Processing Model and Classification of Cybercognitive Attacks: Based on Cognitive Psychology

Ki-Beom Kim[1,2], Eugene Lim[2] and Hun-Yeong Kwon[2]
[1] Ministry of Defense, Seoul, Republic of Korea
[2]Korea University School of Cybersecurity, Seoul, Republic of Korea

nobody85@korea.ac.kr
eugenelim@korea.ac.kr
khy0@korea.ac.kr

Abstract: Cybercognitive attacks, as witnessed in large and small wars and events along with the recent Russia-Ukraine war, are no longer traditional cyber operations, but are increasingly attacking the psychological weaknesses of targeted members of society and target organizations. Therefore, it is timely to systematically analyse and model cybercognitive attacks. Various definitions and case analyses of cybercognitive attacks are currently being actively conducted, but studies on clear classification and processing models of cybercognitive attacks are almost absent. Accordingly, this paper analyzed cases of cybercognitive attacks. The types derived through case analysis were divided into four categories, and cybercognitive attacks were classified and defined. On such basis, a processing model for cybercognitive attacks was designed, and furthermore, cybercognitive attack layers were classified and presented from the attacker and defender's perspective. The corresponding model and layer presented in this paper model both the countermeasures that can be used to perform cyber operations and the psychological mechanisms hidden in each response process. Specifically, a psychology-based cybercognitive attack processing model was designed to achieve goals by inducing behaviour from collecting information for system managers to inducing response/cognitive processing/decision making/compensation. As such, this paper focused on clarifying the definition of cybercognitive attacks and establishing performance procedures, which are only used as actions using deception by presenting cybercognitive attacks scientifically and logically using psychology descriptions. With that, this paper is expected to serve as the ground for cybercognitive kill chain research that can defend against further cyberattacks using cognitive vulnerabilities.

Keywords: Cybercognitive attacks, human vulnerabilities, Psychology, cybercognitive processing model, cybercognitive hierarchical classification

1. Introduction

The 21st century is witnessing a rapidly changing cyber environment such as the era of the 4th Industrial Revolution and the development of IoT. Meanwhile, cyberattacks targeting national critical infrastructure are frequently occurring, such as Russian-Ukraine cyberattacks, US colonial pipeline hacking, and National Nuclear Security Administration hacking. Despite the fact that National Critical Infrastructure is operated separately from the Internet, the reason for hacking accidents can be cited as 'attacks using cognitive vulnerabilities of system managers', not system vulnerabilities. Thus, research on cybercognitive attacks that exploit the cognitive vulnerabilities of system administrators is required along with research on security technologies of National Critical Infrastructure.

Attacking that exploits human cognitive vulnerabilities in cyberspace is called 'cybercognitive attack', which is not new to modern warfare. British strategist B. H. Liddell Hart randomly selected and analysed 280 wars from the ancient Persian War to the First Arab–Israeli War, stating that only six wars were successful without deception, and that almost all wars were successful using deception. Deception in cyberspace began with the discussion of decoy systems such as honeypots to track intruders in the late 1980s, and cognitive attacks are also described in Tom Kellerman's thesis "Cybercrime Recognition"(Tom, 2017).

Table 1: Liddell Hart Strategy Analysis(19th century – World War II)

Random War Selection	Victory Without Deception Strategy	Victory in Deception Strategy
238 times(100%)	6 times(2.1%)	274 times(97.9%)

Cognitive attack originated from conventional warfare in the past and is applied to modern cyberattack. In particular, cybercognitive attacks can exploit cognitive vulnerabilities of National Critical Infrastructure administrators to access internal networks that are physically impervious.

Accordingly, this paper presents a cybercognitive attack processing model using cognitive psychology for cybercognitive attacks, and classifies the layers of cybercognitive attacks from the standpoint of attackers and defenders.

2. Theoretical Background

2.1 Implications of Cognitive Psychology

Psychology is the study of human and animal behavior and the physiological, psychological, and social processes involved in it. In other words, not only individual psychological processes but also physiological processes that control physical functions, inter-individual relationships and social processes are the subjects of study. Psychology is as old as human history, and Democritus was the first to raise the discussion about whether free will or choice exists, given that our actions are affected by external stimuli more than 400 years ago. As such, research on individual behavior has been conducted through psychology for a long time.

Psychology is closely related to war. During World War I and II, it was implemented in conjunction with deception as a field of battle, and during the Persian Gulf War (1990), it was used as a means of persuasion and public opinion on the international stage, and during the Kosovo War (1998), psychological activities were carried out as a means of cyber. Today, hacking mail, whaling, and honeypot cyberattacks are carried out using the psychology of the target. Psychological warfare is the only weapon that can manipulate the thoughts and actions of the enemy without firing a single bullet. As the continuous nuclear threat grows, cognitive attacks that can manipulate the perception and behavior of targets by means of cyber are the best weapons.

2.2 Proof of Human Vulnerability

Humans are known as rational beings, but based on prospect theory and behavioural economics, humans can be proved as unstable and unreasonable beings.

Prospect theory is an experimental psychology theory that assumes that people are more sensitive to loss than to profit, and that both profit and loss are less likely to feel when they continue to occur, and behavioural economics is the theory of how to behave and what happens by studying actual human behaviour, not rational and ideal economics.

In the light of prospective theory value graphs and behavioural economics, when profits and losses are equal, humans feel more painful when losses occur than when profits occur, and when losses continue to occur, adapting to pain indicates that humans are unreasonable.

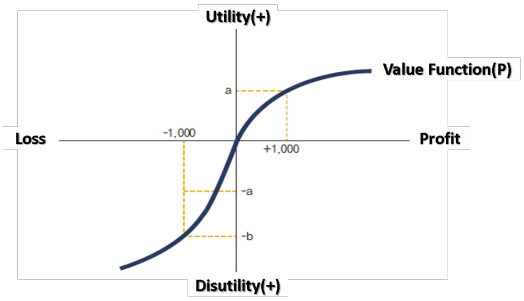

Figure 1: Prospect Theory Value Graph

Prospect theory states that people place more weight on loss than on gain, which means that they place more weight on loss avoidance than on profit-seeking. In other words, it can be inferred that people are much more likely to act not to lose something rather than to act to get something.

If a crisis escalates to avoid losses among countries, the possibility of a preemptive strike may increase. If the current situation is expected to worsen and the loss is expected to expand, policymakers can choose to take preemptive strikes to prevent the expansion of losses(Stein, 1992), and the consequences of avoiding war will further worsen their current status and position(Jervis, 1992).

Looking at the 2003 U.S. attack on Iraq based on prospect theory and behavioral economics, the U.S. reference point is national security and public safety. This is confirmed by U.S. President George W. Bush(2002) claim that war in Iraq is the surest path to peace and security, and Powell's (2002) announcement that collusion between terrorists and WMDs will be the top U.S. concern for years to come. The Bush administration's National Security

Strategy Report, released in September 2002, shows the U.S. government trying to avoid losses through the words ‘protection’ and ‘maintenance’ in its three major goals.

Recognizing the possibility that Iraq could use biochemical and WMD(Weapons of Mass Destruction) against the United States, U.S. President Bush said that Iraq should have a basis for its possible use of WMDs and that if it fails to cope with the threat, something unacceptable will happen (Bush, 2002~2003).

Overall, some view it as an incentive to gain oil-related gains in the Arab region due to the 2003 U.S. attack on Iraq, but the prospect theory explains that it is to avoid loss of U.S. security instability and potential mass destruction of the U.S. people based on national security and public safety.

As such, humans have irrational and cognitive vulnerabilities, and these vulnerabilities are used for cyberattacks.

3. Cybercognitive Attack

3.1 Definition of Cybercognitive Attack

Rosana(2020) classified human cognition into four main categories: Perception, Working Memory, Decision Making, and Action.

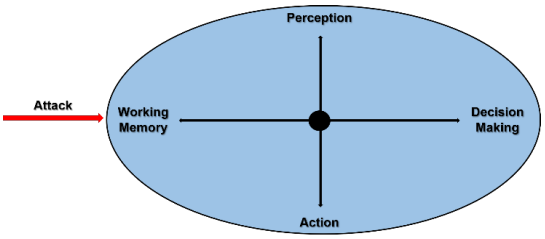

Figure 2: Classification of cybercognitive attack

Perception refers to the conversion of information from words sampled from the senses into neural codes that can be used for intelligent behavior and conscious experience. In the case of Working Memory, it consists of attention and short-term memory, often adjusting processing information by prioritizing specific information over a short period of time to achieve a goal. Decision Making is a gateway to action, prioritizing working memory and information from other unconscious sources. Action means implementing calculations from decision making and other influences. Based on this, attacks on each cognitive element(Perception, Working Memory, Decision Making, and Action) of humans were classified as types of cybercognitive attacks. In this paper, cybercognitive attacks are based on the Working Memory type and are defined as cyberattacks that fuse cognitive psychology to manipulate the perception of targets at the will of the attacker.

Cognitive warfare has been used in the United States since 2017(Underwood, 2017) to describe the ways in which influential groups can act to 'manipulate, infiltrate, influence, or even destroy the cognitive mechanisms of enemies or citizens'. General Goldfein, including James Giordano, a neuroethicist who described the battlefields of the 21st century in the brain and studied the weaponization of neuroscience, described the cognitive war as a war of attrition, while Lieutenant General Stewart of the Defense Intelligence Agency saw it as a cognitive war. The book on Cognitive Superiority, written by Dean S. Hartley et al(2001), developed a theoretical foundation for the sixth area of war that connects technium to noosphere, considered a global expression of human intelligence mediated through technology.

Cognitive attack is a process of changing and deceiving an individual's thoughts and can also be expressed as deception. Deception is defined in Stanford Encyclopedia of Philosophy as intentionally allowing the other party to gain or continue to have false beliefs so that they do not obtain true beliefs. Military flags are defined in the U.S. Military Interpreter JP 3-13.4 MILDEC as "specific actions that allow opponents to deliberately mislead military capabilities, intentions, and operations and contribute to our military operations." Sang et al(2022) defines using defender-dominant information asymmetry as a type of non-cooperative decision-contamination technique that manipulates and deceives potential attackers' cognitive perspectives on defensive deception to continuously construct and maintain false post-action strategies. Defensive cyber deception is viewed as a new concept with unique characteristics that distinguish it from other security factors such as induction, isolation, backtracking, and mutation, while separately having a dedicated Kill Chain process for each application environment and scenario.

3.2 Cybercognitive Attacks Real-world Case

In December 1994, Russia invaded Chechnya to prevent the independence of the Chechen Republic, and the Chechen army fought persistently, conducting cyber propaganda activities such as "about 2,000 soldiers escaped safely despite the siege of the Russian army." Accordingly, Russia blocked cyber propaganda activities by paralyzing the Internet through DDoS attacks. In February 2014, during the Crimean Peninsula War, on the day of the referendum on the annexation of Crimean Peninsula, a website related to the referendum in Crimean Republic was attacked by DDoS, causing it to go dead for about an hour. While Russian cyberattacks were threatening and persistent, Ukraine's response was not clearly visible, so speculation was rampant that it would lose the war with Russia, and that biased broadcasting lowered the rational judgment of the Ukrainian people. In February 22, the Russian-Ukraine war paralyzed government agencies and portal websites, including Ukraine's Defense Ministry, aimed at reducing war fraud, creating fear, neutralizing leadership and resistance, and blocking external information inflows. It can be seen that Russia preoccupied the leadership of the battlefield through cybercognitive attacks and doubled the effect through hybrid operations linked to military operations.

3.3 Literature Review on Cybercognitive Attacks

NATO argued that cybercognitive attacks weaponize public opinion from the outside, causing the target to destroy itself from the inside (Bernal, 2020). Cognitive attacks create destabilization on the public and pursue two complementary goals: government policy and influence on the public. NATO presented six examples of cognitive attacks as follows: confusion-induced destabilization, fragmentation-enhancing destabilization, destabilization as a means of influence, influence recruitment, influence policymaking, and influence as a means of destabilization.

Lucas Hauser(2022) presented a disinformation threat model in which attackers create false information on social media platforms and distribute it to online communities, causing social damage and division. (Step 1: Long-term preparation) False information forms political public opinion, causing division and distrust for future attackers to exploit. In order to spread inflammatory stories, foreign false information providers ask reputable news through followers on social media and try to gain trust in partisan online communities. This behavior(preparation) is the process of gathering information to form the country's domestic political discourse and develop customized disinformation campaigns during the period through cyberattacks. (Step 2: Cyberattack) After deepening the domestic division of the target country, cyberattacks begin at the right time, such as before elections or political scandals. Cyberattacks create a chaotic environment in which customized disinformation can be exploited by damaging computer networks, physical infrastructure, and devices. (Step 3: Tailored Disinformation) Cyberattacks are carried out to escalate the confusion of customized false information. During and immediately after cyberattacks, disinformation channels encourage inflammatory disinformation, maximizing social confusion and polarization and allowing the truth to be buried.

Figure 3: A coordinated Cyber-Disinformation Attack

Johns Hopkins University & Imperial College London classified cognitive operations into single and long-term campaigns. A single campaign focuses on the limited goals of preventing military operations from proceeding as planned or forcing changes in certain public policies, and a long-term campaign confuses entire societies or alliances by pervasive doubts about governance, subverting democratic procedures, and inciting civil unrest or separatist movements. Today, cyber, information psychology, and social engineering are integrated and used to carry out cognitive warfare, and the concept of 'combined weapons' was suggested. It is believed that 'combined weapons' induce behavior that can cause society and groups to become radicalized and divide a cohesive society by sowing seeds of doubt and introducing conflicting negatives.

B.Claverie(2022) evaluate that cognitive warfare is operating around the world as a new war zone following the land, sea, air, space, and cyber areas. This paper describes the concept of cognitive combat, where(aggressive cognitive combat) is a bullying-focused approach and ‘defensive cognitive combat’ involves developing resilience and preventive abilities using similar tools. It also divides cognitive warfare into global perspectives and perspectives based on available tools. ‘Global perspective’ is intended to contribute to a culture of mind coordination or building resilience and global security on the other side of the spectrum and to inform and

educate malicious behavior or intentions, (based on available tools), and considerable interaction with multiple cultures, including decision errors and biases, perceptions and fantasies, cybernetics and control.

3.4 Existing Models and Limitations

Veksler et al (2020) is a model that can generate predictions about the behavior of attackers and defenders, and it is concluded that the threat of cognitive attacks can be reduced by 25% based on small samples of expert decisions using symbolic deep learning (SDL) on the defender's side. He also concluded that the attacker side could use model tracking via dynamic parameter fitting to automatically construct the model during real-time attack scenarios and predict individual attacker preferences by 40-70%. However, the availability of cyber expert decision data is quite rare, often consisting of dozens or hundreds of examples, and DL requires learning data with thousands or millions of examples, so it can be seen that there are limitations. Tzu-Chieh Hung & Tzu-Wei Hung (2020) argued that cognitive attacks and cyberattacks are similar in terms of spreading false information, but cyberattacks differ from cognitive attacks because they attack enemy infrastructure or steal information in practical ways such as distributed denial of service (DDOS) attacks. They also include influencing factors on the human cognitive domain in many types of wars, but there is a limitation in that they concluded that only cognitive warfare weaponizes neuroscience and is committed to brain control. Dit Avocat (2021) provides insightful analysis of how cognitive attacks are implemented on the attacker's side, but there is a limitation that it does not provide details on how human cognition interacts with false information (defenders).

4. Cybercognitive Attack Processing Model

The social engineering cyber operation analysis model presented by Shin et al (2018) modeled the social engineering information collection stage, the social engineering strategy selection stage, and the social engineering strategy execution stage. In the social engineering information collection stage, physical contact with the organization and individual elements to be collected is collected, and in the social engineering strategy selection stage, physical, social, technical, and mixed strategies that can be used socially can be selected. In the social engineering strategy execution stage, it is composed of response of interest, cognitive judgment, and target behavioral stage and psychological agents that operate at each stage.

The social engineering cyber operation analysis model is a model limited to social engineering, and the cybercognitive attack processing model to be presented in this paper is a model designed by collecting and analyzing the following open information that occurred between 07 and 17 years: 20 hacking related to North Korea (Seoul Air Show (ADEX) Defense Contractor Hacking Mail (2015), Blue House Impersonating Hacking Mail (2016), Interpark Personal Information Hacking (2016), etc.), 10 Korean Cases (Hack Mail for Job Applications Targeting Human Resources Officers (2017), Ransomware Impersonating the Payment of Traffic Fines(2017), etc.), 10 overseas cases(The Dalai Lama's Computer Hacking (2009), London Olympics Official Site Impersonation Scam (2012), WhatsApp Fraud (2016), etc.).

Once the information on the attack target has been collected, a response is induced with the following four factors: Expertise which corresponds to the target's specialized field and is recognized as high-quality information, Salience that gives a noticeable stimulus such as color, size, sharpness and movement of information, Curiosity to be interested in celebrities, financial gain and sex-related contents, and Urgency such as information with an ‘urgent’ prefix or with limited access and processing deadlines. It is also expressed as a social engineering technique. If it succeeds here, it will move to the victim's territory, and if it fails, it will be re-performed from collecting information.

Cybercognitive attacks provide false information to the target's cognition, and in this process, cognitive processing and schema are formed to compare and analyze knowledge and behavioral types of the external world stored in the individual's head. Cognition maintains a state of equilibrium, and there is a assimilation process in which false information is accepted and generalized in line with existing schematics, or a control process in which existing schematics are changed or newly made occurs when they do not fit the existing schematics. Finally, there is an instinctive process of organization and equilibrium that reorganizes existing schematics into new and complex structures. After schematic processing, decision-making is made using psychological descriptions related to decision-making such as speculation, partial thinking, group thinking, internal group bias, and prospect theory. If the victim is rewarded with the information or results he or she wants for subsequent actions, he or she will behave as the attacker manipulated without reasonable doubt.

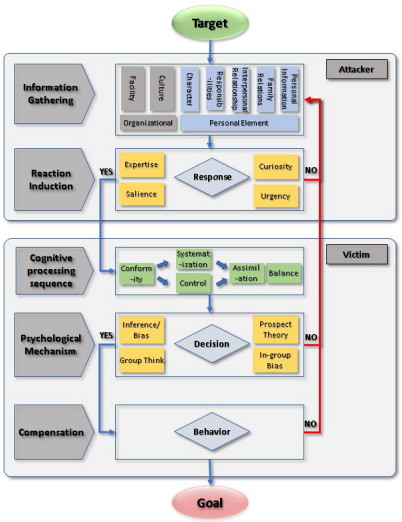

Figure 4: Cybercognitive Attack Processing Model

5. Cybercognitive Attack Hierarchical Classification

Until now, studies related to cybercognitive attack have been focused on cognitive aggressive means, procedures, and cases, and classification according to the type of technology that occurs in the process of human cognitive attack has been sluggish. Accordingly, based on the cybercognitive attack processing model, hierarchical classification was performed on cybercognitive attacks that can be performed from the attacker's point of view and the defender's point of view.

5.1 Cybercognitive Attack from an Aggressive Perspective

Attacks can neutralize the cyber defense system by exploiting the cognitive vulnerabilities of the system personnel responsible for the internal network. An attacker can intentionally provide false information to the victim to induce victim behavior and provide a contact point for the network to penetrate the disconnected closed network.

5.1.1 Spear Phishing

Spear phishing is a highly targeted attack that sends hacking emails with sophisticated design based on the names of people involved, words in company documents, information that makes you believe in normal mail, and common items at work. FireEye analysed that 91% of cyberattacks started from hacking mail, 99.7% of attachments used in hacking mail use social engineering techniques, and 65% of spear phishing attacks were successful. Symantec's 2019 Internet Security Threat Report(ISTR) shows that the number one word in the email attack's title is "urgent". As such, spear phishing attacks are attacks that combine psychological mechanisms based on the information of the target.

5.1.2 Fake News

Fake news causes individuals to believe inaccurate information and influence their opinions and actions. In the past, various groups of people, such as advertisers, political activists, and religious fanatics, used various forms of fake news to influence public opinion or spread propaganda. And modifying fake news doesn't necessarily change people's beliefs. Even if you believe in the revised truth, fake news continues, and the act of refuting it can have negative consequences. The more people hear fake news, the more familiar it becomes, and the more likely it is to believe it real. This effect is due to familiarity and fluency bias.

5.1.3 Reverse Social Engineering

Social engineering is a psychological technique that tricks a person into moving in the direction they want, i.e., by deceiving them to leak sensitive information or bypass the security perimeters associated with information, Reverse Social Engineering(RSE) is a technique that induces an attacker to perform a malicious attack, such as a direct attack. In the past, espionage agents established friendship by solving the problem that the target was in, formed a rapport, recruited, and ordered espionage.

5.2 Defensive Cyber Deception Operation

Rather than waiting for an enemy in defense, you can actively bait them to reduce risk by exploring and attracting them. Defenders provide the attacker with false information that they accept as true, disrupting the attacker's asymmetric advantage and making them believe incorrectly It also has the advantage of being able to get a

counterattack opportunity and reduce the possibility of attack and cyber defense costs by identifying the attacker's strategy, tactics, capabilities, and intentions.

5.2.1 Honey Pot

Talinn Manual 2.0 defines Honeypot as a trick to protect computer systems from malicious manipulation using a physical or virtual environment designed to attract intruders' attention with the aim of deceiving them. Honeypot creates an independent, vulnerable environment that induces malicious users to connect, making it seem like it can be used to steal information from that system or attack other systems. Most of the actions inside the Honeypot are limited, and the commands you enter remain in the log, and the downloaded files are stored separately on the host system. It then records and analyzes all actions of malicious users to respond to subsequent attacks. Security policy design and content are important for honeypot operations. A security policy that is too low can cause an attacker to suspect or avoid access. And the content of the framework needs to be updated continuously.

5.2.2 Cyberattack Traceback

Traceback is a technology that can track the source of attacks. Traceback technology includes Host-based TCP Connection Traceback, which uses backtracking modules installed on systems to locate attackers via multiple different systems, and IP Packet-based Traceback, which installs backtracking modules where network packets can be monitored. Analysis of collected data using Traceback technology can identify attack environment information such as attacker's IP, country, operating system, monitor size, and find attack patterns such as activity time, collected information, and attack tools. From the defender's point of view, you can analyze the attacker's attack environment and pattern to get a chance to counterattack.

5.2.3 Cyber Persona

People represent themselves as cyber personas in cyberspace. Cyber personas form a layer with the physical and logical layers of cyberspace. Cyber personas allow attackers to gather information or identify system weaknesses, but can also be used in reverse.

In the cyber space where the attacker is active, cyber persona can be used to find out the attacker's ability, personality, and interests. IT personnel from North Korea's Kim Il-sung University also team up with athletes from other countries at the CodeCodeforce. If you have formed a close relationship through team activities, you can leak false information such as honey doc to induce attacks or lower rational judgment. Recently, Metaverse, a three-dimensional virtual person working in cyberspace, has not yet been clearly established, but it is being used as a world where real life, legally recognized activities, jobs, and financial learning are connected in three dimensions. Metaverse is an opportunity and a challenge for the IT industry, and there is a risk of hacking such as biometric information hacking, brain hacking, random thought injection, and behavioral pattern manipulation.

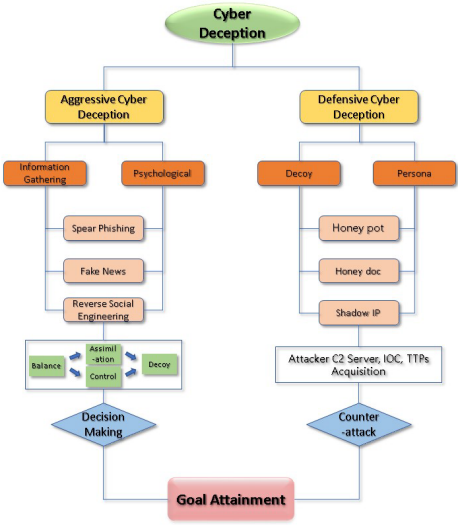

Figure 5: Cybercognitive Attack Layer Classification

6. Conclusion

The cause of malicious code infection targeting the national important system has been determined by receiving hacking mail and social engineering techniques, and technical analysis such as TTPs, source codes, and attack patterns of malicious codes has been conducted. As a result, malware response technology and security systems have become more advanced and robust. Nevertheless, hacking accidents occur because the attacker is using the cognitive vulnerability of the system manager, not the attack using the system vulnerability.

Identifying and attacking systemic vulnerabilities requires a lot of time, budget, and risk, such as zero-day vulnerability development or purchase, supply chain attacks, and physical penetration. However, system managers' cognitive vulnerabilities can benefit from reduced budget and effort, and system incapacitation that cannot be physically infiltrated. In order to attack important national systems, attacks using system manager cognitive vulnerabilities are effective, and cybercognitive attacks are performed because the probability of attack success can be increased.

Improving the security level of the national critical system requires research on technical responses and cognitive attacks using system managers. Previously, system managers judged and processed the path of malicious code infection with simple social engineering techniques, or classified according to the type of technology that occurs in the process of human cognitive attack through cybercognitive attack methods, procedures, and cases. This paper presents a cybercognitive attack processing model based on psychological response induction, psychological writing, and defender cognitive processing based on psychological psychology that scientifically studies decision-making after dividing into attacker and defender areas. In addition, it is meaningful in that it promoted hierarchical classification of cybercognitive attacks and defense activities in cyberspace, and the definition of cybercognitive attacks was clear and the performance procedure was established.

If additional research is further conducted on the attacker's cognitive processing process and purpose of attack in the cybercognitive attack model, it will be possible to devise strategies such as cyberkill chains that can identify and prevent/reject cybercognitive attack mechanisms.

References

Al Amin, M., Shetty,(2019). Attacker Capability based Dynamic Deception Model for Large-Scale Networks.*ICST Transactions on Security and Safety*,*6*(21). https://doi.org/10.4108/eai.13-7-2018.162808

Allcott, H., Gentzkow, M.(2017). Social media and fake news in the 2016 election. In *Journal of Economic Perspectives*(Vol. 31, Issue 2). https://doi.org/10.1257/jep.31.2.211

Bernard Claverie, Baptiste Prébot, Norbou Buchler, François du Cluzel(2022), What Is Cognition? And How to Make it One of the Ways of the War?, NATO Collaboration Support Office, pp.4, 1-17, 978-92-837-2392-9.

Bernal, A., Carter, C., Singh, I., Cao, K., Madreperla, O. (2020). “Cognitive Warfare: An Attack on Truth and Thought”, NATO and Johns Hopkins University: Baltimore MD, USA.

Chang, Keung Ryong.(2004). Why did the U.S attack Iraq?: An Explanation based on Prospect Theory pp. 89-112. The Journal of Political Science & Communicaiton

Flynn, D. J., Nyhan, B., Reifler, J.(2017). The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics. *Political Psychology*, *38*. https://doi.org/10.1111/pops.12394

GRAPHUS .(2020). Retrieved from https://www.graphus.ai/resources/spear-phishing-social-engineering/

Greenhill, K. M., & Oppenheim, B.(2017). Rumor has it: The adoption of unverified information in conflict zones. *International Studies Quarterly*, *61*(3). https://doi.org/10.1093/isq/sqx015

Hasher, L., Goldstein, D., Toppino, T.(1977). Frequency and the conference of referential validity. *Journal of Verbal Learning and Verbal Behavior*, *16*(1). https://doi.org/10.1016/S0022-5371(77)80012-1

Hung, T. C., & Hung, T. W.(2022). How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars. *Journal of Global Security Studies*, *7*(4), 1–18. https://doi.org/10.1093/JOGSS/OGAC016

Jervis, R. (1992). Political implications of loss aversion. Political Psychology, 13(2), 187–204. https://doi.org/10.2307/3791678

Kim, J.T., Han, M.H., Lee, J.H., Kim, J.H., & Kim, I.K.(2014). *Technical Trends of the Cyberattack Traceback*(pp. 93-103). Electronics and Telecommunications Trends Volume 29 Issue 1: Electronics and Telecommunications Research Institute.

Kulíšek,J.(2012). Military Deception. *Vojenské Rozhledy*, *21*(2). https://doi.org/10.3849/2336-2995.21.2012.02.040-058

Lee, Jonghyun.(2018). Critical Analysis on the Application of Due Diligence Principle in the Cyber Context. *Korea International Law Review*, *49*, pp. 143-170.

Liddlell Hart, B. H.(1967). Strategy second revised edition. In *International Affairs*.

Mary-Ann Russon.(2021). *US fuel pipeline hackers 'didn't mean to create problems'*. BBC News.

Murray, A.(2016). *How to report fake news to social media* , BBC News.

Myers, D. G., & Dewall, C. N.(2015). Psychology in Modules - by Myers and DeWall. In *Worth Publishers*.

Natasha B, Eric W.(2020). *Nuclear weapons agency breached amid massive cyber onslaught*. Politico.

Norman, D.A.(1986), Cognitive Engineering, In D.A. Norman & S.W. Draper, Eds. User Centered Systems Design, pp. 15-34, Hillsdale, NJ: Lawrence Erlbaum Associates

Oh, H.(2015). Unsupervised Scheme for Reverse Social Engineering Detection in Online Social Networks. *KIPS Transactions on Software and Data Engineering*, *4*(3). https://doi.org/10.3745/ktsde.2015.4.3.129

Piaget, J.(1932). The moral judgment of the child. London: Routledge & Kegan Paul.

Sang Seo, Dohoon Kim, Sangwoo Han(2022). Simulation and Analysis of Drone Combat Damage Effect Against Cyber-Electronic Threats. *JKIIT*, 20(11), 163-185.

Schmitt, M. N.(2013). Short form citations. In *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, para. 28, Cambridge: Cambridge University Press.

Stein, J. G., & Pauly, L. W. (1991). Choosing to Co-Operate: How States Avoid Loss. International Journal, 47(2), 199–201.

Shin, D. C., & Park, Y. H.(2017). Development of Risk Assessment Indices for Social Engineering Attacks. *Journal of Security Engineering*, *14*(2). https://doi.org/10.14257/jse.2017.04.01

Shin,K., Kang,J., Yoo,J., Kim, J., Kang, S., Lim, H., & Kim, Y.(2018). A Study on the Concept of Social Engineering Based Cyber Operations. *Journal of The Korea Institute of Information Security and Cryptology*, *28*(3).

Stoll, C., & Connolly, J.W.D.(1990). The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. *Physics Today*, *43*(8). https://doi.org/10.1063/1.2810663

Wells, L.(2017). Cognitive-Emotional Conflict: Adversary Will and Social Resilience. *Prism*, *7*(2).

Yoon Soo, Choi.(2015). *Results of interim investigation into KHNP's cyber terrorism case*, Republic of Korea: Prosecution Service.