This is the peer reviewed author accepted manuscript (post print) version of a published work that appeared in final form in:

Thinyane, Mamello 2024 'Aspectual human performance variability in social engineering attacks', Journal of Information Warfare, vol. 23, no. 1

This un-copyedited output may not exactly replicate the final published authoritative version for which the publisher owns copyright. It is not the copy of record. This output may be used for non-commercial purposes.

Persistent link to the UniSA Research Outputs Repository:
https://researchoutputs.unisa.edu.au/11541.2/38711

General Rights

Copyright and moral rights for the publications made accessible in the UniSA Research Outputs Repository are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the persistent link identifying the publication in the UniSA Research Outputs Repository

If you believe that this document breaches copyright, please contact us and provide details. We will remove access to the work immediately and investigate your claim.

Aspectual Human Performance Variability in Social Engineering Attacks

M Thinyane

STEM Unit
University of South Australia
Adelaide, Australia

E-mail: mamello.thinyane@unisa.edu.au

***Abstract**: Most of the influence and persuasion techniques used in social engineering have been documented across many domains, including cybersecurity, and have been shown to rely on similar effect mechanisms used in areas such marketing, scams, and street cons. This paper shows that while these attacks are explained in terms of the social and psychological effect mechanisms, the aspectual lens provides a more nuanced understanding of human performance variability implicated in social engineering. The aspectual lens provides a comprehensive analytical and ontological framing, and hints at aspectually informed measures for mitigating social engineering attacks and dampening the said human performance variability.*

Keywords: *Cybersecurity, Social Engineering, Aspectual Analysis, Human Performance Variability,*

Introduction

Social engineering takes different manifestations in different domains, however, it is primarily the act of influencing individuals to take actions that may or may not be in their best interest (Abeywardana et al., 2016; Sabouni et al., 2017). Traditionally social engineering has been used in scams and street cons to trick the mark (i.e., the intended victim) into behaviours that are not in their interest (Stajano & Wilson, 2011). In the military domain and in the context of information warfare, which as with any form of warfare, is about the exercise of power to influence certain behaviours in others, social engineering is associated with manipulating human behaviour in order to "protect, exploit, corrupt, deny or destroy information or information resources in order to achieve a significant advantage" (Denning, 1998; Schwartau, 1996; Taddeo, 2017). In cybersecurity, where it remains one of the most effective attack vectors, social engineering is about taking advantage of human weaknesses in order to breach individual or organizational security (Al-Thani, 2022).

However social engineering techniques are not only used towards adversarial and malicious ends, but they have also been effectively and ethically used in marketing (e.g., social-marketing, charitable marketing, cause-related marketing) to influence certain behaviours in consumers. These techniques also underly many persuasive technology solutions (Kennedy & Parsons, 2014).

It is widely understood that across all these different domains, social engineering fundamentally exploits elements of human psychology and social functioning to manipulate, trick, convince, persuade, manoeuvre, or confuse people into performing specific actions. These effect mechanisms and principles have been well researched and document in literature (Cialdini, 2007; Ferreira et al., 2015; Gragg, 2003; Stajano & Wilson, 2011). While the framing of these effect mechanisms generally accounts for and explains the psychological and social exploitation of human weaknesses, they have generally been inductively formulated from the case studies and observations of specific social engineering incidents.

This research explores social engineering from the perspective of the theory of modal aspects, a philosophical framework that accounts for diversity and holism of every day human functioning. The paper shows that the aspectual lens not only accommodates the current formulations of social engineering effect mechanisms, but it also provides a more philosophically grounded ontological framing of the effect mechanisms, as well as a nuanced and comprehensive understanding of social engineering as representing human performance variability and detrimental functioning across the different modal aspects.

The rest of the paper is structured as follows, the next section discusses the overall research approach including the scoping review and aspectual analysis methodologies used in this research. The paper then presents a review of the current literature on social engineering effect mechanisms, principles, and technique; discusses the notion of human performance variability as it relates to safety and security in socio-technical systems; and introduces the theory of modal aspects. This is followed by an analysis of social engineering from the aspectual lens and discussion of the benefits and limitations of this framing.

Research approach

The primary line of inquiry in this research is to explore social engineering attacks through the lens of the theory of modal aspects and to demonstrate the utility of the aspectual lens for enriching the understanding of social engineering attacks. The research started with a scoping review of the current body of knowledge on social engineering attacks. Scoping reviews are a methodological approach for evidence synthesis and for mapping out and clarifying key concepts and elements associated with a research area (Arksey & O'Malley, 2005; Peters et al., 2015). They generally have a broader focus and are less rigorous than systematic literature reviews.

The review undertaken in this research is informed by the framework proposed by Peters et al (2015). The main questions addressed in the scoping review are "What are the effect mechanisms, techniques and principles in social engineering?", "What theoretical instruments are used for explicating social engineering?" and lastly "What are the classification heuristics used for social engineering attacks?". The scoping review was limited to articles from the IEEEXplore database and to articles about social engineering attacks, approaches, or techniques excluding techno-centric articles, especially those related to machine learning solutions – as per the search terms below:

("Document Title": "social engineering") AND
("All Metadata": attack OR "All Metadata": technique OR "All Metadata": approach) NOT ("All Metadata": "machine learning" OR "All Metadata": "model")

The main inclusion criteria for the articles were conference, book, and journal articles published in the English language between 2006 and 2023 and readily available. In total 73 articles were identified from the search and ultimately 47 articles were reviewed – as detailed in the flow diagram in *Figure 1*.

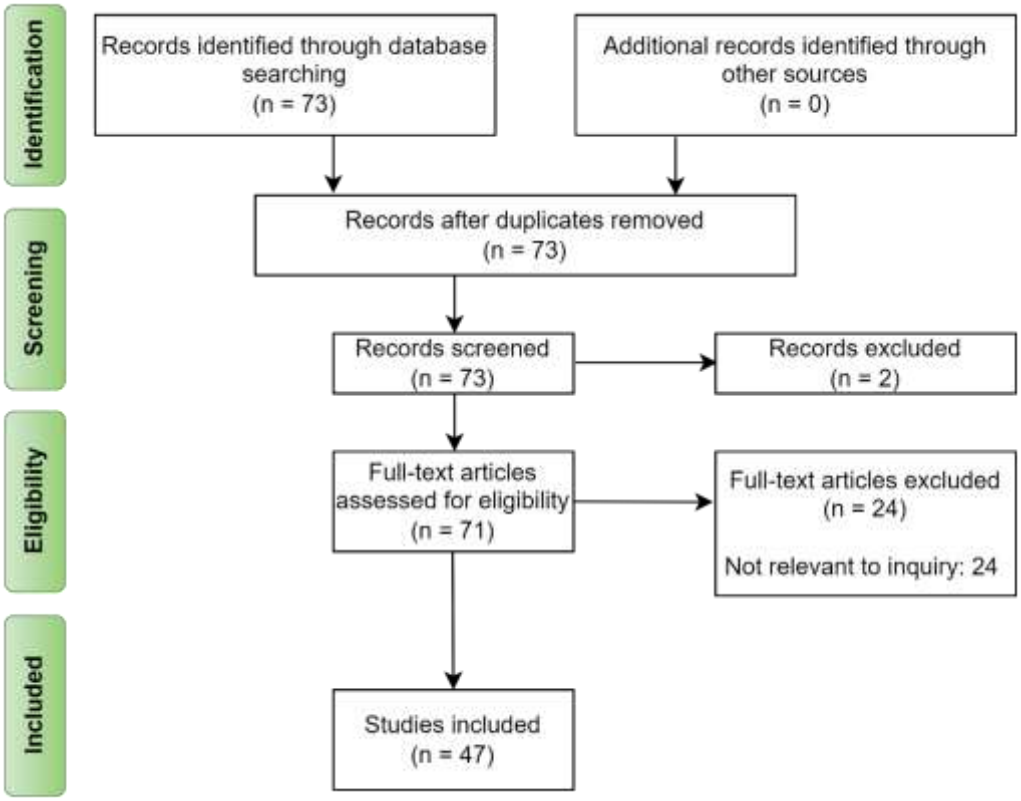


Figure 1 - PRISMA flow diagram for selection of articles for the scoping review

For the analysis of the included articles, a template analysis approach was employed. Template analysis is a narrative analysis method that codes data based on an *a priori* codebook which is refined as the analysis ensues (Brooks et al., 2015). For this research, the *a priori* codebook was derived from the scoping review questions listed above. The analysis was undertaken on the NVivo qualitative analysis software.

Once the key social engineering effect mechanisms, principles, and techniques were identified through the scoping review, aspectual analysis was undertaken to characterize these elements. Aspectual analysis is an analysis method that can be used to reviews text to identify the key modal aspects operational in the text (Basden, 2023). This method is based on the Theory of Modal Aspects, which is introduced in the next section.

Literature Review and Background

Social engineering effect mechanisms and defences

The effectiveness of social engineering as an attack vector and the difficulty of mitigation is fundamentally related to the variability and complexity of human behaviour. Research to understand the effect mechanisms (i.e., how social engineering techniques exploit human vulnerabilities) and their effectiveness has been undertaken across many disciplines, including from neuroscience – to understand brain functioning across the neocortex, limbic system, and reptilian brain, during social engineering attacks; cognitive science – in terms of the cognitive biases that affect human decision-making; psychology – to understand human behaviour and mental processes associated with social engineering; and information and communication sciences – to understand the effects of messaging on effectiveness of social engineering attacks. A large body of work explains the effectiveness of social engineering techniques, such as phishing, pretexting, shoulder surfing, and piggybacking, with reference to exploiting psychological and social human functioning through persuasion and deception (Wang et al., 2021).

Cialdini (2015) identified persuasion techniques and mechanism that are used in sales and marketing and which have relevance to social engineering. Other principles were identified from scams and street cons by Stajano and Wilson (2011), and in another effort, Gragg (2003) identified and enumerated psychological triggers in social engineering. Commonalities across these effect mechanisms have been noted and have inspired the formulation of the principles of persuasion in social engineering, namely: authority; social proof; liking, similarity and deception; commitment, reciprocation and consistency; and distraction (Ferreira et al., 2015). Further research has explored social engineering specifically within the cybersecurity context and enumerated the following effect mechanisms: persuasion; social influence; cognition, attitude and behaviour; trust and deception; language, thought and decision; and emotion and decision making (Wang et al., 2021). These principles and effect mechanisms have not only been found to be prevalent in many phishing attacks but have also been found to be used in combinations of specific pairs or triplets (Ferreira et al., 2015).

Other psychological functioning factors have been found to explain why people fall for social engineering attacks, namely that as an efficiency-thoroughness trade-off people employ a heuristic process and mental shortcuts to make judgements about incoming information. The heuristic thinking process is the way the mind quickly interprets stimuli and inputs from the environment along existing input-to-event patterns (Qin & Burgoon, 2007; Vishwanath, 2022). This interpretation, and the associated risk belief, is informed by the perceived task complexity, expertise belief, and metacognition. Tasks that are perceived to be simple and that individuals have expertise to perform, such as using email or the Internet, tend to be perceived as less risky. Further, individual's poor metacognition (i.e., self-knowledge of one's lack and deficits) can lead to inaccurate risk belief with the corollary of risky behaviour. A low cyber risk belief is associated with heuristic thinking where, in the case of phishing attacks, individuals are reluctant to exert any cognitive effort towards appraising senders' communicative behaviours (Vishwanath, 2022). Besides the psychological functioning, research has also found that susceptibility to social engineering attacks may be related to psychometrics and demographics, such as level of education, socioeconomic status, gender, and family structure (Al-Thani, 2022).

Research has been undertaken on the adversarial elements of social engineering attacks. These include attack frameworks and models, such as the "Mitnick Attack Cycle" - comprising "information gathering, rapport building, attack and utilization" steps, or the related "information gathering, relationship development, exploitation, and execution" cycle (Abeywardana et al., 2016; Wilson & Hadnagy, 2010). These instruments help defenders to better understand the attackers' tactics, techniques, and procedures (TTPs) to inform relevant countermeasures.

Efforts to detect and defend against social engineering are broadly in terms of technical, human and social, physical, organizational, and legal controls. The technical controls are generally targeted at preventing attacks or assisting humans in detecting attacks. For the former these include solutions such as firewalls, real-time email blocking and security (e.g., Domain-based Message Authentication Report and Conformance – DMARC, Sender Policy Framework – SPF, or DomainKeys Identified Mail Policy - DIMP), end-point security measures, and intrusion detection systems (IDS). For the latter these include Automatic Deception Detection Systems to assist humans in identifying and detecting deception (Qin & Burgoon, 2007). Human and social level controls typically emphasize awareness raising, training, and security education, including phishing simulations to improve the ability of individuals to recognize signs of phishing attacks. Physical security, such as biometrics and access controls, restrict physical access to specific critical assets within an organization and mitigate physical social engineering attacks (Abeywardana et al., 2016). Organizational controls are mostly enacted through security policies and information security governance within the organization, with reference to well-established enterprise security standards such as the Control Objectives for Information and Related Technology (COBIT) published by Information Systems Audit and Control Association (ISACA) and the Information Security Management Systems (ISMS) – created through the ISO/IEC27001 and 27002 standards. Lastly legal controls and countermeasures are meant to dissuade attackers from perpetrating the attacks in the first place.

The effectiveness of some of these solutions has been demonstrated in specific contexts, particularly for the less complex, more technical, and physical elements of social engineering attacks. For example, email filtering systems, especially coupled with recent artificial intelligence capabilities, are increasingly effective at identifying phishing attacks. However, for the most sophisticated and targeted attacks, humans are still the primary and most important layer of defence against phishing attacks; thus, alluding to the importance of strengthening human capabilities to mitigate social engineering attacks. Research has demonstrated challenges associated with human and social solutions (e.g., user security training), which include the complexity of human psychosocial functioning and the techno-centric, narrowly defined solutioning that is not informed by insights from social and cognitive sciences (Vishwanath, 2022). Thus, the challenge is at one level, about understanding human performance variability, which is discussed in the next section, and at another level, about expanding the paradigm within which these solutions are formulated and framed.

Human performance variability in socio-technical systems

Cybersecurity has traditionally been concerned with the security of technological artifacts, including data, systems, and networks. However, with the recent digital transformation, the

cybersecurity domain has evolved to encompass the complex assemblages at the confluence of cyber-physical-social spaces. Socio-technical systems perspectives account for this complexity by giving recognition to the fact that cybersecurity is enacted across the technical and social dimension, with the later comprising the human and social elements (Malatji et al., 2019).

Many models and frameworks have been developed, in the fields of safety management, safety science, and security studies, to understand safety and security in socio-technical systems. These models have made headways into the cybersecurity domain to inform the thinking around security in cyber-physical-social spaces from the socio-technical systems perspective (Ebert et al., 2023; Friedberg et al., 2017). One relevant framework, for this research, is the functional resonance analysis method (FRAM) which is an approach for modelling the functional behaviour of complex socio-technical systems. This method addresses the limitations of deterministic linear and probabilistic approaches for understanding such systems (Hollnagel, 2012; Patriarca et al., 2020). FRAM describes systems in terms of the interactions between interrelated functions of the system, specifically in terms of how outputs from functions interact with elements of the downstream functions (e.g., as resources, pre-conditions, timing, or controls). Some of the key insights from this method is the recognition that adverse systems outcomes, such as failure, can be associated with functional resonance across the elements of the system, and that the resonance is a result of the coupling of the performance variability between functions (Hollnagel, 2012).

In socio-technical systems, performance variability can be identified across technological functions – which are the operations undertaken by machines or computers, human functions – which are undertaken by people individually or collectively, or organizational functions – which are explicitly organized operations undertaken by groups of people within an organizational context. In general, technical functions are stable and exhibit limited performance variability. Organizational functions have low frequency performance variability due to organizational inertia, however, can have high amplitude of performance variability. On the other hand human and social systems are typically characterised by high levels of human performance variability, both in terms of frequency (i.e., quick and varied response to changes and input) and amplitude (i.e., potential for large differences between levels of performance). (Hollnagel, 2012). The high performance variability in humans is not only unavoidable and indispensable for socio-technical systems, but also useful and necessary for system's agility and responsiveness (e.g., to respond the threats and opportunities)(Hollnagel, 2012). The reasons for performance variability in system functions can be endogenous – associated with the nature of the function, exogenous – from the working environment, or a result of functional coupling between upstream and downstream function (Hollnagel, 2012).

Relating these to social engineering, one of the reasons why it remains an effective attack vector against individuals and organizations, is because of the high performance variability in humans and social systems. In different contexts and based on different factors, individuals' response to social engineering attacks can vary quickly and dramatically, as discussed in the earlier section in terms of attack effect mechanisms. This human performance variability in social engineering can be due to: endogenous sources - mainly human vulnerabilities (including those associated with demographic and psychometrics - (Al-Thani, 2022)) which are exploited by attackers towards specific adversarial outcomes; exogenous sources – within the organizational

environment including latent conditions that are exploited in social engineering attacks; or due to the influence of upstream functions (e.g., failure in an email-filtering systems). Thus, the effort to mitigate social engineering and reduce human vulnerabilities can be framed in terms of the effort to dampen human performance variability towards consistently secure human behaviour and practices.

Theory of modal aspects

In order to understand performance variability in humans, it is essential to have a sufficiently thorough understanding of human functioning in their everyday life. Dooyeweerd's philosophy and his Theory of Modal Aspects provides a framework for understanding everyday functioning as holistic, coherent, and diverse. This diversity of functioning can be understood in terms of the following fifteen modal aspects in which humans operate and through which things are meaningful: *quantitative* (i.e., discrete amounts), *spatial* (i.e., continuity), *kinematic* (i.e., motion), *physical* (i.e., matter and forces), *biotic* (i.e., life functions), *sensitive* (i.e., feeling and sensing), *analytical* (i.e., logical conceptualization), *formative* (i.e., creative forming), *lingual* (i.e., symbolic meaning), *social* (i.e., interactions), *economic* (i.e., scarcity and limits), *aesthetic* (i.e., harmony), *juridical* (i.e., appropriateness), *ethical* (i.e., self-giving love), and *pistic* (i.e., belief) (Basden, 2019; Dooyeweerd, 1958). Every day, humans function in all these different aspects. Illustratively, authoring this paper involves the reading (i.e., *sensitive*) relevant papers, analysing (i.e., *analytical*) their relevance for the subject of this paper, and synthesizing (i.e., *formative*) a well-argued (i.e., *analytical*) and well-presented (i.e., *aesthetic*) narrative (i.e., *lingual*) that makes due (i.e., *juridical*) contribution to the body of knowledge in this field, while keeping within the word count and page limits (i.e., *economic*). While all these modal aspects are involved in everyday functioning, specific activities and entities become meaningful in specific key modal aspects. With reference to authoring this as a scientific paper, it may be argued that the "most significant" aspects are the *analytical* and the *formative* aspects, while poetry might be most meaningful in the *lingual* and the *aesthetic* aspects.

While a detailed discussion of the theory of modal aspects is beyond the scope of this paper, some of the features of the modal aspects which are relevant for this paper will be discussed. One of these features is that modal aspects have a linear ordering from the quantitative, at the lowest, to the pistic, at the highest - which establishes foundational and anticipatory dependency between the aspects. The foundational dependency means that all aspects depend on and are supported by earlier/lower aspects. For example, symbolic signification and expression at the *lingual* aspect is supported by the lower aspects including *formative*, *analytical*, and *sensitive*. Illustratively, for this sentence to be meaningful (in the *lingual* aspect), it must be possible to create (i.e., *formative*) sequences of letters which are delineated into words in a syntactically meaningful way (i.e., *analytical*) and in a font colour that can be read (i.e., *sensitive*). On the other hand, anticipatory dependence recognizes the potential of aspects to anticipate meaning provided in later aspects – for example irrational numbers (*qualitative* aspect) are meaningful in anticipation of *spatial* functioning (Basden, 2023).

Another relevant and important feature of aspects is that along with providing spheres of meaning and of law, they are also spheres of normativity and define positive (i.e., good) and detrimental (i.e., bad) functioning across the aspects – at least from the *sensitive* modal aspect.

For example, within the *lingual* aspect, clarity and understanding are positive, while misunderstanding and confusion are detrimental functioning. As a basis for normativity evaluations, the theory of modal aspects provides a framework for analysing positive and negative functioning - as has been undertaken in this research to assess positive and detrimental elements of human performance variability associated with social engineering.

Aspectual lens to social engineering attacks

This research explores social engineering from the aspectual lens to enrich the understanding of social engineering broadly and specifically human performance variability associated with social engineering attacks. For the analysis, social engineering effect mechanisms, principles, and techniques from literature are examined and mapped to the underlying modal aspects within which they operate and are meaningful (see Table *1*).

The first mechanism, persuasion, which is the overarching mechanism in social engineering, is the ability to influence people to think or behave in a certain way. Principles of persuasion and influence, including reciprocation, commitment and consistency, social proofs, liking, authority, scarcity, distraction, social compliance, herd, dishonesty, kindness, need and greed, and time principles are used extensively in many domains to achieve specific outcomes (Cialdini, 2007; Stajano & Wilson, 2011). The same principles are employed in social engineering attacks towards adversarial attack goals (Ferreira et al., 2015). Overall, persuasion is primarily outworked at the *analytical* and *social* aspects in terms of influencing peoples' cognitive functioning, however, some of the principles of persuasion operate across other aspects, for example: distraction, which can be about impeding individuals' concentration or perception operates mostly within the *sensitive* aspect; reciprocation, which involves a mutual exchange and doing something proportionate in return for someone, is mostly enacted within the *social* and *juridical* aspects; commitment and consistency are elements of functioning in the *pistic* aspect; and lastly scarcity is essentially the kernel definition of functioning within the *economic* aspect.

The second mechanism, social influence, relies on the effect of the social group to influence individual behaviour. The main modal aspect implicated in this is the *social* aspect which expresses individuals' interaction and engagement within a collective. Several other social engineering techniques and principles are enacted across the *social* aspect, including social proof, herd principle, group influence and conformity, social responsibility norm – which also includes an element of *juridical* functioning, bystander effect, reciprocity norm, and social exchange effect (Ferreira et al., 2015; Wang et al., 2021). The third effect mechanism is "cognition, attitude, and behaviour", which is primarily enacted at the *analytical* aspect with regards to individuals' cognitive functioning that leads to specific behavioural outcomes (e.g., tricking a victim to click a malicious link). Trust and deception, the fourth effect mechanism, is outworked primarily at the *ethical* aspect because trust entails willingness of give oneself to others and to be vulnerable to others. The fifth effect mechanism, "language, thought and decision", is primarily enacted across the *lingual* and *analytical* aspects, and lastly, "emotion and decision-making" effect mechanisms is enacted across *sensitive* and *analytical* aspects.

While not all discussed in detail, the different social engineering effect mechanisms, principles, and techniques that have been identified from the scoping review can all be mapped across the different aspects as summarized in Table *1* and illustrated in Figure *2*.

Table 1 - Aspectual mapping of social engineering effect mechanisms, principles, and techniques

	Aspect	**Effect mechanisms**	**Performance variability**
1	Quantitative	*Determinative functioning across these modal aspects*	*Traditional system failure modes*
2	Spatial		
3	Kinematic		
4	Physical		
5	Biotic		
6	Sensitive	- Emotion and decision making - Micro expression identification - Facial-action coding system - Facial expression - Deception leakage - Distraction (persuasion and manipulation) - Emotion-arousing	- Inaccuracy - Misperception
7	Analytical	- Cognition, attitude, and behaviour - Persuasion - Cognitive dissonance - Deception leakage - Value perception manipulation - Thought overloading	- Confusion - Deception
8	Formative	- Need and greed principle	- Misdirected
9	Lingual	- Language, thought, and decision. - Persuasive communication (elaboration likelihood) - Language framing effect - Negative language expressions	- Misunderstanding - Lack of clarity
10	Social	- Social influence - (Persuasion) - Group influence and conformity - Informational influence (social proof) - Social compliance - Herd (safety in numbers) - Social responsibility norm - Bystander effect - Deindividuation in group - Source credibility - Obedience to authority - Normative influence (social validation) - Reciprocity norm and social exchange - Self-disclosure norm - Social loafing effect	- Misled - Pressured (social)
11	Economic	- Time pressure - Scarcity: perceived value	- Pressured (urgency)

12	Aesthetic	- Similarity, liking and helping (persuasion) - Group cohesion effect - (Cognitive dissonance)	- Interest (fascination)
13	Juridical	- Moral duty - Dishonesty principle - (Diffusion of responsibility)	- Responsibility
14	Ethical	- Trust and deception - Social responsibility norm (helpfulness) - Trust propensity	- Distrust
15	Pistic	- Commitment and consistency - Foot-in-the-door effect	- Commitment - Loyalty

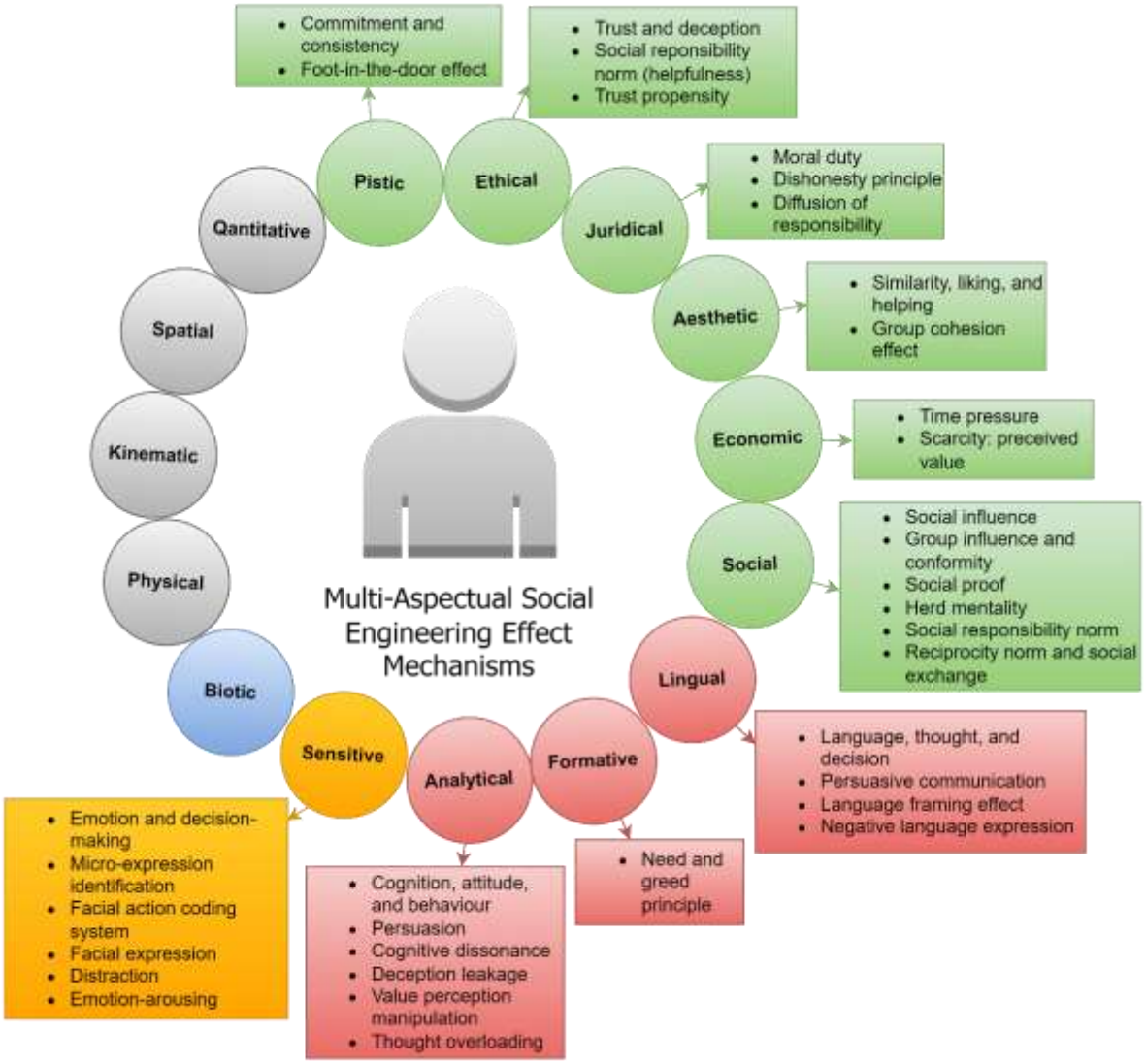


Figure 2 - Aspectual mapping of social engineering principles, effect mechanisms, and techniques

Extensive research has been undertaken on human vulnerabilities and performance variability that is observed across the different social engineering effect mechanisms and techniques.

Research has explored psychological traits and triggers as well as contextual factors that make people more susceptible to social engineering attacks (Ferreira et al., 2015). Exploring the performance variability through the aspectual lens highlights the detrimental functioning, associated with performance variability across all these aspects. For example, typosquatting, which is a technique in which attackers mimic legitimate websites, through URL misspellings, incorrect top-level domains, or subdomain squatting, operate primarily at the *sensitive* aspect and rely on individuals' misperception of the URL. This misperception or inaccuracy represents human performance variability within the *sensitive* aspect. Another example is baiting – where target individuals are enticed with something of value, or quid pro quo – where target individuals are promised something of value in return for help (i.e., including revealing their passwords or sensitive information). Both these attacks are associated with the value perception manipulation technique which primarily operates within the *analytical* aspect. The main human performance variability associated with these attacks and effect mechanism is deception, which leads individuals into believing that there is something of value to be gained in engaging with the attacker. Further elements of detrimental functioning across each aspect, associated with human performance variability, have been listed in *Table 1*.

The analysis undertaken above illustrates that human performance variability can be mapped across the different modal aspects, and that Dooyeweerd's theory of aspects provides an effective framework that can enrich the understanding of social engineering attacks. The next section discusses the main utility of this framing and the opportunities that it opens for exploring mitigation strategies against social engineering attacks.

Discussion

The aspectual analysis presented in this paper highlights the more fundamental, philosophically grounded, kernel mechanisms that are at play across different social engineering effect mechanism. It goes beyond the broad psychological and social dimensions to demonstrate that the interaction between individuals and social engineering attacks is enacted across the different modal aspects, which represent the horizon of every day human functioning. This granular perspective to the effect mechanisms can inform more detailed analyses and solutioning to mitigate social engineering attacks.

The framing presented in this paper provides a nuanced understanding that also allows a distinction to be made between what are typically clustered as similar effect mechanisms. For example, "liking, similarity and deception" are typically clustered together, so are "commitment, reciprocation, and consistency" and "language, thought, and decision" (Ferreira et al., 2015; Wang et al., 2021). However, as revealed from the aspectual analysis above, some of these mechanisms operate at and are meaningful in different aspects. For example, while reciprocation is primarily *social* functioning that anticipates *juridical* functioning, commitment is more associated with *pistic* functioning. Further, for "language, thought, and decision", language is functioning in the *lingual* aspect, while thought and decision are *analytical* functioning. These mechanisms might be clustered together because of co-occurrence in different social engineering attacks; however, the underlying aspectual fundamentals are different and would require different interventions to mitigate.

The aspectual framing presented in this paper, because of the basis on a normative philosophical framework, elevates the discussions about the role and importance normativity of human functions in complex socio-technical systems. One of the key elements of Dooyeweerd's philosophy is the principle of "simultaneous realization of norms", which asserts that detrimental functioning across any aspect leads to unfavourable system outcomes in the long run. For the context of this paper, the principle suggests that monitoring and reducing detrimental functioning in humans across each of the modal aspects identified above, could not only lead to addressing the specific social engineering effect mechanisms, but could also lead to positive system outcomes overall.

Having noted the benefits of the this framing above, it is also worth noting that the main limitation and weakness of this research is that the aspectual mapping undertaken across the different social engineering effect mechanisms, principles and techniques (presented in Table *1* and Figure *2*) could benefit from more rigorous analysis, supplemented by a secondary validation of the mappings. Further, the scoping review used in this research means that the paper hasn't presented a comprehensive enumeration of effect mechanisms, principles, and techniques. However, both limitations simply inform how the mappings should be used, but do not impact the main contribution of the paper – which is to advance the aspectual perspective for understanding human vulnerabilities in social engineering attacks specifically and human performance variability in general.

Conclusion

Social engineering is used in many domains, including cybersecurity and information warfare, to influence and persuade individuals towards certain behaviours. It relies on exploiting elements of humans' psychological and social functioning through well documented effect mechanisms, principles, and techniques. The effectiveness of social engineering attacks and the challenge of mitigating against them is associated with the high variability of human performance (and behaviour). This human performance variability has traditionally been articulated in terms of human weakness and biases enumerated across psychological and social dimensions. This paper, on the other hand, has framed this human performance variability in social engineering in terms of detrimental aspectual functioning – as informed by the Theory of Modal Aspects. The paper demonstrates that the aspectual lens provides a more comprehensive and philosophically grounded analytical and ontological framework that enriches the understanding of social engineering attacks. This aspectual framing invites further research to explore how alternative mitigation strategies can be shaped along the different modal aspects and be coupled for greater effectiveness at defending against social engineering attacks.

References

Abeywardana, K. Y., Pfluegel, E., & Tunnicliffe, M. J. (2016). A layered defense mechanism for a social engineering aware perimeter. *2016 SAI Computing Conference (SAI)*, 1054–1062. https://doi.org/10.1109/SAI.2016.7556108

Al-Thani, N. A. (2022). Adolescents' and social engineering: The role of psychometrics factors in determining vulnerability and designing interventions. *2022 9th International Conference on Behavioural and Social Computing (BESC)*, 1–5. https://doi.org/10.1109/BESC57393.2022.9995705

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

Basden, A. (2019). *Foundations and Practice of Research: Adventures with Dooyeweerd's Philosophy* (1st ed.). Routledge. https://doi.org/10.4324/9781315194912

Basden, A. (2023). *The Dooyeweerd Pages*. https://dooy.info/

Brooks, J., McCluskey, S., Turley, E., & King, N. (2015). The Utility of Template Analysis in Qualitative Psychology Research. *Qualitative Research in Psychology*, *12*(2), 202–222. https://doi.org/10.1080/14780887.2014.955224

Cialdini, R. B. (2007). *Influence: The psychology of persuasion.* (EPub edition.). HarperCollins Publishers.

Denning, D. E. (1998). *Information Warfare and Security*. Addison Wesley.

Dooyeweerd, H. (1958). *A New Critique of Theoretical Thought V1-IV*. Paideia Press. https://paideiapress.ca/products/the-new-critique-of-theoretical-thought

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, *134*, 103435. https://doi.org/10.1016/j.cose.2023.103435

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. In T. Tryfonas & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 36–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-20376-8_4

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, *34*, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

Gragg, D. (2003). *A Multi-Level Defense Against Social Engineering*. SANS Institute - InfoSec Reading Room.

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems*. Taylor & Francis Group.

Kennedy, A.-M., & Parsons, A. (2014). Social engineering and social marketing: Why is one "good" and the other "bad"? *Journal of Social Marketing*, *4*(3), 198–209. https://doi.org/10.1108/JSOCM-01-2014-0006

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Patriarca, R., Di Gravio, G., Woltjer, R., Costantino, F., Praetorius, G., Ferreira, P., & Hollnagel, E. (2020). Framing the FRAM: A literature review on the functional resonance analysis method. *Safety Science*, *129*, 104827. https://doi.org/10.1016/j.ssci.2020.104827

Peters, M. D. J., Godfrey, C. M., Khalil, H., McInerney, P., Parker, D., & Soares, C. B. (2015). Guidance for conducting systematic scoping reviews. *JBI Evidence Implementation*, *13*(3), 141. https://doi.org/10.1097/XEB.0000000000000050

Qin, T., & Burgoon, J. K. (2007). An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. *2007 IEEE Intelligence and Security Informatics*, 152–159. https://doi.org/10.1109/ISI.2007.379548

Sabouni, S., Cullen, A., & Armitage, L. (2017). A preliminary radicalisation framework based on social engineering techniques. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–5. https://doi.org/10.1109/CyberSA.2017.8073406

Schwartau, W. (1996). *Information Warfare: Second Edition* (2nd edition). Thunder's Mouth Press.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, *54*(3), 70–75. https://doi.org/10.1145/1897852.1897872

Taddeo, M. (2017). Information Warfare: A Philosophical Perspective. In *The Ethics of Information Technologies*. Routledge.

Vishwanath, A. (2022). Why do people fall for social engineering? In *The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing* (pp. 89–116). MIT Press. https://ieeexplore.ieee.org/document/9986068

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633

Wilson, P., & Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking* (1st edition). Wiley US.