechanism using the behavioral psychology 'Skinner's operant conditioning theory' in the case of the Russian-Ukrainian cyber cognitive warfare.

There are various theories in behaviorist psychology, but most of them only explain the response to conditioned stimuli, making it difficult to apply them to case studies that change behavior. However, Skinner's operant conditioning theory is a theory for intentionally changing and reinforcing behavior, and many experiments have proven that it is effective in changing behavior. And case studies provide a medium to include meaningful features of real events and convey knowledge that cannot be expressed in words. Another reason for using the case study method is to test, verify, and explain theories. This is also the ultimate goal of psychological case studies.

The disadvantage of case studies is that it is difficult to argue with confidence that a single case represents the whole, and it is said that it is impossible to obtain generalizable results such as statistical analysis. Here, Yin explained, "A case study is intended to draw general conclusions about theoretical assumptions in order to extend a theory, rather than making statistical generalizations," and Stake used the term, "Even if a case study is not a scientific generalization, it can be a type of 'naturalistic generalization' that recognizes the similarity of certain elements of a phenomenon or the cause of behavior within that context."

Cyber cognitive warfare case studies are also not intended to obtain quantitative generalizations such as statistical analysis, but rather to explain the similarities in war cases or the recognition of the causes of behavior within that context.

3. Cyber Cognitive Warfare Concept

3.1 Cognition From a Psychological Perspective

Psychology is the study of human behavior and the physiological, psychological, and social processes related to that behavior. In other words, it studies not only the psychological processes of individuals, but also the physiological processes that control bodily functions, interpersonal relationships, and social processes(David G. Myers, 2022). Psychology is as old as human history, and Democritus first raised the question of whether free will or choice exists when he saw that our behavior is influenced by external stimuli about 400 BC. In this way, the study of human behavior has been continued as psychology for a long time. Cognitive vulnerabilities are based on psychology, and psychology provides scientific evidence for cyber cognitive warfare.

Accordingly, we would like to explain the behavioral change mechanism based on psychology. For centuries, we have pointed to the mind as the cause of behavior. Where is this mind? The answer has been that what we call the mind is a psychological thing that exists in the immaterial world and cannot be heard or predicted. Skinner argued that what cannot be observed and measured cannot be studied scientifically. At the same time, although sensations, emotions, and thoughts cannot be observed, conditioned behaviors can be observed and recorded as people react to various situations, so behavioral psychology was defined as the "scientific study of observable behavior."

Looking at cyber cognitive warfare from a psychological perspective, the manipulation of cognition through disinformation and its manifestation as behavior can be explained by a three-stage schema (stimulus-cognition-response) in which physical elements are transmitted to the human mind, go through cognitive processing procedures, and are then expressed as physical activity.

3.2 Cyber Cognitive Warfare Characteristics

First, the 'cause of irrational behavior' is considered to be that behavior is determined by cognitive distortions such as cognitive errors and biases in the process of receiving disinformation and not being able to accurately perceive it (Claverie and Cluzel, 2023).

Second, the 'targeting goal' aims to control the reactions of individuals and the public to disinformation (Bernal et al, 2020.)

Third, the 'approach to the target' is a method of inducing one's own decision through cognitive processing that connects the brain and mind.

Fourth, 'attack means' use digital means in cyberspace, and the influence on individuals and groups is increasing due to the development of Internet, platform (SNS, etc.), and AI technology.

Fifth, in terms of 'diversity of performers', the subject of cognitive warfare is the military, but civilians who are voluntary participants and professional technicians who can be called mercenaries also participate.

Finally, 'battle damage assessment' focuses on how specific stimuli can lead to incorrect decisions and changes in behavior.

4. Case Study Methodology

4.1 Cyber Cognitive Warfare Case Study Model Analysis and Limitations

Cyber cognitive warfare has been frequently discussed in recent inter-state wars, and many experts are conducting research from various perspectives.

Table 1: Cyber cognitive warfare case analysis method model comparison

Author	Title	Contents and Limitations
Rosana Montañez (2020)	Human Cognition Through the Lens of Social Engineering Cyberattacks	A model that limits human cognitive functions to four and induces behavior is presented, but there is insufficient explanation of cognitive processing mechanisms and operational means.
Lucas Hauser (2022)	Synchronized Cyberwarfare and Disinformation Attacks	Disinformation model divided into three stages, lacks explanation of psychological-based cognitive processing and behavioral changes
Sasakawa Peace Foundation (2022)	Prepare for disinformation from foreign countries! - The threat of information manipulation in cyberspace	The cognitive processing procedure based on external information was presented using psychological knowledge, but the research was limited in that the cause of behavioral change was determined by the mind.
Bernard Claverie (2023)	The Cognitive Warfare Concept	Presenting a cyber cognitive warfare model by applying psychological knowledge, but lacking explanations for the causes of behavioral changes
Kang Hyung-goo (2023)	India's Coercive Strategy Against Pakistan as Seen in the Kargil War: Focusing on Expansion Superiority and Cognitive Warfare	Morgan's 3D model of expansion is presented, and the use of case analysis such as cognitive processing and behavioral changes is limited.
Kim Ki-beom (2023)	Processing Model and Classification of Cybercognitive Attacks_Based on Cognitive Psychology	Presentation of a cyber cognitive warfare model targeting system managers, lacking as a national cyber cognitive warfare model and lack of explanation of causes of action.

4.2 Skinner's Operant Conditioning Theory

Behaviorist psychology viewed all behavior as a result of conditioning and sought to identify behavioral changes based on the relationship between stimulus and response in the basic human formula. This can be proven to

others. The core of Skinner's theory is to increase the frequency or intensity of behavior. When a stimulus called a reinforcement is received for a specific behavior, an incentive to do it is generated, and as a result, humans react to reinforce the behavior again. In other words, reinforcement triggers motivation, and that motivation triggers behavior, so reinforcement occurs.

Reinforcement can be divided into positive reinforcement and negative reinforcement, which increase behavior depending on the nature of the stimulus, and positive punishment and negative punishment, which decrease behavior. Positive reinforcement increases behavior by providing a stimulus that is pleasurable in response to the behavior, and negative reinforcement increases behavior by removing a negative stimulus. Positive punishment decreases a response by providing an unpleasant stimulus, and negative punishment decreases a response by removing a liked stimulus.

4.3 Set Variables

Since the decision-making process and behavior of humans involve human desires and the active and positive will that follows, there are clear limitations in proving causality with behavioral psychology. Therefore, variables are set and research is conducted, and since variables that affect cognition and decision-making are slightly different for each applied model, this paper uses Skinner's theory as a methodology to interpret the similarity of phenomenon elements and behavioral change mechanisms in that context, and sets the variables as follows (Lee Hyeon-gyeong, 2019).

In humans, between a stimulus called a reinforcer and a response called an action, there is a human desire to take action and an active and active will accordingly. Therefore, in order to interpret the cause of behavior change using behaviorist psychology, variables are set and research is conducted.

The independent variables are reinforcement and punishment to change behavior, and the dependent variable is set as the change in behavior.

Control variables include various variables that affect behavior, such as sociocultural characteristics, past experiences, political inclinations, and target characteristics that affect an individual's cognition and behavior.

Reinforcers are secondary reinforcers such as will, stability, patriotism, and emotion.

4.4 Research Subject

The research subjects are cyber-cognitive warfare cases in which changes in the behavior of the general public, such as residents and international public opinion, occurred in the cyberspace between Russia and Ukraine based on public information.

A. 2014 Russian annexation of Crimea (referendum results)

B. 2022 Russia-Ukraine War (Russia's international public opinion formation)

B. 2022 Russia-Ukraine War (Ukraine's international public opinion formation)

5. Case Studies of Cyber Warfare Between Nations

5.1 2014 Russian Annexation of Crimea (Referendum Results)

In 2014, Russia overturned Western expectations and annexed Ukraine's Crimea Peninsula without military conflict. This was a new form of warfare never seen before, with almost no casualties and without the use of force. This new way of waging warfare by Russia shows the characteristics of cyber-cognitive warfare.

In an effort to suppress the legitimate voices of pro-Ukrainian residents on the Crimean Peninsula, Russia reported hundreds of posts containing pro-Ukrainian messages on Facebook and Twitter, claiming that the posts contained hate expressions or obscene remarks. After receiving thousands of reports, Facebook deleted the posts and suspended the activities of the posters. In fact, pro-Ukrainian voices have disappeared from social media platforms. This is analyzed as a negative reinforcement that removes pro-Ukrainian information and increases Russian support. And in order to spread a positive image of Russia, from the end of February 2014, when the Crimean crisis was intensifying, they tried to disguise themselves as positive by providing photos of themselves posing with young girls, children and mothers, the elderly, and pets, called Polite People, on social media. These activities can be seen as positive reinforcement.

According to a preliminary opinion poll, 75%(Россия 1, 2015 / heraldcorp, 2014) of Crimean residents are in favor of Russia's annexation. If we apply Skinner's operant conditioning theory to the above case, it is interpreted

that negative reinforcement and positive reinforcement were used as independent variables to strengthen residents' behavior, and the dependent variable resulted in a referendum result of 97% in favor.

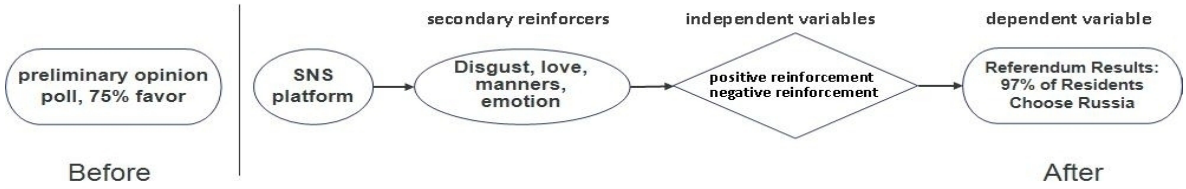

Figure 1: Application of Skinner's Theory: The Case of Russia's Annexation of Crimea

5.2 2022 Russia-Ukraine War (Russia's International Public Opinion Formation)

A March 2022 survey by the Russian Public Opinion Research Center (VTSIOM) at the beginning of the war found that a majority of Russians (60%) supported Russia's special military operation in Ukraine, while a CNN online poll of more than 1,000 people in both countries found that one in two Russians (50%) believed that the use of force to prevent Ukraine's entry into NATO was justified.

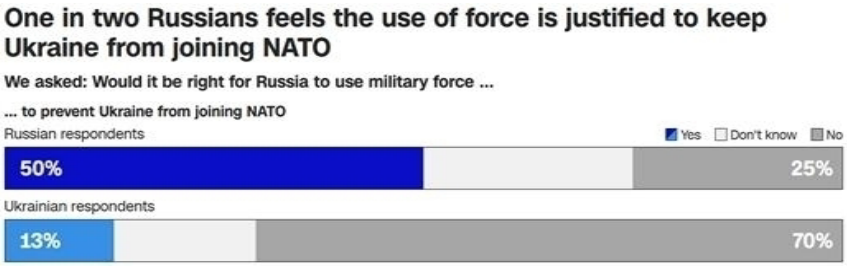

Figure 2: CNN Poll Results: Russia's Use of Force Justified

While waging war, Russia used digital means such as social media to spread disinformation, including news that the United States was supporting Ukraine's biological weapons research, that Western weapons were massacring pro-Russian forces in Ukraine, that Ukraine was indiscriminately shelling hospitals and civilians, that Ukrainian President Zelensky had escaped Kiev, and a video of a surrender declaration using deepfake technology. This behavior is analyzed as a form of static punishment that lowers the will to fight and creates fear. However, after the outbreak of the war, the intervention of third countries such as the European Digital Media Observatory, which specializes in fact checking, revealed that most of the Russian disinformation was factually incorrect, and a survey conducted by the Russian public opinion research group (Levada) of 1,600 people living in Russia asking who was responsible for this war gave different results from the early days of the war.

The results showed that 8% of online new media readers, 10% and 28% of social network and Telegram channel readers answered that Russia was responsible for the war, while 25% of online new media readers, 30% and 28% of social network and Telegram channel readers answered that they did not know or avoided the question.

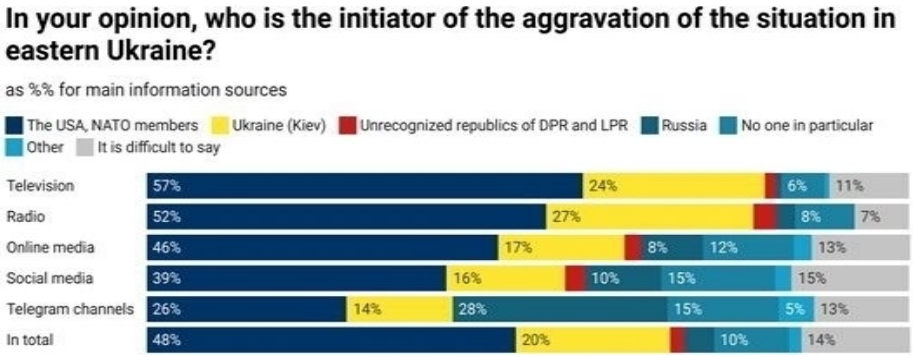

Figure 3: Levada Poll Results: Responsibility for Russia-Ukraine War by Media

Applying Skinner's operant conditioning theory, it can be interpreted that Russia attempted to use positive punishment as an independent variable, but the dependent variable did not come out properly due to an error in the control variable called intervention by a third country.

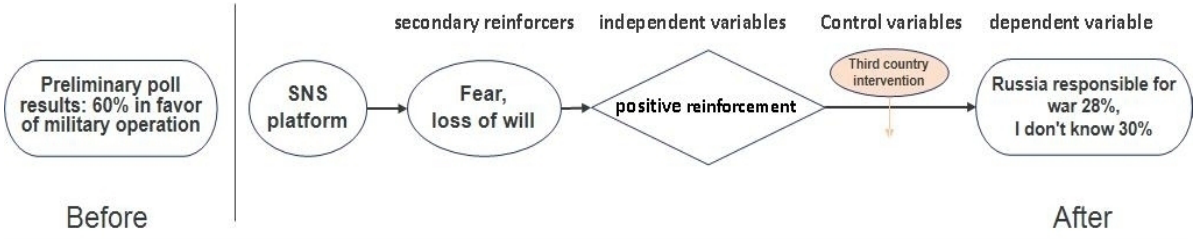

Figure 4: Application of Skinner's Theory: The Case of Russia's Failure to Shape International Public Opinion

5.3 2022 Russia-Ukraine War (Ukraine International Public Opinion Formation)

While Ukraine did not respond adequately to cyber-cognitive attacks at the time of the annexation of Crimea, it actively responded to Russian cyber-cognitive warfare in 2022, emphasizing that Russian aggression was a political maneuver by Putin and attempting to shape international opinion about Russia's imperialist actions.

President Zelensky uses social media such as Twitter and Instagram to inform them of the specific situation of the war every day, and speeches to other countries' parliaments through video conferences. The actions of a country's president to inform governments and the public of the war situation around the world, thereby creating international public opinion (Song Tae-eun, 2022.), appear to be positive reinforcement that provides desirable stimulation.

In addition, providing undesirable stimuli, such as by sharing on Twitter a 45-second video of the Eiffel Tower in Paris being blown up and Paris being attacked, a composite video produced by a Frenchman, warning the international community of the dangers of Russian air raids, can be seen as positive punishment.

According to a survey of American adults conducted by the Pew Research Center from March 21 to 27, 2022, 72% of Americans have a positive opinion of President Zelensky, while 6% have a positive opinion of President Putin, showing that public opinion in the United States was on Ukraine's side at the beginning of the war.

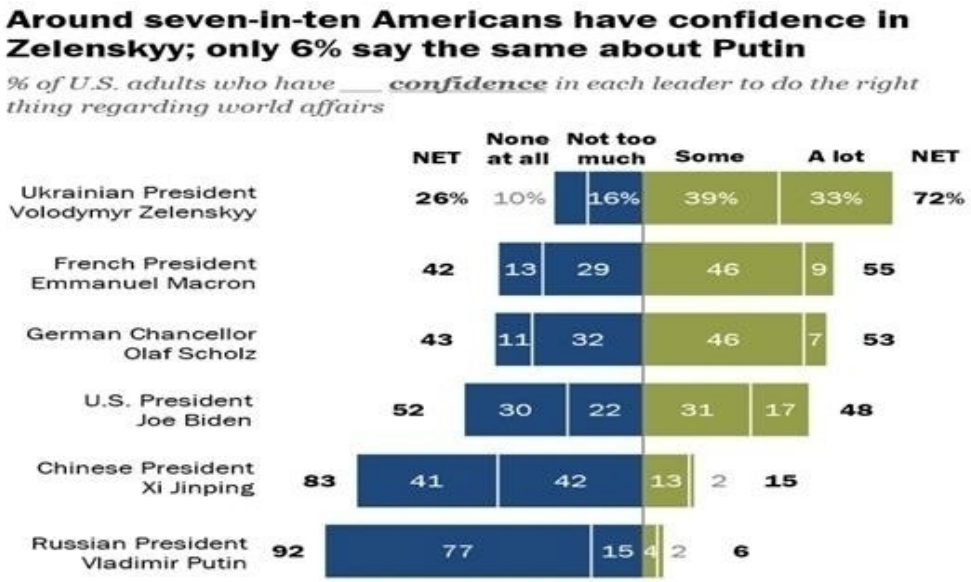

Figure 5: 2022 Pew Research Center Poll Results: Zelensky & Putin Trust Ratings

A year after the outbreak of the war, the Pew Research Center again surveyed American adults from March 20 to 26, 2022, and found that more than half of American adults (56%) trust President Zelenskyy to do the right thing regarding world issues, while only 7% responded that they trust Russia's Putin and 90% responded that they do not trust him.

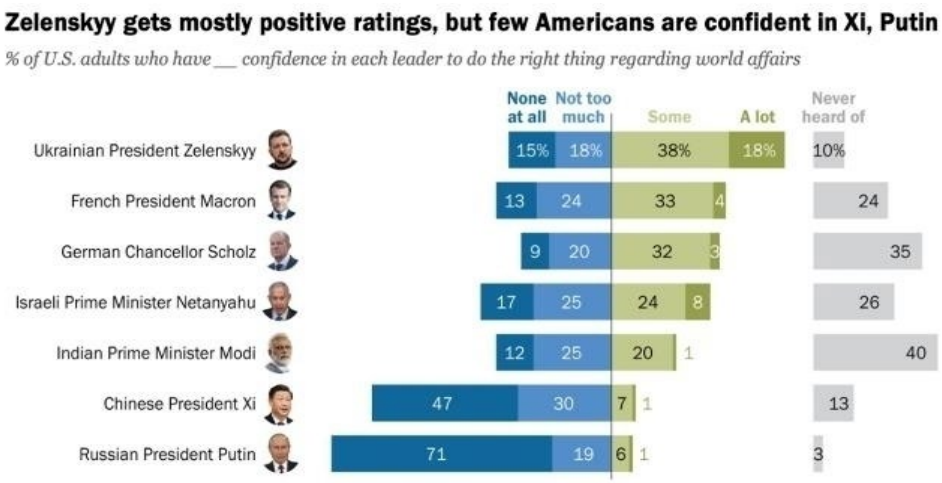

Figure 6: 2023 Pew Research Center Poll Results: Zelensky & Putin Trust Ratings

If Russia's cyber-cognitive warfare performance was poor due to the error of the control variable of the intervention of a third country, Ukraine experienced the same error of the control variable of the intervention of a third country, such as analyzing and fact-checking Russian fake videos on representative social media companies such as Meta and Facebook in the United States, but the opposite result was achieved. Russia lost credibility through fact-checking, but Ukraine responded with the truth, admitting that 'Ghosts of Kiev' was fabricated information (BBC News, 2022.)

Looking at the above case using Skinner's operant conditioning theory, Ukraine attempted positive reinforcement and positive punishment. In Ukraine's case of cyber cognitive warfare to create public opinion in the international community, unlike Russian cyber cognitive warfare, the intervention of a third country had a positive effect, and truthful answers to disinformation increase credibility, showing the two sides of fact checking.

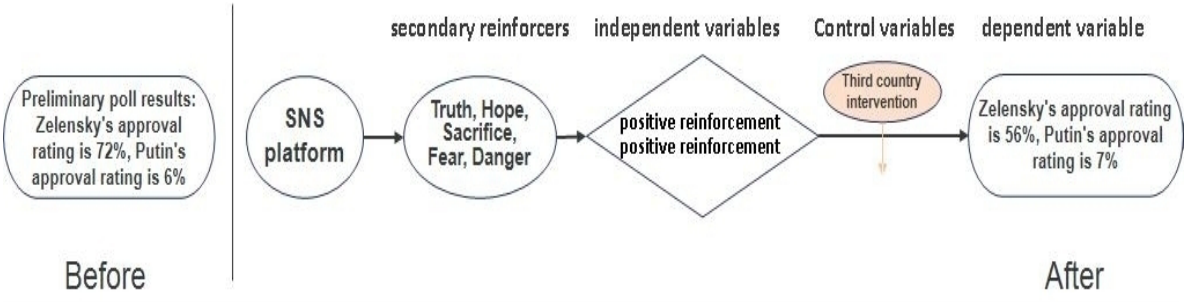

Figure 7: Application of Skinner's Theory: The Case of Ukraine Successful to Shape International Public Opinion

5.4 Research Limitations and Implications

The research sample was not sufficient as the research subject was only analyzing cases where changes in behavior were confirmed due to cyber cognitive warfare, and as humans are beings who actively think and act, there are clear limitations in generalizing to behaviorist psychology. And the secondary reinforcers that strengthen behavior exist in the invisible cognitive domain and are difficult to quantify.

Nevertheless, we were able to find important implications by studying cyber cognitive warfare cases using Skinner's operant conditioning theory.

By conducting a case study using Skinner's theory, it was confirmed that the behavior change mechanism can be interpreted as a 'naturalistic generalization' that recognizes the similarity of phenomenon elements or the cause of behavior within the context as claimed by Stake.

In addition, it was confirmed that 'third country intervention' is an important variable in cyber-cognitive warfare, and 'fact checking' is a way to offset weaponized narratives such as disinformation or, conversely, increase reliability with truthful responses.

6. Conclusion

This study proposes a case study methodology to interpret the behavioral change mechanism using the theory of behavioral psychology (Skinner's operant conditioning theory) regarding the manipulation of cognition and change in behavior due to disinformation, and derives implications.

The results obtained while conducting the research can be summarized as follows.

The Skinner operating conditioning theory is a theory for intentionally changing and reinforcing behavior. When applied to the case of the Russia-Ukraine war, it was confirmed that the methodology of a case study of cybercognitive warfare using behavioral psychology is possible because the results of the dependent variable according to the independent variable can be interpreted. Conversely, this could find important implications that psychological theory can be helpful in establishing cybercognitive warfare plans.

And it was confirmed that the control variable of third country intervention in cyber cognitive warfare acts as a highly influential variable and that fact checking is a two-sided method that can reduce or increase the effect of weaponized narratives. In addition, since cyber-cognitive warfare targets the people, there are limits to responding to it solely through the military, so each country is establishing specialized response organizations, and experts are also gathering opinions on the necessity.

In conclusion, cyber cognitive warfare is inherently invisible, creeping into targets, and by the time the impact is recognized, it is often too late to respond. In cyber cognitive warfare, it is necessary to clearly state that cyber is a means and the essence is cognition, and to conduct research based on psychology with an emphasis on cognitive domain, cognitive processing, and behavioral change research, so that many studies can be conducted beyond the limitations of technology. Therefore, at a time when various studies on behavioral change mechanisms through cognitive manipulation are needed, this study is expected to serve as a foundation for future behavioral change research through cyber cognitive warfare.

Ethics Declaration: Ethical Clearance Was Not Required For the Research

AI Declaration : AI Tools Were Not Used For the Research

References

B.F.Skinner. (2003) “Skinner’s Behavioral Psychology”, Kyoyangin

BBC. (2022) Ukraine Invasion: Russian Military Shells Obstetrics and Gynecology Hospital... Zelensky Criticizes 'Barbaric Attack', https://www.bbc.com/korean/60673420(Accessed 2024.8)

Bernard Claverie, François du Cluzel.(2023) “The Cognitive Warfare Concept”

Choi Shin-jeong. (2012) “Comparison of the Effects of Positive and Negative Reinforcement on Employees’ Customer Service Behavior: Verification of Response Generalization and Backlash”, Master’s thesis, Graduate School of Chung-Ang University

CNN. (2022) Half of Russians say it would be right to use military force to keep Ukraine out of NATO, https://edition.cnn.com/interactive/2022/02/europe/russia-ukraine-crisis-poll-intl/index.html(Accessed 2025.2)

David G. Myers. (2022), "Myers' Introduction to Psychology: The 13th Edition," Sigma Press

Francois du Cluzel. (2020) “Cognitive Warfare, a Battle for the Brain”, Innovation Hub

Herbert Marshall McLuhan. (2023) Understanding Media: An Extension of Humanity, Minumsa

Ha Min-soo. (2016) “Cognitive Bias that Hinder Rational Problem Solving and Exploring Decognitive Bias Methods through Higher Science Education”, Journal of the Korean Educational Science Association Vol. 36 No. 6

Heraldcorp. (2014), "more than 80% of Crimea residents approve of Russian attribution," https://biz.heraldcorp.com/article/66163/(Accessed 2025.3)

Interfax. (2022) More than two-thirds of Russians support Russian special operation in Ukraine – poll, https://interfax.com/newsroom/top-stories/74819/(Accessed 2025.3)

Jeon Hyun-ok. (2009) “The Effect of Token Reinforcement Techniques for Reinforcing Learning Behavior of Underperforming Students in Classrooms”, Master’s thesis, Graduate School of Education, Ajou University

JCS(Joint Chief of Staff). (2016) “Joint Operating Environment 2035 The Joint Force in a Contested and Disordered World”

Johns Hopkins University & Imperial College London. (2021) “Counting cognitive warfare: awareness and resilience, Nato Review

John W. Creswell. (2016) Qualitative Research Methodology – Five Approaches, Hakjisa

Kim Gwi-bun et al. (2005) Qualitative Research Methodology, Hyunmunsa

Kim Jin-ho, Choi Young-chan. (2023) “Development Direction of Korean Military Cognitive Warfare in Preparation for Future Warfare: Cognitive Warfare Concepts, Development Patterns, and Strategic Responses,” Defense Policy Research Vol. 141

Kim Kang-moo. (2020) “The Effects of Cognitive Bias on Decision-making Process and the Application of Structured Analysis Techniques for Decognitive Bias (Focusing on the Perspective of Information Analysis)”, National Intelligence Research Vol. 14 No. 2
Kim Hyun-ah. (2006) “A Study on the Effect of Reception of Government-related Media Reports on Government Trust”, Graduate School of Journalism, Korea University
Klaus Bruhn Jensen et al. (2005) Qualitative Methodology in Media Research, Ilshinsa
Kimberly Underwood. (2017) Cognitive Warfare Will Be Deciding Factor in Battle, https://www.afcea.org/signal-media/cyber/cognitive-warfare-will-be-deciding-factor-battle(Accessed 2025.1)
Kwon Tae-young and Kim Pureum. (2019), "China's Three Wars and Korea's Response Direction", Strategic Research Vol. 26, Vol. 1, Vol. 77.
Lee Yu-na. (2007) “A Study on the Application of Case Study Method in Domestic Public Relations Research”, Hankuk University of Foreign Studies
Lee Chang-min et al. (2020) “Aspects of Future Warfare in the Hyper-connected Era”, The Journal of the Convergence on Culture Technology (JCCT) Vol. 6 No. 3
Lee Jeong-ha. (2022) “Information-Psychological Operations and Reflexive Control in the Russian Federation” Journal of Western History Vol. 66
Lee Jae-hee. (2010) “Comparison of the Relative Effects of Positive and Negative Reinforcement on Safety Behavior”, Master’s thesis, Graduate School of Chung-Ang University
Lee Hyun-kyung et al. (2019) “The Effect of Symbolic Modeling Learning Process According to Operant Conditioning on Changes in Prosocial Behavior in Early Adulthood”, Journal of the Korean Wellness Society Vol. 14 No. 3
Lea Kristina Bjørgul. (2021) “Cognitive warfare and the use of force”, https://www.stratagem.no/cognitive-warfare-and-the-use-of-force(Accessed 2024.2)
Leonid Savin. (2021), “NATO Developed New Methods of Cognitive Warfare”, https://nournews.ir/en/news/81120/NATO-Developed-New-Methods-of-Cognitive-Warfare(Accessed 2024.2)
Lee, Hyeon-Kyeong. (2019), “The Effects of Symbolic Modeling Learning Process Based on Operant Conditioning on Prosocial Behavior Changes in Early Adulthood” Journal of the Korean Wellness Society Vol. 14 No. 3
NATO. (2015) “Analysis of Russia’s Information Campaign against”, NATO Strategic Communications Centre of Excellence
NATO. (2021) “RUSSIA’S STRATEGY IN CYBERSPACE”, NATO Strategic Communications Centre of Excellence
NATO. (2022) “concept Development and Experimentation Contributes to the Alliance Warfare Development Agenda” NATO Strategic Communications Centre of Excellence
NISHIKAWA T. (2023) “The Mind Is a Battlefield: Lessons from Japan's Security Policy on Cognitive Warfare”, Views on Germany's National Security Strategy, Berlin (GE): Global Public Policy Institute (GPPi)
Newstown. (2024) Taiwan Presidential Election, China's '311 Base' Intervening with "Cognitive Warfare", https://www.newstown.co.kr/news/articleView.html?idxno=594311(Accessed 2024.3)
Nathan Beauchamp-Mustafaga. (2019), “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations”, Publication: China Brief Volume: 19 Issue: 16
Otake Fumio. (2020) “Easy-to-Follow Behavioral Economics”, AK Communications
Pewresearch. (2023) Zelenskyy inspires widespread confidence from U.S. public as views of Putin hit new low, https://www.pewresearch.org/short-reads/2022/03/30/zelenskyy-inspires-widespread-confidence-from-u-s-public-as-views-of-putin-hit-new-low/(Accessed 2024.8)
Россия 1. (2015), “Крым. Путь на Родину. Документальный фильм” (Accessed 2025.3)
Rand Waltzman. (2017) “The Weaponization of Information The Need for Cognitive Security”Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity
Sinan Aral. (2022) “Hype Machine: How Has Social Media Changed Humanity?”, Sam & Parkers
Song Tae-eun. (2021) “Goals and Tactics of Cyber Psychological Warfare as a Hybrid Threat in the Digital Age: Focusing on the Responses of the United States and Europe”, Journal of World Regional Studies Vol. 39No. 1
Song Tae-eun. (2023), “Inflow of State-sponsored Disinformation and National Security”, Monthly KIMA Military and Security Vol. 69
Sasakawa Peace Foundation. (2022), “Prepare for disinformation from foreign countries! - The threat of information manipulation in cyberspace”, Cyber Security Research, https://www.spf.org/cyber/publications/20220207_cyber.html(Accessed 2025.3)
TIMOTHY THOMAS. (2004) “Russia's Reflexive Control Theory and the Military”, The Journal of Slavic Military Studies Volume 17, 2004 - Issue 2
YTN. (2022) Russia, Ukraine, etc., Claiming US Secret Biological Weapons Development... Propaganda War, https://www.yna.co.kr/view/AKR20220905078200009(Accessed 2025.2)