

WEAPONIZATION OF CONSCIENCE IN CYBERCRIME AND ONLINE FRAUD: A NOVEL SYSTEMS THEORY

Michelle ESPINOZA

M0e73021@marymount.edu

MARYMOUNT UNIVERSITY, ARLINGTON, USA

ABSTRACT:

This article introduces the concept of weaponization of conscience as a complex system and tactic employed by fraudsters to camouflage their activity, coerce others, or to deceive their victims. This study adopts a conceptual approach, drawing from the theoretical underpinnings of military propaganda and psychological operations doctrines and adapting them to serve as a lens through which to understand and defend against weaponization of conscience.

KEYWORDS:

Cybercrime detection, cyberpsychology, cybersecurity, fraud detection

1. Introduction

When a problem is growing exponentially, such as cybercrime, it is because a positive feedback loop is dominating the system at that point in time. Exponential growth is limited by the carrying capacity of the system, and to regulate, slow, or reverse cybercrime's growth, one must identify the positive feedback loop and then counter it with a negative feedback loop or break the positive feedback loop entirely. The problem's growth may be within a department, an organization, and/or society. Systems are akin to matryoshka (nesting) dolls, each subsystem embeds within and interacts with a larger system. This is why cybercrime and online fraud require examination through the lens of complexity science (Espinoza, 2024). Constructing a solution within an organization or at a societal level requires understanding how it works, why it works, and/or why it does not work.

This research introduces the concept of *weaponization of conscience* as a complex system and tactic employed by fraudsters to camouflage their activity, coerce others, or to deceive their victims. Weaponization of conscience can be used alone or in combination with other tactics such as weaponization of bias and weaponization of silence to synergize results and extend the effectiveness of their *modi operandi*. Additionally, weaponization of conscience can be employed against coerced victims to strengthen their attack against the target. Weaponization of conscience is a complex subsystem within the larger complex system of social engineering. This article contributes to the ongoing discourse on theoretical innovation and the advancement of knowledge in cybercrime and online fraud detection from a system dynamics perspective.

Hardin's seminal article on the Tragedy of the Commons posits that to

appeal to an individual's conscience is to intentionally opt for the extinction of all conscience in the long run (Hardin, 1968). Hardin refers to the conscience as pathogenic and likens the conjuring of conscience to using a biological weapon. Hardin's arguments are rooted in Darwin's (1859) theory on survival of the fittest, which posits that organisms best adjusted to their environment are the most successful in surviving and reproducing. Put simply, to act with empathy, compassion, altruism is to sentence oneself to death in a world of barbarians. But without empathy and compassion for one another, what more are we but barbarians? Defending against the weaponization of conscience requires striking the balance between self-awareness and compassion or pro-social behaviors.

The human mind is considered a new domain of operations across Western, Chinese, and Romanian information operation doctrines (Neculcea & Răpan, 2022). Deceptive practices are reaching new levels of realism and complexity due to technological advances (Masakowski & Blatny, 2023; Onushi, 2023). There exists a vast body of research on decision-making processes within highly specific contexts. In contrast, the realm of decision-making in information warfare is a disputable and neglected area of investigation (Maksymenko & Derkach, 2023). The deceptive practices used by fraudsters and scammers bear a striking resemblance to the dynamics at play in the landscape of information warfare where misinformation, deceit, manipulation, and other psychological tactics are employed to achieve strategic objectives.

2. Problem statement

Fraud and other crime are not new, however digitization and the internet transformed the threat landscape so that crimes once requiring proximity of the offender to their victim, can now be carried out across the world with the click of a button (Cross, 2020). Transnational collusion, jurisdictional issues, and the

exponential growth of cybercrime present significant implications for law enforcement as it relates to their ability to investigate, arrest, and prosecute offenders (Cross, 2020; Kshetri, 2017; Salih & Dabagh, 2023). Consequently, many municipalities have insufficient funding and resources to protect their citizenry from victimization by fraudsters (Darii & Meleca, 2022). Understanding how and why fraudsters' *modi operandi* succeed is essential to constructing an effective defense (Rutherford, 2017). 95% of cyber incidents are human-enabled (Nobles, 2018). Modeling decisions and decision interactions as complex systems enables practitioners to incorporate situational or domain-specific details with decision theories to pinpoint vulnerabilities in historical and prospective cyber defense strategies. This article:

1. Defines the weaponization of conscience as a complex system.
2. Explores how the principles of system dynamics are applicable to the weaponization of conscience.
3. Provides examples of how weaponization of conscience manifests, why it may be successful, and presents strategic recommendations for fortifying defenses against such tactics.

3. Method

This study adopts a conceptual approach, drawing from the theoretical underpinnings of military propaganda and psychological operations doctrines and adapting them to serve as a lens through which to understand and conceptualize how cognitive strategies, specifically the weaponization of conscience, is employed by fraudsters in camouflaging their activities and deceiving victims. Writing theory is challenging, partly due to the lack of straightforward formulas or templates (Cornelissen, 2017; Ragins, 2012). Theory adaptation revises extant knowledge by proposing a novel perspective on an extant conceptualization whereas typology aims to

develop a categorization that explains the fuzzy nature of many subjects by logically and causally combining different constructs into a more nuanced understanding of a phenomenon or concept (Cornelissen, 2017; Jaakkola, 2020). This paper uses a hybrid of theory adaptation and typology. Building on the legal definitions and frameworks of conscience laws in the United States and using Greene's (2009) dual-process theory, this researcher provides a base system model template which practitioners can use to visualize decision processes and interactions. By incorporating the critical features of psychological operations, the principles of system dynamics, and using extant cognition and behavior theories from multiple disciplines, this article then provides practical examples of how weaponization of conscience might manifest and presents strategic recommendations to defend against it.

4. Conscience laws

The history of conscience laws in the United States reflects a complex interplay between legal, ethical, and religious considerations. Conscience laws, often referred to as conscience clauses or accommodation laws, are designed to protect individuals and entities from being compelled to participate in activities that conflict with their deeply held moral or religious beliefs. In summary, the history of conscience laws in the U.S. reflects a dynamic evolution, driven by changing societal values, legal interpretations, and ongoing debates about the balance between religious freedom and the rights of individuals (Health and Human Services Department, 2024; Office for Civil Rights (OCR), 2010). The purpose behind incorporating references to conscience laws within this theory adaptation is to underscore the notion that conscience transcends mere philosophical abstraction. By grounding the discussion on conscience as defined in within a legal context, we can focus on the mechanics of the theory.

For this framework, conscience is

defined as an intrinsic motivational force guided by a person's moral beliefs. Those moral beliefs may or may not be rooted in religion and a person's moral beliefs can change or evolve. Moral beliefs or decisions can also be situational or relative. One need only ponder a variant of the trolley problem to realize how moral dilemmas can scramble our understanding of decision-theory.

5. Psyops

Propaganda and other variants of psychological manipulation have been used since the dawn of time. The US Department of Defense updated its doctrine on psychological operations and clarified that the purpose of PSYOPS is to convey selected information, indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals favorable to the originator's objectives (US Department of Defense, 2010). The term PSYOPS has been used interchangeably with information warfare, psychological warfare, and information operations at different points in history, but the overarching objective has always been to influence the target's behaviors through information and emotion (Hwang & Rosen, 2019; Linebarger, 1950). According to Pop (2017), all critical PSYOPS have three core objectives: acquiring knowledge, thwarting the enemy's attempts at the acquisition of knowledge, and misleading the enemy to build a database containing inefficient and useless information. Malyuk (2022) argues that the most important elements in information operations are informational and psychological suppression of the enemy, but also acknowledges that if citizenry know how to recognize the tactics of information warfare it weakens and minimize their effectiveness (Malyuk, 2022). Fraudsters use the weaponization of conscience to influence their victims' behaviors through information and emotion.

6. Complex systems

Complexity science is the study of the relationship between systems. At its inception in the 1950s, system dynamics focused primarily on corporate and industrial problems such as production cycles, and supply chains. It relied heavily on hand-drawn simulations and calculations before computer modeling was available. Today, the principles of system dynamics are applied across various disciplines and industries including public policy, healthcare, and social systems (Gentili, 2021). The transferable principles of dynamic systems and amenability to qualitative manual model construction make system dynamics well-suited for modeling the weaponization of conscience. Complex systems are highly interdependent, decentralized, self-organized, adaptive, and sensitive to feedback loops (Forrester, 2003). Complex systems may also exhibit the butterfly effect, borrowed from chaos theory, where a small change in the system exhibits an unexpectedly amplified effect in the output (Samoilenko & Osei-Bryson, 2007). According to the system dynamics perspective, every decision is made in the context of a feedback loop, a circular flow of information or effects that cause the system to regulate or adjust its behavior based on the information returned in each cycle (Forrester, 2003). Complex systems obey the laws of conservation and accumulation. The law of conservation states that energy cannot be created or

destroyed, it can only be transferred or transformed. A key distinction between linear and complex systems is that the behavior of a linear system can be understood by examining its individual parts whereas a complex system is highly interconnected, and the system behavior emerges from the interactions between its parts. Weaponization of conscience is an example of a complex system.

7. Dual process of moral judgement

Dual-process theory of moral judgement asserts that moral decisions are the result of either one of two distinct mental processes, intuitive or conscious (Greene, 2009). Greene's dual-process model of moral judgement posits that intuitive judgements are fast, emotionally-driven, and primarily deontological (rule-based) whereas conscious decisions are deliberative and characteristically utilitarian (Greene, 2009).

For simplicity, the subcomponents of the conscience system are described in binary terms, but it is important to note that each subcomponent is dynamic, interacts with the other subcomponents, and rests on a continuous scale as depicted in Figure no. 1. Moral beliefs shift, emotions shift and vary in intensity. Additionally, this researcher posits that no decisions or actions can be taken without passing through each phase, and the subsystem is activated by an external event or interaction not depicted.

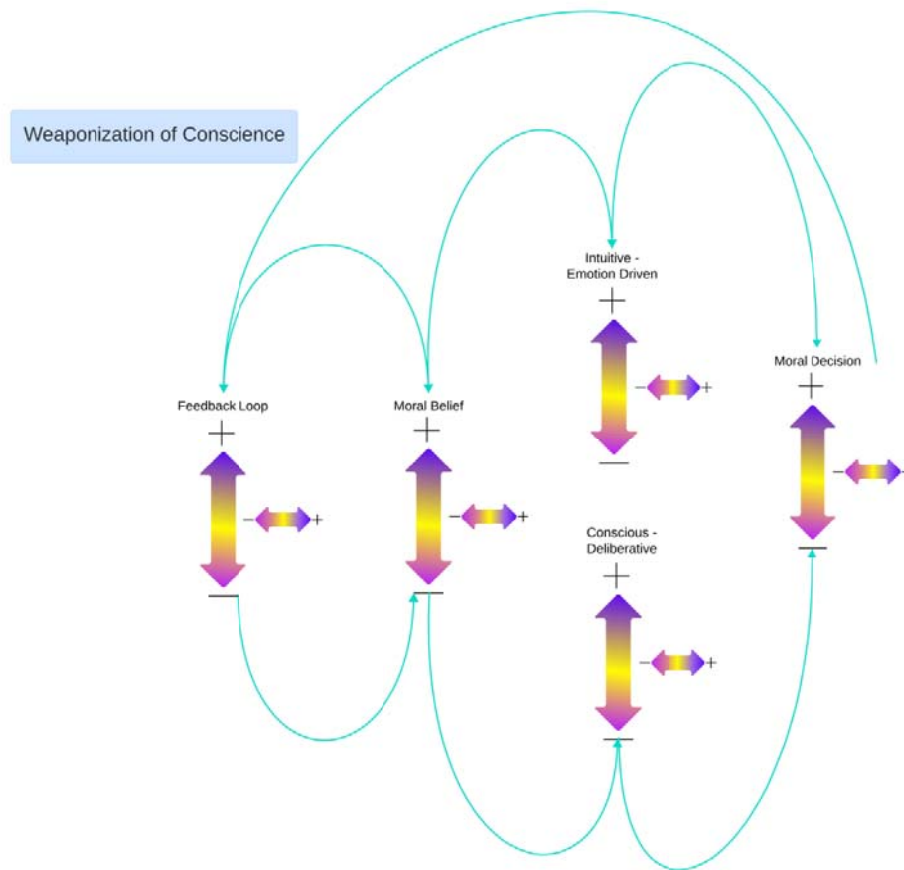


Figure no. 1: *Weaponization of conscience*
(Source: Author's own contribution)

8. Application

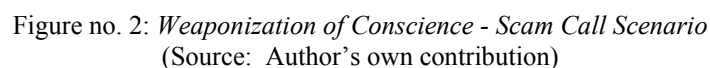
8.1. Scam call example

Financial exploitation from scam calls is one of several growing variants of cybercrime and online fraud costing victims billions each year (Doyle, 2022). The scammer may call their victim posing as a loved one in distress needing money or ransom. A higher level of distress is likely to intensify the victim's level of fear and urgency. Their decision to act, will skew heavily towards intuitive cognitive processes. Now, assume that the scammer(s) call and pose as two loved ones in distress needing money or ransom, but the victim can only afford the ransom for one. The dilemma shifts the victim's moral decision processes more heavily towards conscious/deliberative processes, but the emotional intensity will be [arguably] higher than the intensity experienced in the

single-hostage scenario. Increased fear levels typically slow decision-making and increase deliberative processes (Wake et al., 2020; Wang et al., 2023). The victim's decision processes are strained by the additional cognitive load and weakened further by the intensification of emotion. When moral dilemmas are personal to the decision-maker, studies have demonstrated that utilitarianism is reduced (Starcke & Brand, 2012). Additional variables that might influence how the victim responds include the relationship to the hostage, the intensity of threat, the victim's gender, age, or experience with similar scams.

To counter this double-load effect, one solution may be to hang up the phone and call the loved one directly. Another solution may be to create a pre-arranged code word to authenticate loved ones' identities in these situations. This researcher does not seek to

concept and enable readers to think through cognitive processes from a systems perspective to identify vulnerabilities and tactics used by fraudsters.



person's belief as negative or oppositional leads to firmer entrenchment in that belief (Bizer et al., 2011), fraudsters can increase the intensity of the moral belief dial and potentially the intensity of the intuitive dial before presenting the victim with a phishing site seeking recurring donations in support of a cause likely to appeal to the target. The priming effect of manipulating the victim's conscience system before soliciting donations to a fictitious organization may yield higher donation amounts than if the priming had not been done beforehand. Defending against this weaponization of conscience requires potential victims to be conscious of the reaction that messaging evokes and to consider the source and motives of the messenger.

Voter registration lists are public record in several countries. Knowing a victim's voter party-affiliations, particularly in hyper-partisan countries, enables scammers to estimate their target's belief system and causes or passions that may evoke intense emotional responses. Using the moral belief 'dial' from the weaponization of conscience in Figure no. 3, assume that the target's intensity of belief in a specific cause is in the middle of the spectrum. Combining McGuire's (1964) inoculation theory, whereby initial weak counter-attitudinal messages lead to stronger resistance against subsequent counter-attitudinal messages with valence-framing, where framing a

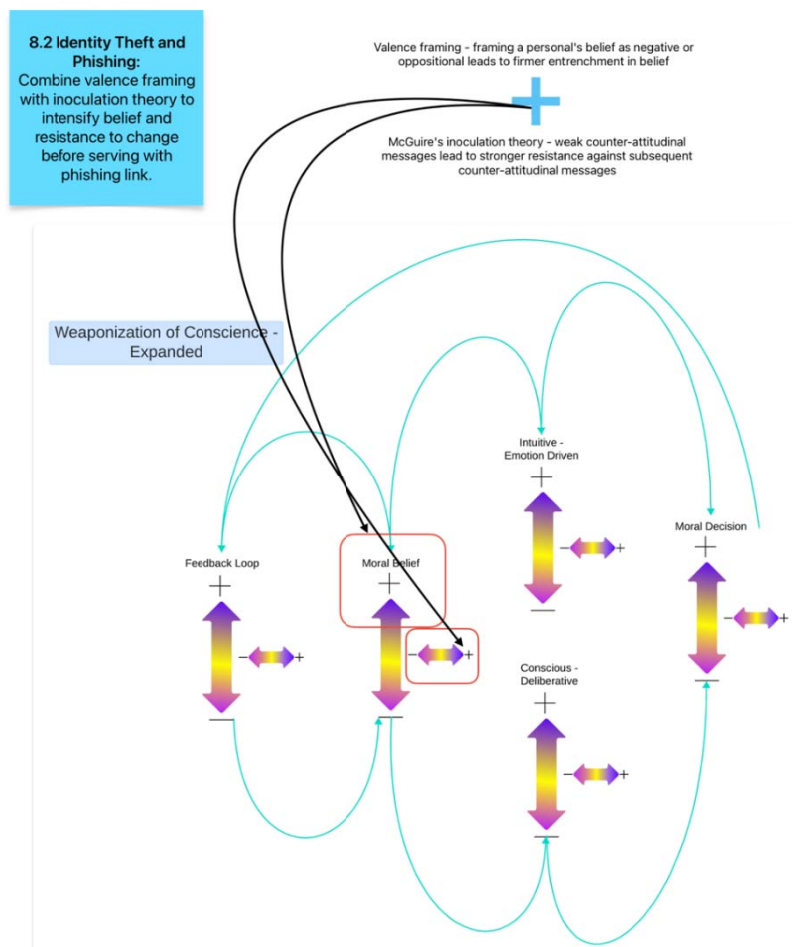


Figure no. 3: *Weaponization of Conscience - Phishing Link Example*
(Source: Author's own contribution)

9. Conclusion

This article introduced the concept of *weaponization of conscience* as a complex system and tactic used by fraudsters to camouflage their activity, coerce others, or to deceive their victims. Weaponization of conscience is a complex subsystem within the larger complex system of social engineering. This framework defines conscience as an intrinsic motivational force guided by a person's moral beliefs. Those moral beliefs may or may not be rooted in religion and a person's moral beliefs can change or evolve. Moral beliefs or decisions can also be situational or relative.

The decision system is always activated by an event or stimulus from outside the conscience subsystem such as when a user is presented with a phishing link or receives a scam call. The starting point (state) of the

conscience system is influenced by multiple factors such as preceding events, mood, time of day, priming events. It is not unusual for multiple feedback loops to manifest in the subsystem and sometimes these feedback loops will have different delay times. Modeling decisions and decision interactions as complex systems enables practitioners to incorporate situational or domain-specific details with decision theories to pinpoint vulnerabilities in historical and prospective cyber defense strategies.

Hardin's argument that the conscience weakens humanity may be true, but just as we developed bulletproof vests because a person cannot survive without a beating heart, so too we must develop defenses against the weaponization of conscience. Without conscience, humanity cannot survive.

REFERENCES

- Bizer, G.Y., Larsen, J.T., & Petty, R.E. (2011). Exploring the valence-framing effect: Negative framing enhances attitude strength: Valence framing. *Political Psychology*, Vol. 32, Issue 1, 59-80.
- Cornelissen, J. (2017). Editor's comments: Developing propositions, a process model, or a typology? Addressing the challenges of writing theory without a boilerplate. *Academy of Management Review*, Vol. 42, Issue 1, 1-9.
- Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice: The International Journal of Policy and Practice*, Vol. 20, Issue 3, 358-375.
- Darii, A., & Meleca, M. (2022). *Trafficking in human beings*. ASEM.
- Doyle, N. (2022). *Elder Financial Exploitation and Scam Activities Targeting Elderly Victims*. Available at: https://repository.stcloudstate.edu/cjs_etds/17/.
- Espinoza, M.D. (2024). A Qualitative Analysis of Challenges in Online Fraud Detection and Investigation. In *Change Dynamics in Healthcare, Technological Innovations, and Complex Scenarios* (pp. 158-170). IGI Global.
- Forrester, J.W. (2003). Dynamic models of economic systems and industrial organizations. *System Dynamics Review*, Vol. 19, Issue 4, 329-345.
- Gentili, P.L. (2021). Why is Complexity Science valuable for reaching the goals of the UN 2030 Agenda? *Rendiconti Lincei. Scienze Fisiche e Naturali*, Vol. 32, Issue 1, 117-134.
- Greene, J.D. (2009). Dual-process morality and the personal/impersonal distinction: A reply to McGuire, Langdon, Coltheart, and Mackenzie. *Journal of Experimental Social Psychology*, Vol. 45, Issue 3, 581-584.
- Hardin, G. (1968). The tragedy of the commons. The population problem has no technical solution; it requires a fundamental extension in morality. *Science (New York, N.Y.)*, 162(3859), 1243-1248.
- Health and Human Services Department. (2024). Safeguarding the Rights of Conscience as Protected by Federal Statutes. In *Federal Register (No. 2024-00091; Vol. 89, pp. 2078-2109)*. Available at: <https://www.federalregister.gov/documents/2024/01/11/2024-00091/safeguarding-the-rights-of-conscience-as-protected-by-federal-statutes>.
- Hwang, T., & Rosen, L. (2019). *Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps*. demtech.oii.ox.ac.uk. Available at: <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf>.
- Jaakkola, E. (2020). Designing conceptual articles: four approaches. *AMS Review*, 10 (1-2), 18-26.
- Kshetri, N. (2017). Cybercrime Firms' Internationalization Strategy and Tactics: An Exploratory Framework. *AMCIS 2017 Proceedings*. Available at: <https://aisel.aisnet.org/amcis2017/Global/Presentations/12/>.
- Linebarger, P. (1950, March 1). *Psychological Warfare*. Naval War College Information Services for Officers. Naval War College Press. Available at: <https://orangelabel.co/wp-content/uploads/2023/08/1951-Psychological-Warfare-US-Navy-War-College.pdf>.
- Maksymenko, S.D., & Derkach, L.M. (2023). Understanding modern cognitive ware in the global dimension, its genesis in the Ukrainian context: A review and directions for future research: Cognitive warfare and social impact operations. *Defense & Strategy/Obrana a Strategie*, Vol. 23, Issue 1.

Malyuk, A.A. (2022). Socio-psychological techniques of information warfare. *Bezopasnost Informacionnyh Tehnologiy*, Vol. 29, Issue 3, 18-37.

Masakowski, Y.R., & Blatny, J.M. (2023). Mitigating and responding to cognitive warfare. *North Atlantic Treaty Organization (NATO), Tech. Rep.* Available at: <https://apps.dtic.mil/sti/citations/trecms/AD1200226>.

Neculcea, C.-A., & Răpan, F. (2022). Information operations– comparative doctrinal analysis. *Strategic Impact*, Vol. 85, No. 3-4, 68-79.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, Vol. 9, Issue 3, 71-88.

Office for Civil Rights (OCR). (2010, October 14). *Conscience and Religious Nondiscrimination*. Hhs.gov; US Department of Health and Human Services. Available at: <https://www.hhs.gov/conscience/conscience-protections/index.html>.

Onushi, K. (2023). Toward clarifying the gap between prohibited perfidy and ruses: A role for the principle of good faith? *Doshisha Law*, Vol. 74, Issue 8. Available at: <https://doshisha.repo.nii.ac.jp/record/29547/files/028004340003.pdf>.

Ragins, B.R. (2012). Reflections on the craft of clear writing. *Academy of Management Review*, Vol. 37, 493-501.

Rutherford, J.R. (2017). *A Holistic Approach Using Honey Communities For Cyber Event Detection and Protection in Communities and Large Distributed Organizations* (G. B. White, Ed.) [The University of Texas at San Antonio]. Available at: <http://proxymu.wrlc.org/login?url=https://www.proquest.com/dissertations-theses/holistic-approach-using-honey-communities-cyber/docview/1902262409/se-2>.

Salih, K., & Dabagh, N. (2023). Digital forensic tools: A literature review. *Journal of Education and Science*, Vol. 32, Issue 1, 109-124.

Samoilenko, S., & Osei-Bryson, K.-M. (2007). *Chaos Theory as a Meta-theoretical Perspective for IS Strategy: Discussion of the Insights and Implications*. Available at: <https://aisel.aisnet.org/sais2007/45/>.

Starcke, K., & Brand, M. (2012). Decision making under stress: a selective review. *Neuroscience and Biobehavioral Reviews*, Vol. 36, Issue 4, 1228-1248.

US Department of Defense. (2010). *Joint publication on psychological operations*. Available at: <https://irp.fas.org/doddir/dod/jp3-13-2.pdf>.

Wake, S., Wormwood, J., & Satpute, A.B. (2020). The influence of fear on risk taking: a meta-analysis. *Cognition & Emotion*, Vol. 34, Issue 6, 1143–1159.

Wang, L., Chen, S., & Xiao, W. (2023). Effect of real-world fear on risky decision-making in medical school-based students: A quasi-experimental study. *Frontiers in Behavioral Neuroscience*, Vol. 17, 1030098.